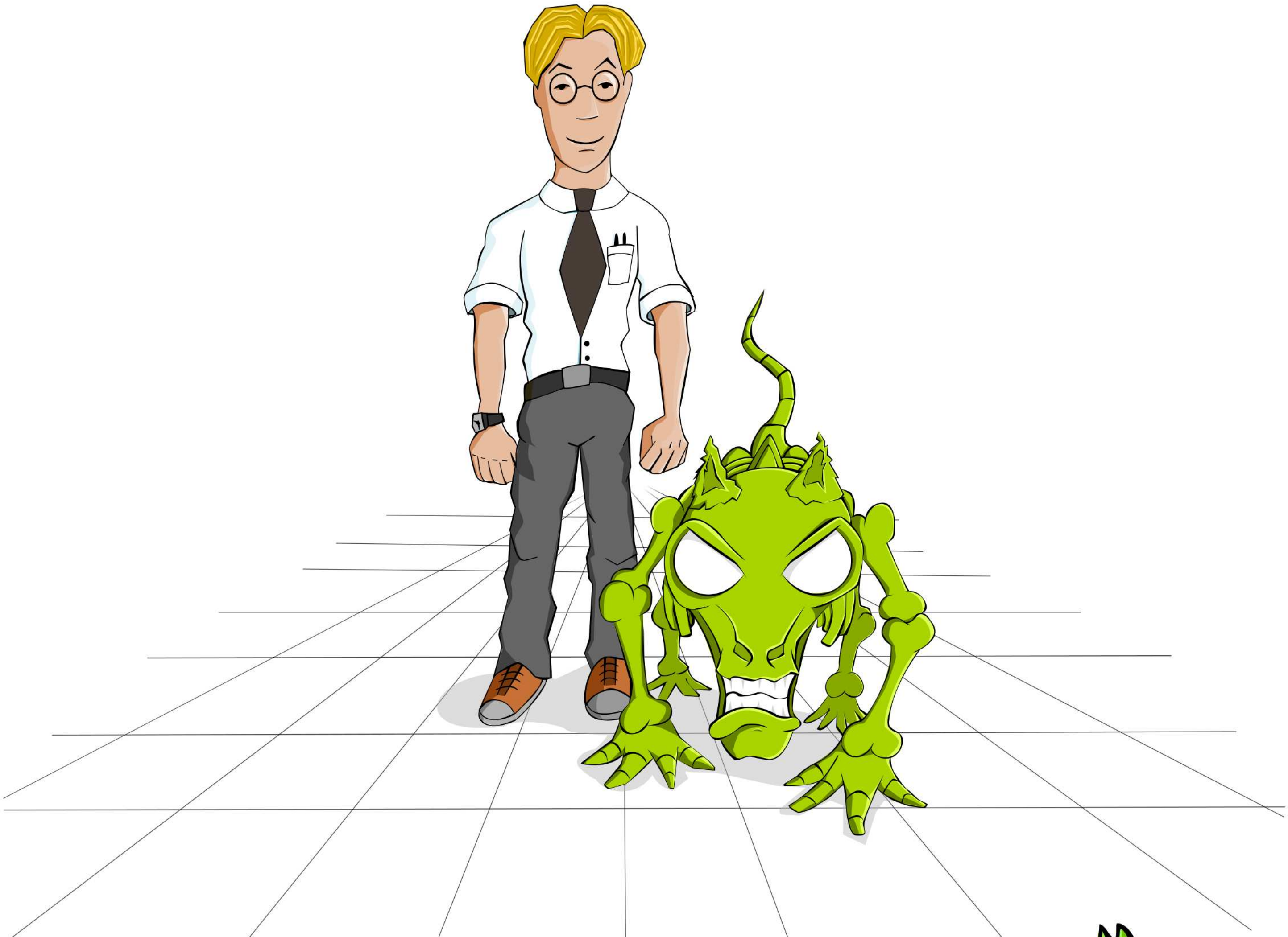
Greenbone Security Manager

with
Greenbone OS 3.1



User Manual

Greenbone

Greenbone

Greenbone Networks GmbH
Neuer Graben 17
49074 Osnabrück Germany
http://www.greenbone.de

Status: GOS 3.1.22, January 26, 2016

This is the manual for the Greenbone Security Manager with Greenbone OS (GOS) version 3.1. Due to the numerous functional and other differences between GOS 3.1 and previous versions, this manual should not be used with older versions of GOS.
The Greenbone Security Manager is under constant development. This manual attempts to always document the latest software release. It is, however, possible that latest functionality has not been captured in this manual.
Should you have additional notes or error corrections for this manual please send an email to support (mailto:support@greenbone.de).

Contributers to this manual are:

- Greenbone Networks GmbH
- OpenSource Training Ralf Spenneberg
- Alexander Rau, arX IT Services

The copyright for this manual is held by the company Greenbone Networks GmbH. Greenbone and the Greenbone-logo are registered trademarks of Greenbone Networks GmbH. Other logos and registered trademarks used within this manual are the property of their respective owners and are used only for explanatory purposes.

CHAPTER 1

Introduction

Vulnerability management is a core element in modern information technology (IT) compliance. IT compliance is defined as the adherence to legal, corporate and contractual rules and regulations as they relate to IT infrastructures. Within its context IT compliance mainly relates to information security, availability, storage and privacy. Companies and agencies have to comply with many legal obligations in this area.

The control and improvement in IT security is an ongoing process that consists at a minimum of these three steps:

- Discovery of the current state
- Taking actions to improve the current state
- Review of the measures taken

The Greenbone Security Manager (GSM) assists companies and agencies with automated and integrated vulnerability assessment and management. Its task is to discover vulnerabilities and security gaps before a potential attacker would. GSM can achieve this through different perspectives of an attacker:

External The GSM attacks the network externally. This way it can identify badly configured or misconfigured firewalls.

DMZ Here the GSM can identify actual vulnerabilities. These could be exploited by attackers if they get past the firewall.

Internal Many attacks are executed internally by insiders through methods of social engineering or a worm. This is why this perspective is very important for the security of the IT infrastructure.

For DMZ and internal scans it can be differentiated between authenticated and non-authenticated scans. When performing an authenticated scan the GSM uses credentials and can discover vulnerabilities in applications that are not running as a service but have a high risk potential. This includes web browsers, office applications or PDF viewers.

Due to new vulnerabilities being discovered on a daily basis, regular updates and testing of systems are required. The Greenbone Security Feed ensures that the GSM is provided with the latest testing routines and can discover the latest vulnerabilities reliably. Greenbone analyzes CVE [1] messages and security bulletins of vendors and develops new testing routines daily.

With a scan using the Greenbone Security Manager, staff responsible for IT, receive a list of vulnerabilities that have been identified on the network. Especially if no vulnerability management has been practiced, the list is often extensive. For the selection of remediation measures a prioritization is inevitable. Most important are the measures that protect against critical risks and remediate those respective security holes.

The GSM utilizes the Common Vulnerability Scoring System (CVSS). CVSS is an industry standard for the classification and rating of vulnerabilities. This assists in prioritizing the remediation measures.

[1] The Common Vulnerability and Exposures (CVE) project is a vendor neutral forum for the identification and publication of new vulnerabilities.

To deal with vulnerabilities fundamentally two options exist:

1. Removal of the vulnerability through updating the software, removal of the component or a change in configuration.
2. Implementation of a rule in a firewall or intrusion prevention system (virtual patching).

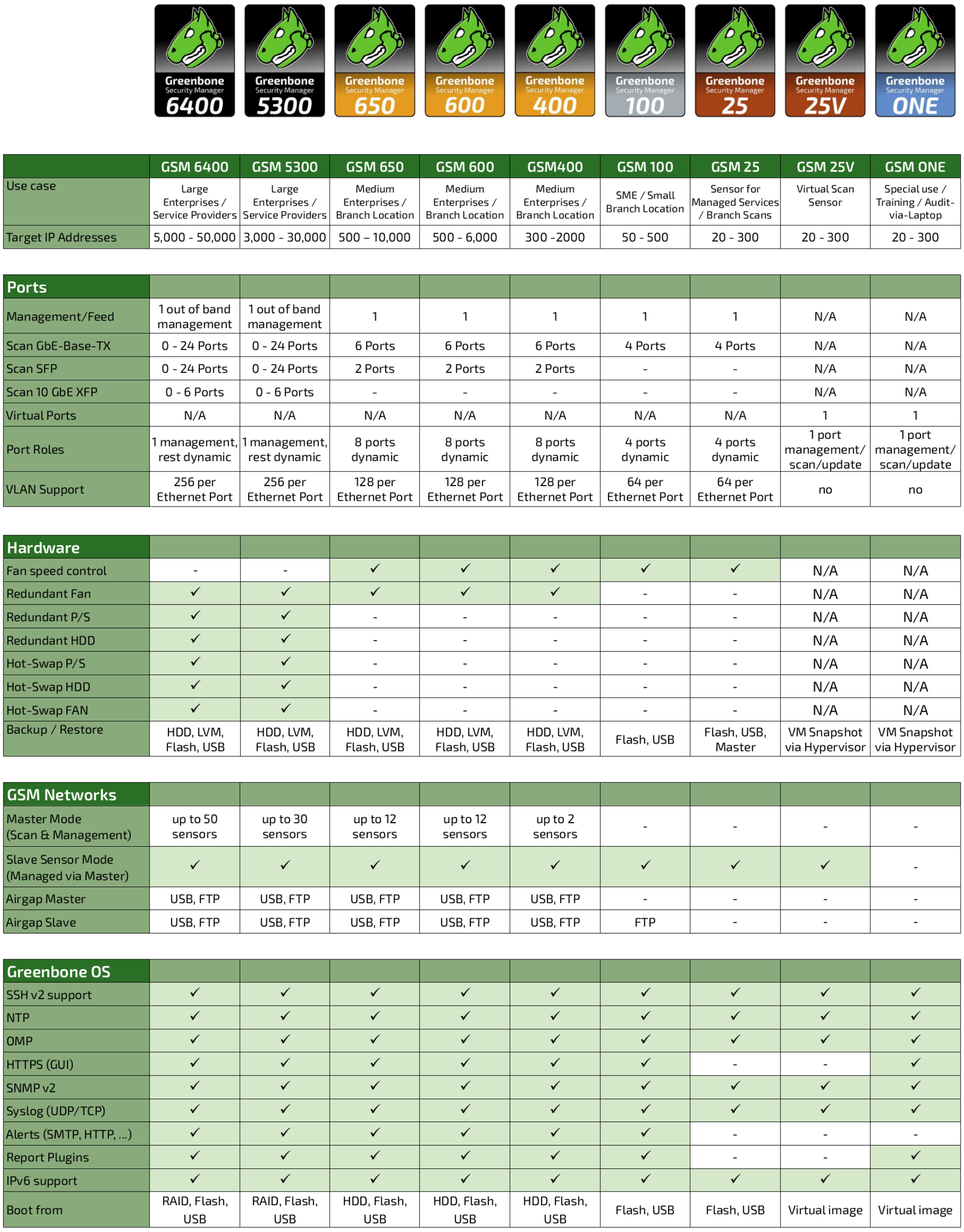
Virtual patching is the apparent remediation of the vulnerability through a compensating control. The real vulnerability still exists. The attacker can still exploit the vulnerability if the compensating control fails or by utilizing an alternate approach. An actual patch/update of the affected software is always preferred over virtual patching.

The Greenbone Security Manager supports the testing of the implemented remediation measures as well. With its help responsible IT staff can document the current state of IT security, recognize changes and document these changes in reports. To communicate with management the GSM offers abstraction of technical details in simple graphics or in the form of a traffic light that displays the state of security in the colours red, yellow and green. This way the IT security process can be visualized in a simplified way.

CHAPTER 2

GSM Overview

The Greenbone Security Manager is a dedicated appliance for vulnerability scanning and vulnerability management. It is a specifically developed platform optimized for vulnerability management. It is offered in different performance levels.



	GSM 6400	GSM 5300	GSM 650	GSM 600	GSM400	GSM 100	GSM 25	GSM 25V	GSM ONE
Use case	Large Enterprises / Service Providers	Large Enterprises / Service Providers	Medium Enterprises / Branch Location	Medium Enterprises / Branch Location	Medium Enterprises / Branch Location	SME / Small Branch Location	Sensor for Managed Services / Branch Scans	Virtual Scan Sensor	Special use / Training / Audit-via-Laptop
Target IP Addresses	5,000 - 50,000	3,000 - 30,000	500 – 10,000	500 - 6,000	300 -2000	50 - 500	20 - 300	20 - 300	20 - 300

Ports									
Management/Feed	1 out of band management	1 out of band management	1	1	1	1	1	N/A	N/A
Scan GbE-Base-TX	0 - 24 Ports	0 - 24 Ports	6 Ports	6 Ports	6 Ports	4 Ports	4 Ports	N/A	N/A
Scan SFP	0 - 24 Ports	0 - 24 Ports	2 Ports	2 Ports	2 Ports	-	-	N/A	N/A
Scan 10 GbE XFP	0 - 6 Ports	0 - 6 Ports	-	-	-	-	-	N/A	N/A
Virtual Ports	N/A	N/A	N/A	N/A	N/A	N/A	N/A	1	1
Port Roles	1 management, rest dynamic	1 management, rest dynamic	8 ports dynamic	8 ports dynamic	8 ports dynamic	4 ports dynamic	4 ports dynamic	1 port management/ scan/update	1 port management/ scan/update
VLAN Support	256 per Ethernet Port	256 per Ethernet Port	128 per Ethernet Port	128 per Ethernet Port	128 per Ethernet Port	64 per Ethernet Port	64 per Ethernet Port	no	no

Hardware									
Fan speed control	-	-	✓	✓	✓	✓	✓	N/A	N/A
Redundant Fan	✓	✓	✓	✓	✓	-	-	N/A	N/A
Redundant P/S	✓	✓	-	-	-	-	-	N/A	N/A
Redundant HDD	✓	✓	-	-	-	-	-	N/A	N/A
Hot-Swap P/S	✓	✓	-	-	-	-	-	N/A	N/A
Hot-Swap HDD	✓	✓	-	-	-	-	-	N/A	N/A
Hot-Swap FAN	✓	✓	-	-	-	-	-	N/A	N/A
Backup / Restore	HDD, LVM, Flash, USB	HDD, LVM, Flash, USB	HDD, LVM, Flash, USB	HDD, LVM, Flash, USB	HDD, LVM, Flash, USB	Flash, USB	Flash, USB, Master	VM Snapshot via Hypervisor	VM Snapshot via Hypervisor

GSM Networks									
Master Mode (Scan & Management)	up to 50 sensors	up to 30 sensors	up to 12 sensors	up to 12 sensors	up to 2 sensors	-	-	-	-
Slave Sensor Mode (Managed via Master)	✓	✓	✓	✓	✓	✓	✓	✓	-
Airgap Master	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	-	-	-	-
Airgap Slave	USB, FTP	USB, FTP	USB, FTP	USB, FTP	USB, FTP	FTP	-	-	-

Greenbone OS									
SSH v2 support	✓	✓	✓	✓	✓	✓	✓	✓	✓
NTP	✓	✓	✓	✓	✓	✓	✓	✓	✓
OMP	✓	✓	✓	✓	✓	✓	✓	✓	✓
HTTPS (GUI)	✓	✓	✓	✓	✓	✓	-	-	✓
SNMP v2	✓	✓	✓	✓	✓	✓	✓	✓	✓
Syslog (UDP/TCP)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Alerts (SMTP, HTTP, ...)	✓	✓	✓	✓	✓	✓	-	-	-
Report Plugins	✓	✓	✓	✓	✓	✓	-	-	✓
IPv6 support	✓	✓	✓	✓	✓	✓	✓	✓	✓
Boot from	RAID, Flash, USB	RAID, Flash, USB	HDD, Flash, USB	HDD, Flash, USB	HDD, Flash, USB	Flash, USB	Flash, USB	Virtual image	Virtual image

2.1 Enterprise class (GSM 5300/6400)

The GSM 5300 and GSM 6400 are designed for the operation in large companies and agencies. The GSM 6400 can control sensors in up to 50 security zones and is recommended for up to 50,000 monitored IP addresses. The GSM 5300 can control sensors in up to 30 security zones and is recommended for up to 30,000 monitored IP addresses. The appliances themselves can be controlled as a slave sensor by another master.

Fig. 2.1: The GSM 6400 supports up to 50,000 IP addresses

The appliances in the enterprise class come in a 2U 19" chassis for easy integration into the data center. For easy installation and monitoring they are equipped with a two line, 16 characters per line LCD display. For uninterruptable operation they have redundant, hot swappable power supplies, hard drives and fans.

For management of the appliance, in addition to an out-of-band management Ethernet port, a serial port is available. The serial port is setup as a Cisco compatible console port.

To connect to the monitored systems both appliances can be equipped with three modules. The following modules can be used in any order:

- 8 Port Gigabit Ethernet 10/100/1000 Base-TX (copper)
- 8 Port Gigabit Ethernet SFP (small-form factor-pluggable)
- 2 Port 10-Gigabit Ethernet XFP

Up to 256 VLANs can be configured and managed per port.

2.2 Midrange class (GSM 400/600/650)

The GSM 400, GSM 600 and GSM 650 are designed for mid-sized companies and agencies as well as larger branch offices. The GSM 650 can control sensors in up to 12 security zones and is recommended for up to 10,000 monitored IP addresses. The GSM 600 can also control sensors in up to 12 security zones and is recommended for up to 6,000 monitored IP addresses. The GSM 400 can control 2 sensors and is recommended for up to 2,000 monitored IP addresses. The appliances themselves can be controlled as a slave sensor by another master.

Aside from the current GSM 400, GSM 600 and GSM 650 appliances, Greenbone is still fully supporting the older appliances in this class. The GSM 500, GSM 510 and GSM 550 appliances were replaced by more up to date hardware in 2014.

The appliances in the midrange class come in a 1U 19" chassis for easy integration into the data center. For easy installation and monitoring they are equipped with a two line, 16 characters per line LCD display. For uninterruptable operation the appliances come with redundant fans. However, hot-swapping during operation is not possible.

For management of the appliance, in addition to a management Ethernet port, a serial port is available. The serial port is setup as a Cisco compatible console port.

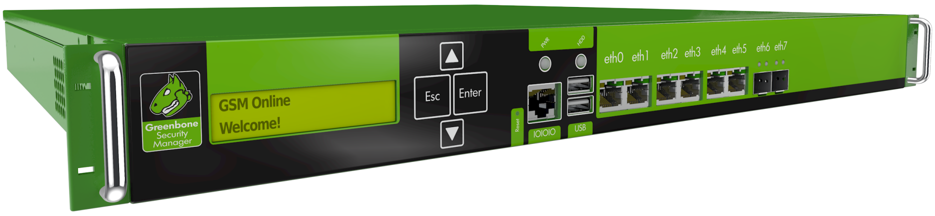


Fig. 2.2: The GSM 650 supports up to 10,000 IP addresses

To connect to the monitored systems both appliances are equipped with eight ports in total, which are pre-configured and set up as follows:

- 6 Port Gigabit Ethernet 10/100/1000 Base-TX (copper)
- 2 Port Gigabit Ethernet SFP (small-form factor-pluggable)

A modular configuration of the ports is not possible. Up to 128 VLANs can be configured and managed per port. One of these ports is also used as management port.

2.3 SME class (GSM 100)

The GSM 100 is designed for smaller companies and agencies as well as branches. The GSM 100 is recommended for the monitoring of up to 100 IP addresses. Controlling sensors in other security zones is not considered. However, the GSM 100 itself can be controlled as a slave-sensor by another master.

The appliance comes as 1U steel chassis. For easy integration into the data center an optional rack kit can be used. The appliance does not come with a display.

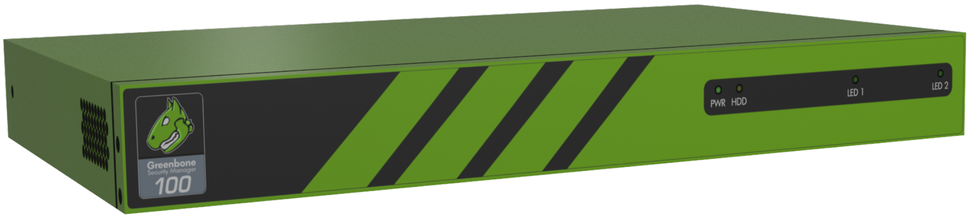


Fig. 2.3: The GSM 100 intended for smaller companies

For management of the appliance, in addition to a management Ethernet port, a serial port is available. The serial port is setup as a Cisco compatible console port.

To connect to the monitored systems the appliance comes with four 10/100/1000 Gigabit Ethernet Ports (RJ45) in total. These ports support up to 64 VLANs. One of these ports is also used as management port.

2.4 Sensors (GSM 25/25V)

The GSM 25 is designed as sensor for smaller companies and agencies as well as branches. The GSM 25 is recommended for up to 300 monitored IP addresses and requires the control of an additional appliance in master mode. The GSM of the midrange an enterprise class (GSM 500 and up) can be utilized as controllers for the GSM 25/25V.

The GSM 25 appliance comes as a 1U steel chassis. For easy integration into the data center an optional rack kit can be used. The appliance does not come with a display.

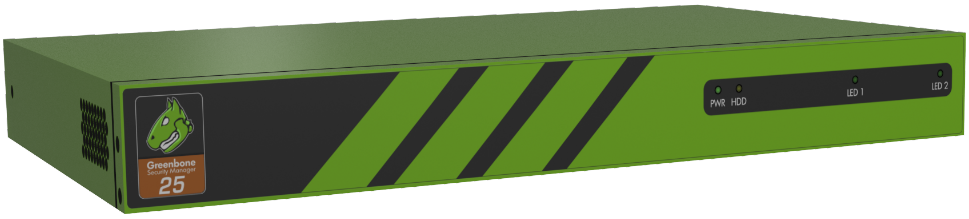


Fig. 2.4: The GSM 25 is a sensor and can only be operated with a GSM

For management of the appliance, in addition to a management Ethernet port, a serial port is available. The serial port is setup as a Cisco compatible console port.

To connect to the monitored systems the appliance comes with four 10/100/1000 Gigabit Ethernet Ports (RJ45) in total. These ports support up to 64 VLANs. One of these ports is also used as management port.

The GSM 25V is a virtual Appliance and provides a simple and cost effective option to monitor virtual infrastructures. In contrast to the GSM 25 the virtual version only comes with one virtual port for management, scanning and updates. However, the virtual port does support 64 VLANs as well.

2.5 GSM ONE

The GSM ONE is designed for specific requirements such as audit using a laptop or educational purposes. The GSM ONE is recommended for up to 300 monitored IP addresses and can neither control other sensors nor be controlled as a sensor by a larger appliance.

The GSM ONE only comes with one virtual port that is used for management, scan and updates. This port does not support the use of VLANs.

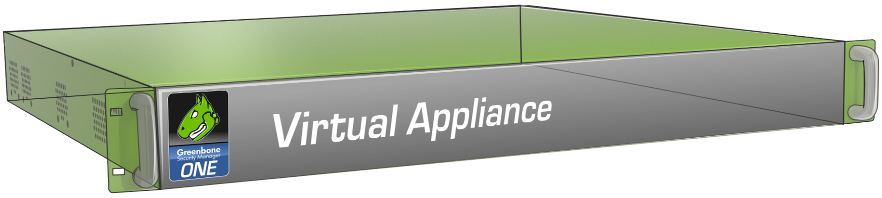


Fig. 2.5: The GSM ONE is a virtual instance.

The GSM ONE has all the functions of the larger systems except for the following:

- Master Mode: the GSM ONE cannot control other appliances as sensors.
- Slave Mode: the GSM ONE cannot be controlled as a slave sensor by other master-mode appliances.
- Alerts: the GSM ONE cannot send any alerts via SMTP, SNMP, syslog or HTTP.
- VLANs: the GSM ONE does not support VLANs on the virtual port.

CHAPTER 3

I want to ...

This chapter will guide you to different areas of the manual to complete simple single tasks.

I want to ...

- do my first scan. Please see section *Simple Scan* (page 53).
- do an authenticated scan. Please see section *Authenticated Scan* (page 67).
- upgrade the GSM. Please see section: *Upgrade* (page 39).
- configure new sensors. Please see section *Master and Slave Setup* (page 203).
- setup central authentication using LDAP. Please see section *Central User Management* (page 174).
- connect verinice to the GSM. Please see section *Verinice* (page 208).
- connect OMD/Check_MK/Nagios to the GSM. Please see section *Nagios* (page 213).
- use notes to manage the results. Please see section *Notes* (page 78).
- manage false positives using overrides. Please see section *Overrides and False Positives* (page 81).
- manage and use report formats. Please see section *Report Plugins* (page 88).

CHAPTER 4

Setup

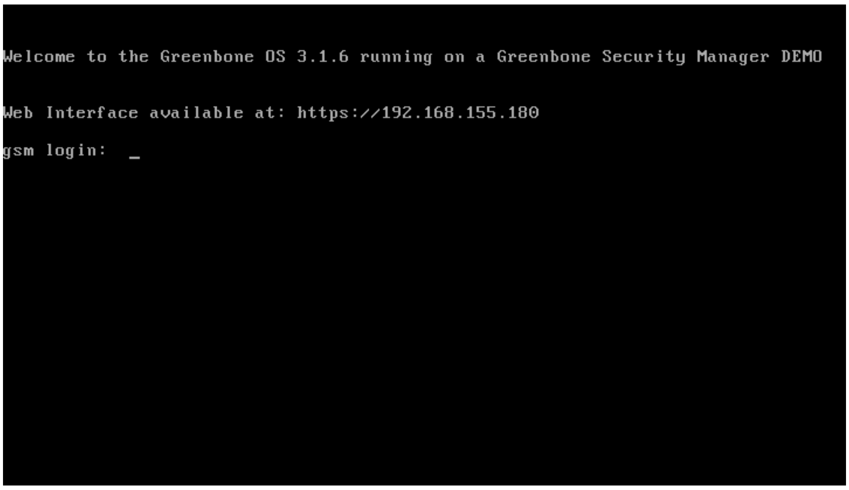
This chapter covers the first steps of the setup of your appliance. The steps in this chapter are shared among the various GSM appliance models. You will find appliance specific setup and trouble shooting in the chapter *Setup Guides* (page 233):

- *GSM ONE* (page 233)
- *GSM 25V* (page 237)
- *GSM 25* (page 239)
- *GSM 100* (page 241)
- *GSM 500/510/550* (page 243)
- *GSM 400/600/650* (page 245)
- *GSM 5300/6400* (page 247)

The setup is also explained in a video at http://docs.greenbone.net/Videos/gos-3.1/en/GSM-Setup-GOS-3.1-en-20150629.mp4.

4.1 Log in as admin

Once turned on the appliance will boot up. The boot process can be monitored via serial console. The boot process of the virtual appliance can be monitored in the hypervisor (VirtualBox or VMWare).



```
Welcome to the Greenbone OS 3.1.6 running on a Greenbone Security Manager DEMO

Web Interface available at: https://192.168.155.180

gsm login: _
```

Fig. 4.1: Boot screen of the appliance

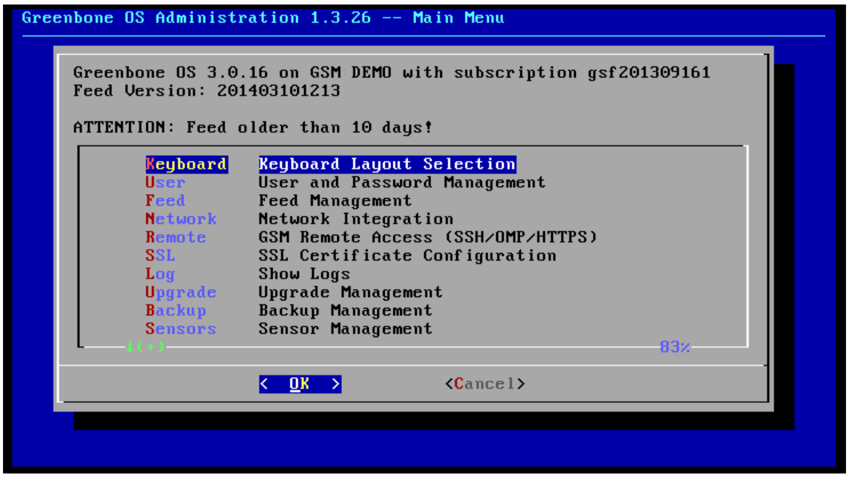
After the boot process is completed you can log into the system locally. The default login is user: `admin` with password: `admin`. At the login prompt (if not already configured) the GSM reminds you that no web user has been configured (see section *Web admin user* (page 13)).

4.2 Base configuration

The following sections cover the base configuration of the appliance. The base configuration should not be done via network connection rather than the serial console or the virtual console of the hypervisor.

4.2.1 Keyboard layout

First check the keyboard layout of the appliance and if necessary, set it appropriately to your required needs and locale. To configure the keyboard layout start the administrative menu from the command line after you logged into the appliance as admin (see section *Log in as admin* (page 9)). Entering the command `gos-admin-menu` will bring up the administrative menu (see figure *Greenbone OS Admin Menu* (page 10)).



```
Greenbone OS Administration 1.3.26 -- Main Menu

Greenbone OS 3.0.16 on GSM DEMO with subscription gsf201309161
Feed Version: 201403101213

ATTENTION: Feed older than 10 days!

        Keyboard      Keyboard Layout Selection
        User          User and Password Management
        Feed          Feed Management
        Network       Network Integration
        Remote        GSM Remote Access (SSH/OMP/HTTPS)
        SSL           SSL Certificate Configuration
        Log           Show Logs
        Upgrade       Upgrade Management
        Backup        Backup Management
        Sensors       Sensor Management
     ↓(+)                                                83%

              <  OK  >            <Cancel>
```

Fig. 4.2: Greenbone OS Admin Menu

In this menu select the first option *Keyboard* using the arrow keys and confirm with `Enter` [2]. Select the desired layout in the new dialog. After confirming the selection the option *Commit* must be selected and confirmed with `Enter`. The change will be confirmed with the message `The keyboard changes are submitted and become active within the next 5 minutes.` Alternative by selecting the *Rollback* option you can return to the original state.

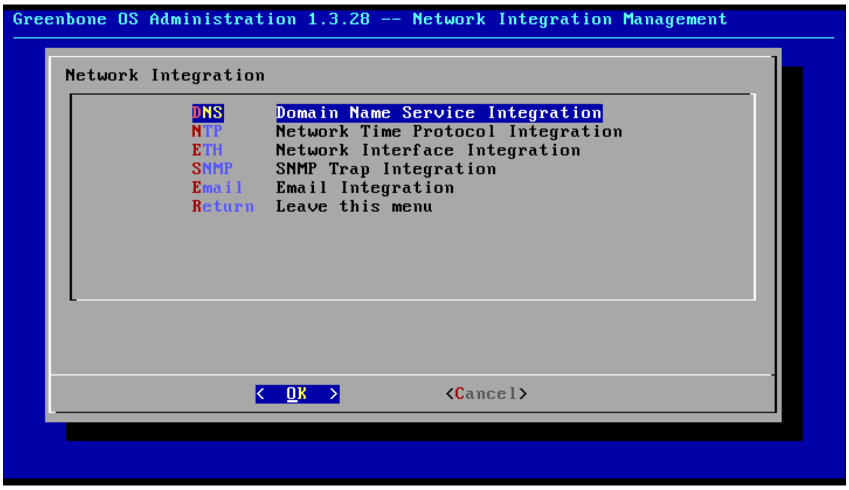
4.2.2 Network

The configuration of the network adapter `eth0` is required to perform the base configuration and to attach the appliance to the network. To configure the adapter start the admin menu from the command line after logging in as admin (see section *Log in as admin* (page 9)). Enter the command `gos-admin-menu` at the command line. A text based menu will be displayed which can be navigated by using the arrow keys and the `Enter`-key (see figure *Greenbone OS Admin Menu* (page 10)).

Under the menu option *Network* the network settings can be set. A new menu (see figure *Greenbone OS Admin: Network configuration* (page 11)) with the following options will be displayed:

[2] Alternatively the keyboard selection can be performed via the `keyboard_layout` variable.

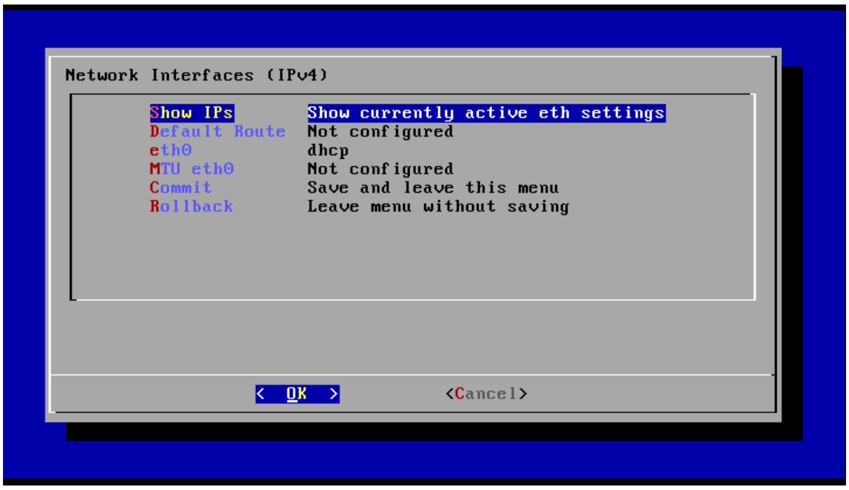
- *DNS*: Configuration of the DNS servers. These are not set automatically even when DHCP is used. The DHCP settings only have an effect on the IP-address and the default gateway!
- *NTP*: Configuration on the NTP servers. These are also not set automatically when DHCP is used. The DHCP settings only have an effect on the IP-address and the default gateway!
- *ETH*: Configuration of the Ethernet adapters.
- *SNMP*: Configuration of the SNMP-Trap-Settings. The community string for an external SNMP-Trap-Receiver for error messages can be configured.
- *Email*: Configuration of an external mail server for sending GSM emails (such as scan reports).



```
Greenbone OS Administration 1.3.28 -- Network Integration Management

Network Integration

          DNS       Domain Name Service Integration
          NTP       Network Time Protocol Integration
          ETH       Network Interface Integration
          SNMP      SNMP Trap Integration
          Email     Email Integration
          Return    Leave this menu

              <  OK  >              <Cancel>
```

Fig. 4.3: Greenbone OS Admin: Network configuration

To configure the IP address of the management port use option *ETH*. `eth0` is of special importance. This adapter is being used as the management port. The other possible adapters can be disregarded during the base configuration. The `eth0` adapter relates to the physical appliance adapter `LAN1`.



```
Network Interfaces (IPv4)

      Show IPs             Show currently active eth settings
      Default Route        Not configured
      eth0                 dhcp
      MTU eth0             Not configured
      Commit               Save and leave this menu
      Rollback             Leave menu without saving

              <  OK  >              <Cancel>
```

Fig. 4.4: Greenbone OS Admin: Ethernet configuration

By selecting option *eth0* the network adapter can be configured. There are three options:

`dhcp`: The IP address of the network adapter is configured via DHCP. This relates only to the IP address and the default gateway and not the DNS servers in use.

IP address: Entering an IP address with CIDR-netmask sets the IP address. The netmask must be entered as CIDR notation (/24, /25, and so on) and not as bitmask (255.255.255.0).

Blank: The network adapter is deactivated.

When setting a static IP address you must also set the default gateway in order to receive the GSM feeds and updates through the network. It can be set in the *Network-ETH-Default Route*. Entering the IP address of the default gateway is enough. All changes must be confirmed by *Commit*.

4.3 Management Adapter

If more than one network adapters are available you can chose through which network adapter the administrative interface of the GSM will be available. This is set by the GSM variable `ifadm`.

4.4 DNS configuration

In order to receive GSM feeds and updates you require a reachable DNS server for name resolution. In the factory default settings two Google name servers are configured:

- google-public-dns-a.google.com: 8.8.8.8
- google-public-dns-b.google.com: 8.8.4.4

The default DNS servers should be replace by your own DNS servers. This is especially necessary when the GSM cannot reach the Google DNS servers due to firewall rules. You can add up to three DNS servers. All changes must be confirmed by *Commit*.

If the DNS-servers can be reached is shown in the Readiness-Check (see section *Readiness* (page 15))

4.5 Password change

Also during the base configuration the password for the GSM administrator should be changed. The factory setting *admin/admin* is not suitable for a production environment.

The respective function is available in the Greenbone OS administration tool (GOS-Admin-menu) under *User*. The following user roles can be configured:

1. GSM-Admin: This is the administrator which can log into via command line (ie. via serial port).
2. Web-Admin: This is the administrator which can log into the web interface.

To change the administrator password select the option *GSM Admin*. You will be asked to enter the current (UNIX) password of the administrator. Afterwards you must enter the new password twice.

This change is effective immediately. A commit of the change is not required. A rollback is not possible either.

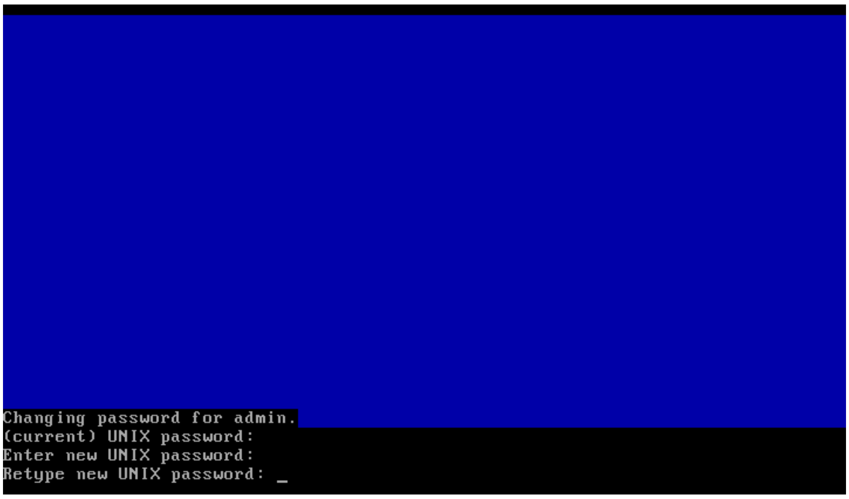
Note: Trivial passwords are being rejected. This includes the default password *admin*.

4.6 Setting up the web interface

Access to the Greenbone Security Manager primarily occurs through the web interface. To use it properly the following two steps are required:

1. Creation of a web administrator

   This user is used to log into the web interface with administrative rights. This user can use all of the features within the web interface.



```
Changing password for admin.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password: _
```

Fig. 4.5: Changing of the GSM administrator password

2. Creation of a SSL certificate

   The SSL certificate is required to for the encrypted communication via HTTPS and OMP with the GSM. A self-signed certificate can be created or issue a certificate from a certificate authority (see section *Certificate by an external certificate authority* (page 21))

4.6.1 Web admin user

To be able to use the GSM appliance a web administrator must be set up. This user is being referred to as Scan Administrator in some documentation and by some applications.

The set-up of a web admin is only possible through the GOS-Admin-Menu or from command line. Within the GOS-Admin-Menu switch to the *User* option and select *Add Web Admin*. Now enter the name and password of the scan administrator.

More than one user with administrative rights can be set up. Configuration of users from the GOS-Admin-Menu is not possible. It is only possible to display existing users or delete them if applicable.

To edit the existing users, or add users with less permissions, use the web-interface.

4.6.2 Certificate

The GSM appliance basically can use two types of certificates:

- Self-signed certificates
- Certificates issued by an external certificate authority

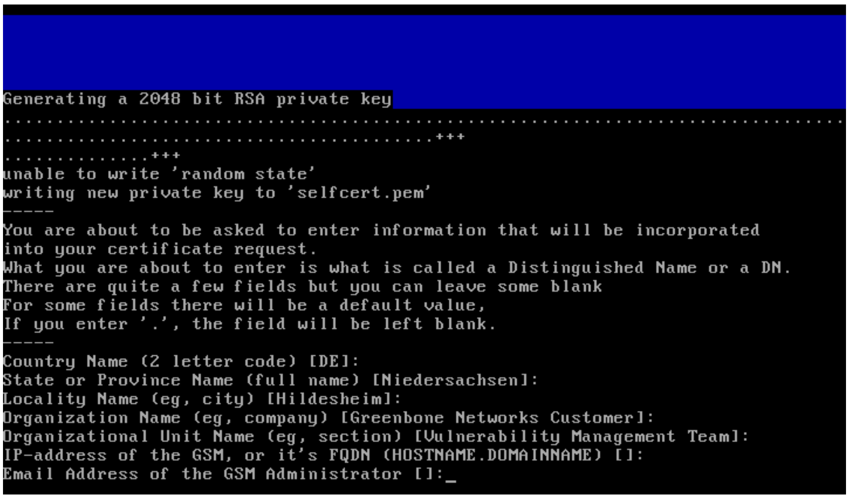
The use of self-signed certificates is the easiest way. It poses, however, the lowest security and more work for the user:

- The trust of a self-signed certificate can only be checked manually by the user through examination of the finger print of the certificate.
- Self-signed certificates cannot be revoked. Once they are accepted by the user in the browser they are stored permanently in the browser.

Usually, a GSM already carries a individual self-signed certificate. The installation of a certificate signed by an external certificate authority is described in section *Certificate by an external certificate authority* (page 21).

4.6.3 Self-signed certificate

To create a new self-signed certificate chose option *SSL* in the GOS-Admin-Menu and then select *Self-Signed*. You will be prompted with a couple of questions. The certificate is build based on the respective answers. The declaration of commonName is not critical as it is not part of the certificate.



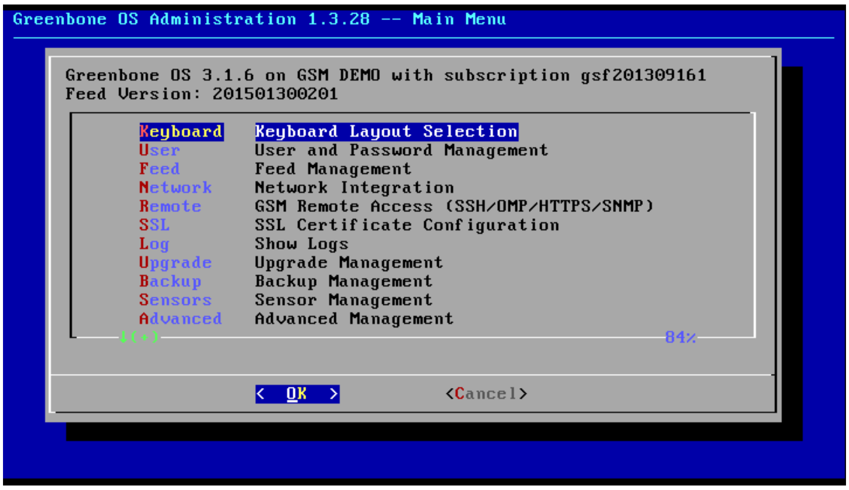
```
Generating a 2048 bit RSA private key
..............................................................................
........................................+++
.............+++
unable to write 'random state'
writing new private key to 'selfcert.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [DE]:
State or Province Name (full name) [Niedersachsen]:
Locality Name (eg, city) [Hildesheim]:
Organization Name (eg, company) [Greenbone Networks Customer]:
Organizational Unit Name (eg, section) [Vulnerability Management Team]:
IP-address of the GSM, or it's FQDN (HOSTNAME.DOMAINNAME) []:
Email Address of the GSM Administrator []:_
```

Fig. 4.6: The creation of a self-signed occurs via dialog.

4.7 Activation key

Every Greenbone Security Manager appliance requires an activation key. The GSM ONE already comes with a pre-installed activation key. If you are evaluating a GSM DEMO an activation key is already pre-installed.

If an activation key is installed can be verified by starting up the GOS-Admin-Menu. The title bar shows if an activation key exists. In the example in figure *Verifying of the activation key* (page 14) the subscription `gsf201309161` is stored.

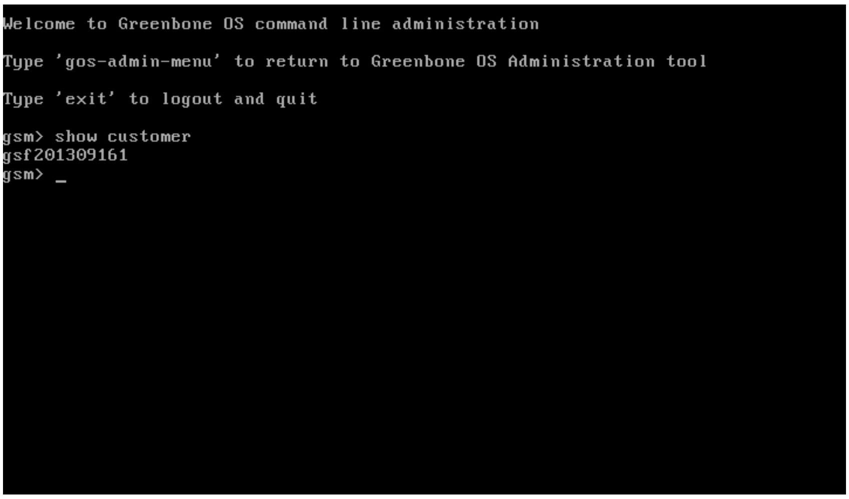


```
Greenbone OS Administration 1.3.28 -- Main Menu

  Greenbone OS 3.1.6 on GSM DEMO with subscription gsf201309161
  Feed Version: 201501300201

          Keyboard    Keyboard Layout Selection
          User        User and Password Management
          Feed        Feed Management
          Network     Network Integration
          Remote      GSM Remote Access (SSH/OMP/HTTPS/SNMP)
          SSL         SSL Certificate Configuration
          Log         Show Logs
          Upgrade     Upgrade Management
          Backup      Backup Management
          Sensors     Sensor Management
          Advanced    Advanced Management
      ↓(+)                                              84%

                    <  OK  >            <Cancel>
```

Fig. 4.7: Verifying of the activation key

Alternatively from the command line execute `show customer`.

If no activation key is stored you should have received it usually separately. After running



```
Welcome to Greenbone OS command line administration

Type 'gos-admin-menu' to return to Greenbone OS Administration tool

Type 'exit' to logout and quit

gsm> show customer
gsf201309161
gsm> _
```

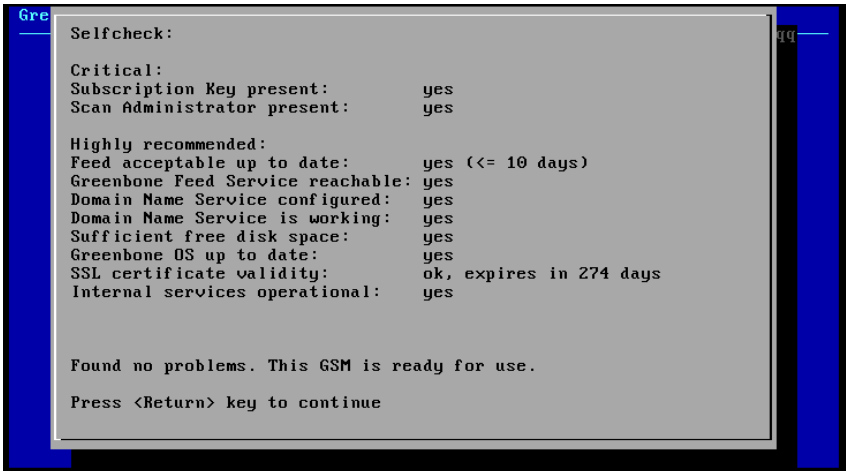
Fig. 4.8: Verifying of the activation key from the command line

`subscriptiondownload` you must enter they key via copy/paste. Ideally this is done via SSH connection with the appliance. Possibly SSH access needs to be activated (see *SSH Access* (page 30)).

4.8 Readiness

To verify the availability and correct configuration of the appliance the GOS-Admin-menu offers the possibility of a self-check. Start up the GOS-Admin-Menu and select the *SelfCheck* option.

The GSM now verifies if all pre-requisites exist to operate.



```
Selfcheck:

Critical:
Subscription Key present:         yes
Scan Administrator present:       yes

Highly recommended:
Feed acceptable up to date:       yes (<= 10 days)
Greenbone Feed Service reachable: yes
Domain Name Service configured:   yes
Domain Name Service is working:   yes
Sufficient free disk space:       yes
Greenbone OS up to date:          yes
SSL certificate validity:         ok, expires in 274 days
Internal services operational:    yes


Found no problems. This GSM is ready for use.

Press <Return> key to continue
```

Fig. 4.9: Verifying of the operational pre-requisites

The individual pre-requisites are:

- Subscription key
- Web-administrator (scan administrator)
- Up-to date feeds
- Connectivity to the Greenbone feed server
- Configuration of the DNS server
- Connectivity and functionality of the DNS server

- Available disk space of the hard disk
- Version of the operating system
- Validity of the SSL certificate
- Availability of the configured sensors (only Midrange and Enterprise models)
- Operational state of the internal services

Please reboot the appliance if you have changed any fundamental settings or after the first configuration.

CHAPTER 5

Command Line Interface

Besides the GOS-Admin Interface there is the possibility to use the command line interface of the GSM. Some settings like a Syslog server are currently only accessible via this interface. This chapter shows how to perform these changes.

5.1 Command line

The CLI can be accessed via serial console or SSH. However, SSH access is possibly deactivated and has to be enabled via the CLI or the GOS-Admin-Menu through the serial console (see section *SSH Access* (page 30)).

Access via SSH from UNIX/Linux can be done directly via command line:

```
$ ssh admin@<gsm>
```

Replace *gsm* with the IP address or DNS name of the GSM appliance. To verify the host-key, its checksum can be displayed via serial port prior. To do this in the GOS-Admin-Menu, change into the submenu *Remote* and select *SSH Fingerprint*.

While the GOS-Admin-Menu offers a simple menu controlled access for the configuration of the GSM appliance, the command line allows for a much more powerful access to the system. However, in the Command-Line-Interface (CLI) you have to enter the commands in the command line.

Access to the command line via serial port is described in the respective section of the setup guide. Login is preformed with user *admin* (see section *Log in as admin* (page 9)). The factory default password is *admin*. Alternatively SSH can be used to log in (see section *SSH Access* (page 30)).

To avoid typos the `Tab` key can be utilized. It automatically completes entered commands.

Try it: Enter `gos` on the GSM command line and press the `Tab` key. The characters change automatically to `gos-admin-menu`.

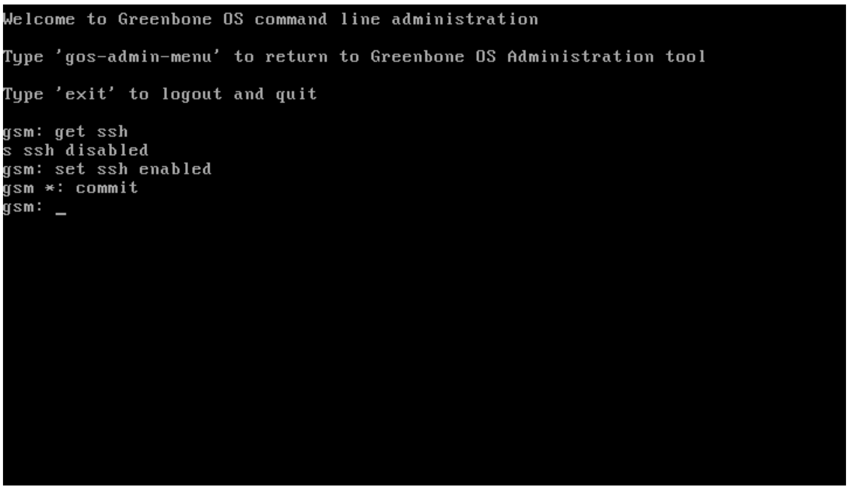
```
gsm: gos<tab>
```

5.2 Configuring settings

All changes in the settings that are being performed in the CLI are not activated immediately. As soon as a setting is changed in the CLI the prompt changes and indicates that there is an unsaved change. An asterisk at the prompt indicates a change that is not activated yet.

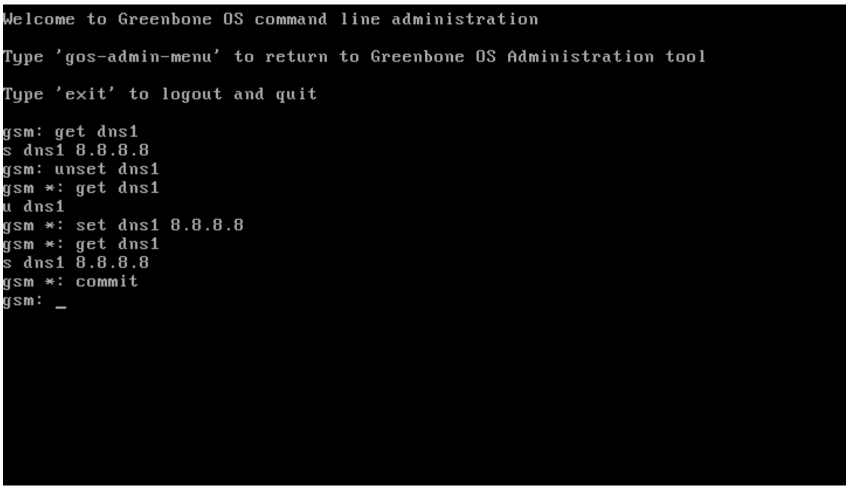
`commit` or `rollback` allows the decision between accepting or reverting of a change.

In addition the `get` command shows if a variable is currently get. This is indicated with an `s` at the beginning of the line. A `u` indicates that the variable currently is not set. Clearing of a variable is possible with the command `unset`. Variables can be configured with `set`.



```
Welcome to Greenbone OS command line administration

Type 'gos-admin-menu' to return to Greenbone OS Administration tool

Type 'exit' to logout and quit

gsm: get ssh
s ssh disabled
gsm: set ssh enabled
gsm *: commit
gsm: _
```

Fig. 5.1: Commit in the CLI



```
Welcome to Greenbone OS command line administration

Type 'gos-admin-menu' to return to Greenbone OS Administration tool

Type 'exit' to logout and quit

gsm: get dns1
s dns1 8.8.8.8
gsm: unset dns1
gsm *: get dns1
u dns1
gsm *: set dns1 8.8.8.8
gsm *: get dns1
s dns1 8.8.8.8
gsm *: commit
gsm: _
```

Fig. 5.2: set and unset in the CLI

5.3 Users and passwords

Like the GOS-Admin-Menu the CLI offers the possibility to change the password of the administrator and to create a web administrator (scan administrator respectively). It features many additional powerful commands.

5.3.1 Admin password change

The command passwd changes the password of the CLI administrator. This is the password required when logging in via serial console or via SSH. To change the password enter the command passwd.

```
gsm: passwd
Changing password for admin.
(current) UNIX password: old-password
Enter new UNIX password: new-password
Retype new UNIX password: new-password
passwd: password updated successfully
```

5.3.2 Creating a web administrator (scan administrator)

To create a web administrator the CLI use the command `addadmin`. This command expects the user name and password of the creating Administrator.

```
gsm: addadmin webadmin:kennwort
Creating user with temporary password.
User created with password 'b759489e-c0ba-40eb-90c1-c165b641700c'.
Setting password to desired value.
User was successfully created.
```

5.3.3 Superuser

On the GSM command line the command `shell` starts a UNIX command line as unprivileged user *admin*. Any UNIX command can be executed.

This superuser is not identical and as such independent from the Super Admin that can be created for the web interface (see section *Super Admin* (page 170)).

To obtain root rights (superuser) on the GSM appliance the command **`su`** needs to be entered. In the factory default settings this is only possible when connected locally via serial console. When logging in via SSH access to root is blocked. For day-to-day operation the *admin* user should be enough. The enabling of root access should only be done by exception and by consulting with Greenbone support.

To enable login as root the variable `superuser` must be set.

```
gsm: get superuser
s superuser disabled
gsm: set superuser enabled
gsm *: commit
gsm: get superuser
s superuser enabled
```

After this change a reboot of the GSM appliance is required!

When enabling superuser access a secure password for the *root* user should be set, too. The `superuserpassword` variable can be used to set the root password. By default the password is *disabled*.

```
gsm: get superuserpassword
s superuserpassword disabled

gsm: set superuserpassword kennwort
gsm *: commit
gsm:
```

5.4 Certificates

The GSM appliance basically can use two types of certificates:

- Self-signed certificates
- Certificates issued by an external certificate authority

The use of self-signed certificates is the easiest way. It poses, however, the lowest security and more work for the user:

- The trust of a self-signed certificate can only be checked manually by the user through examination of the finger print of the certificate.
- Self-signed certificates cannot be revoked. Once they are accepted by the user in the browser they are stored permanently in the browser. If an attacker gains access to the corresponding

private key a man-in-the –middle attack on the connection protected by the certificate can be launched.

The use of a certificate issued by a certificate authority has several advantages:

- All clients trusting the authority can verify the certificate directly and establish a security connection. No warning is displayed in the browser.
- The certificate can be revoked easily by the certificate authority. If the clients have the ability to check the certificate status they can decline a certificate that may still be within its validity period but has been revoked. As mechanisms the Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) can be used.
- Especially when multiple systems within an organization serve SSL protected information the use of an organizational CA simplifies the management drastically. All clients simply have to trust the organizational CA to accept all of the certificates issued by the CA.

All modern operating systems support the creation and management of their own certificate authority. Under Microsoft Windows Server the Active Directory Certificate Services support the administrator in the creation of a root CA[3]. For Linux systems various options are available. One option is described in the IPSec-Howto[4].

When creating and exchanging certificates it needs to be considered that the admin verifies how the systems are accessed later before creating the certificate. The IP address or the DNS name respectively, is stored when creating the certificate. Additionally after creating the certificate a reboot is required so that all services can use the new certificate. This needs to be taken into consideration when changing certificates.

5.4.1 Self-signed certificates

To support a quick setup the GSM supports self-signed certificates. However, by factory default of many variants such a certificate is not pre-installed and must be created by the administrator. The GSM ONE, however, already comes with a pre-installed certificate. Please refer to section *Self-signed certificate* (page 14).

Self-signed certificates can be easily created in the command line. Alternatively the admin can create a self-signed certificate via the GOS-Admin-Menu (*SSL-Self-Signed*). Before creating the certificate the admin needs to verify how the GSM is accessed later. Is it accessed via IP address (*https://192.168.15.5*) or a DNS name (*https://gsm.example.com*)?

The IP address or the DNS name respectively, must be entered when creating the certificate. It can only be changed at a later point by creating a new certificate.

After creating the certificate a reboot is required so all services can use the new certificate.

```
gsm: sslselfsign
Generating a 2048 bit RSA private key
.+++
.................................................................................+++
unable to write ’random    state ’
writing new private key to ’selfcert.pem ’
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value ,
If you enter ’.’, the field will be left blank.
-----
Country Name (2 letter code) [DE]: DE
State or Province Name (full name) [ Niedersachsen ]: Bundesland
```

[3] https://technet.microsoft.com/en-us/library/cc731183.aspx

[4] http://www.ipsec-howto.org/x600.html

```
Locality Name (eg , city) [Hildesheim ]: Stadt
Organization Name (eg , company) [Greenbone Networks Customer ]: Firma
Organizational Unit Name (eg , section) [ Vulnerability Management Team ]: Abteilung
IP -address of the GSM , or it 's FQDN (HOSTNAME.DOMAINNAME) []: 192.168.155.180
Email Address of the GSM Administrator []: mail@firma.de
```

To read and display the certificate use the `sslcatself`.

5.4.2 Certificate by an external certificate authority

To import a certificate by an external certificate authority switch to the command line. Exit the GSM-Admin-Menu to get to the GSM prompt: `gsm:`.

Note: Certificate data is transferred via copy/paste so it makes sense to perform this task via a SSH connection. SSH access possibly must be activated (see section *SSH Access* (page 30)).

Now disable the support of self-signed certificates by entering **`set selfsigssl disabled`**. This disables the variable `selfsigssl`. Confirm the change via `commit`.

The next step depends on whether you require a certificate signing request (CSR) which will be subsequently signed by a certificate authority or whether you already have a key and signed certificate you would like to use for this GSM.

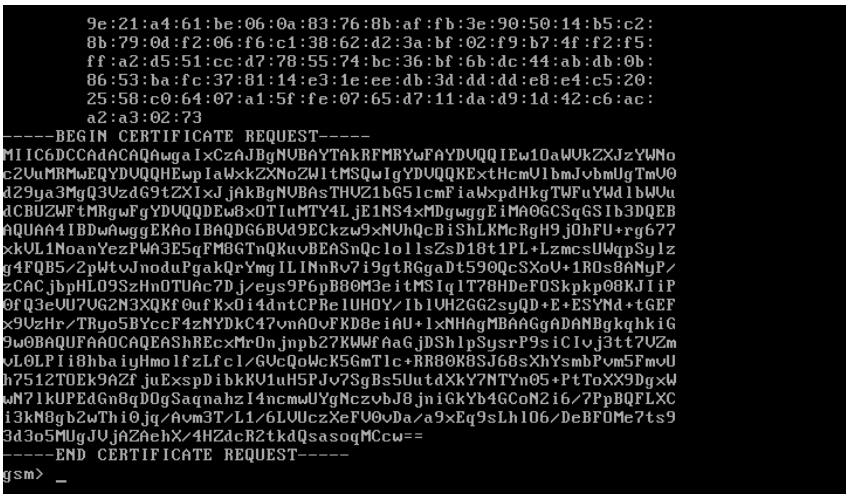
A new certificate signing request can be created with `sslreq`. Please enter your data correctly. Especially of importance is the common-name (CN). It must correspond to the browser entry later. If you access the GSM via IP address enter the IP address here. When using the server name enter the name here.

```
gsm: set selfsigssl disabled
gsm *: commit
gsm: sslreq
Generating a 2048 bit RSA private key
.....................................................................+++
..+++
unable to write 'random state '
writing new private key to 'tckey.pem '
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value ,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [DE]: DE
State or Province Name (full name) [ Niedersachsen ]: Bundesland
Locality Name (eg , city) [Hildesheim ]: Stadt
Organization Name (eg , company) [Greenbone Networks Customer ]: Firma
Organizational Unit Name (eg , section) [ Vulnerability Management Team ]: Abteilung
IP -address of the GSM , or it 's FQDN (HOSTNAME.DOMAINNAME) []: 192.168.155.180
Email Address of the GSM Administrator []: mail@firma.de
```

The certificate signing request will be displayed in the terminal directly after. The command `sslcatkey` can be used in case the entries need to be re-entered.

The certificate signing request displayed now needs to be sent to a certificate authority with the request for signature.

After the signed certificate is received back from the certificate authority it must be transferred back again to the GSM in PEM format (Base64). The command `ssldownload` is used to transfer the certificate with copy/paste and the entry is completed by entering `Ctrl-D` on an empty line.



```
        9e:21:a4:61:be:06:0a:83:76:8b:af:fb:3e:90:50:14:b5:c2:
        8b:79:0d:f2:06:f6:c1:38:62:d2:3a:bf:02:f9:b7:4f:f2:f5:
        ff:a2:d5:51:cc:d7:78:55:74:bc:36:bf:6b:dc:44:ab:db:0b:
        86:53:ba:fc:37:81:14:e3:1e:ee:db:3d:dd:dd:e8:e4:c5:20:
        25:58:c0:64:07:a1:5f:fe:07:65:d7:11:da:d9:1d:42:c6:ac:
        a2:a3:02:73
-----BEGIN CERTIFICATE REQUEST-----
MIIC6DCCAdACAQAwgaIxCzAJBgNVBAYTAkRFMRYwFAYDVQQIEw1OaWVkZXJzYWNo
c2VuMRMwEQYDVQQHEwpIaWxkZXNoZW1tMSQwIgYDVQQKExtHcmVlbmJvbmUgTmV0
d29ya3MgQ3VzdG9tZXIxJjAkBgNVBAsTHVZ1bG5lcmFiaWxpdHkgTWFuYWdlbWVu
dCBUZWFtMRgwFgYDVQQDEw8xOTIuMTY4LjE1NS4xMDgwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDG6BVd9ECkzw9xNVhQcBiShLKMcRgH9jOhFU+rg677
xkVL1NoanYezPWA3E5qFM8GTnQKuvBEASnQclollsZsD18t1PL+LzmcsUWqpSylz
g4FQB5/2pWtvJnoduPgakQrYmgILINnRv7i9gtRGgaDt59OQcSXoV+1ROs8ANyP/
zCACjbpHLO9SzHnOTUAc7Dj/eys9P6pB8OM3eitMSIqlT78HDeFOSkpkp08KJIiP
0fQ3eVU7VGZN3XQKf0ufKxOi4dntCPRelUHOY/IblVHZGGZsyQD+E+ESYNd+tGEF
x9VzHr/TRyo5BYccF4zNYDkC47vnAOvFKD8eiAU+lxNHAgMBAAGgADANBgkqhkiG
9w0BAQUFAAOCAQEAShREcxMrOnjnpb27KWWfAaGjDShlpSysrP9siCIvj3tt7VZm
vL0LPIi8hbaiyHmolfzLfcl/GVcQoWcK5GmTlc+RR8OK8SJ68sXhYsmbPvm5FmvU
h7512TOEk9AZfjuExspDibkKV1uH5PJv7SgBs5UutdXkY7NTYn05+PtToXX9DgxW
wN7lkUPEdGn8qDOgSaqnahzI4ncmwUYgNczvbJ8jniGkYb4GCoN2i6/7PpBQFLXC
i3kN8gb2wThi0jq/Avm3T/L1/6LVUczXeFV0vDa/a9xEq9sLhl06/DeBFOMe7ts9
3d3o5MUgJVjAZAehX/4HZdcR2tkdQsasoqMCcw==
-----END CERTIFICATE REQUEST-----
gsm> _
```

Fig. 5.3: The certificate signing request is in the paragraph between `BEGIN CERTIFICATE REQUEST` and `END CERTIFICATE REQUEST`

If you already have a key and a signed certificate you would like to use for this GSM, the command `certdownload` must be used instead to transfer the key and certificate to the GSM. The command expects the key and certificate in PEM format (Base64) and the entry is completed by entering `Ctrl-D` on an empty line.

Note: When importing the certificates there could be warnings. The Greenbone OS itself checks for validity of the certificate. A list of certificate authorities that is stored within the Greenbone OS is used for this. If the issuing authority is not known to the Greenbone OS a warning is displayed during the import of the certificate. They can be ignored as the GSM does not have to verify the validity of the certificate later anymore. It is important that the browsers that are used to connect to the GSM trust the certificate authority.

5.5 Appliance Management

This section covers the CLI commands for the management of the appliance. This includes reboot and shutdown, the setting up of the network configuration and the configuration of mail servers and logging servers.

5.5.1 Reboot and shutdown of the appliance

To shut down the appliance enter the `shutdown` command in the CLI. Depending on the model in use it can happen that the appliance does not shut itself off automatically. However, as soon as the shutdown is performed the appliance can be powered off.

```
gsm: shutdown
Are you sure you want to shutdown the system?
y/n?
y
```

Possible running scan processes can be restarted after reboot.

To reboot the appliance enter the `reboot` command in the CLI.

```
gsm: reboot
Are you sure you want to reboot the system?
y/n? y
```

A reboot or shutdown will be declined if essential administrative changes are running on the appliance such as an upgrade.

5.5.2 Network configuration

The network configuration in the CLI is preformed via the setting of variables. A `commit` is always required after. The following parameters can be set.

`hostname`

The name of the appliance appears in the scan reports and in the Syslog messages on a central logging server. It makes sense to choose a descriptive name. The following characters can be used:

- lower case and upper case letters a-z A-Z
- numbers 0-9
- dash -

```
gsm: get hostname
s hostname gsm
gsm: set hostname gsm-frankfurt
gsm *: commit
gsm: get hostname
s hostname gsm -frankfurt
```

`domainname`

The domain name like the hostname appears in the scan reports and the Syslog messages on a central logging server. Furthermore the configured domain will be used automatically with emails as the sending domain. Additionally the domain name is appended to not fully qualified hostname as such suffix.

The domain name can use the same characters as the hostname.

```
gsm: get domainname
s domainname greenbone.net
gsm: set domainname musterfirma.de
gsm *: commit
gsm: get domainname
s domainname musterfirma.de
```

DNS server

The GSM appliance supports up to three DNS servers. At least one DNS server is required. Additional servers will only be used at an outage of the first server.

Three variables are available:

- `dns1`
- `dns2`
- `dns3`

To delete a DNS server use the `unset` command.

```
gsm: get dns2
s dns2 8.8.4.4
gsm: unset dns2
gsm *: commit
```

```
gsm: get dns2
u dns2
```

IP Addresses

The GSM appliances come with up to 24 network adapters. Each of these adapters can be configured with an IPv4 and an IPv6 address. When using IPv4 addresses the keyword *dhcp* can be entered. An IP address will be assigned via DHCP. The variables are.

- `address_ethX_ipv4`
- `address_ethX_ipv6`

For X any number between 0 and 23 can be entered. This depends on the hardware in use.

```
gsm: get address_eth0_ipv4
s address_eth0_ipv4 dhcp
gsm: set address_eth0_ipv4 192.168.155.108/24
gsm *: commit
gsm: get address_eth0_ipv6
u address_eth0_ipv6
gsm: set address_eth0_ipv6 2001:db8:0:1::1/64
gsm *: commit
gsm:
```

After configuring the IP addresses a reboot is required so that the addresses are in actual use.

To delete an IP address use the command `unset`. When deleting and IPv4 address it only deactivates this address. The IPv6 address is still reachable.

Tip: Basically the IPv6-link-local-address is always active on every network adapter as well. If IPv6 should be disabled the `ipv6support` variable is used. It deactivates IPv6 support for the entire appliance. The link-local-addresses will disabled as well.

Default Gateway

To configure the default gateway use the variable `default_route_ipv4`. When using DHCP to assign IP addresses the default route will also be set via DHCP unless with the variable `default_route_ipv4` a router is set explicitly.

```
gsm: get default_route_ipv4
u default_route_ipv4
gsm: set default_route_ipv4 192.168.155.1
gsm *: commit
gsm:
```

Only the IPv4 default gateway can be configured via the CLI. Complex routing settings must be done via the expert network configuration (see section *Expert Network Configuration* (page 27)).

Network Time Protocol

To synchronize the appliance with central time servers the GSM appliance supports the NTP-Protocol. Two NTP servers the appliance will use for time synchronization can be configured. The appliance will chose the most suitable server. During an outage of a server the other server will be used automatically.

The variables `ntp_server1` and `ntp_server2` are available. Both variables require an IP address as an entry. The entry of a DNS name is not allowed.

```
gsm: set ntp_server1 192.53.103.104
gsm *: commit
```

To test the use and functionality of the protocol use the `ntpq` command.

```
gsm: ntpq
remote refid st t when poll reach delay offset jitter
==============================================================================
*ptbtime1.ptb.de .PTB. 1 u 245 1024 377 14.131 -0.432 0.495
+ptbtime2.ptb.de .PTB. 1 u 1012 1024 377 13.544 0.015 0.354
   LOCAL (0) .LOCL. 10 l 53h 64 0 0.000 0.000 0.000
```

You can determine the configured NTP server, polling, reachability, time delay, offset and jitter. The asterisk (*) in the first column indicates which server the appliance currently synchronizes with.

Mail Server

If you want to send reports after completion of a scan automatically via email the appliance needs to be configured with a mail server. The appliance itself does not come with a mail server.

Confirm that the mail server that the mail server accepts emails sent form the appliance. The appliance does not store emails in case of delivery failure. A second delivery attempt at a later time will not be attempted. On the mail server possible spam protection such as grey listing must be deactivated for the appliance. Authentication using a username and password is also not supported by the appliance. The authentication must be done IP based!

To configure the mail server use the `mailhub` variable.

```
gsm: get mailhub
s mailhub mail.greenbone.net
gsm: set mailhub mx.musterfirma.de
gsm *: commit
```

Central Logging Server

The GSM appliance allows for the configuration of a central logging server for the collection of the logs. The GSM appliance uses the Syslog protocol. Central collection of the logs allows for central analysis, management and monitoring of logs. Additionally the logs are also stored locally.

Two logging servers can be configured. Both will be used. As transport layer both UDP (default) and TCP can be used. TCP ensures delivery of the logs even when packet loss occurs. If packet loss occurs during a transmission vie UDP the log messages will be lost.

Two variables can be configured:

- `syslog_server1`
- `syslog_server2`

The format is as follows:

```
[udp|tcp://]ip[:port]
```

Example:

```
gsm: set syslog_server1 tcp://192.168.0.5:2000
gsm *: commit
```

If no port is specified the default port 514 will be used. If the protocol is not specified UDP will be used.

SNMP

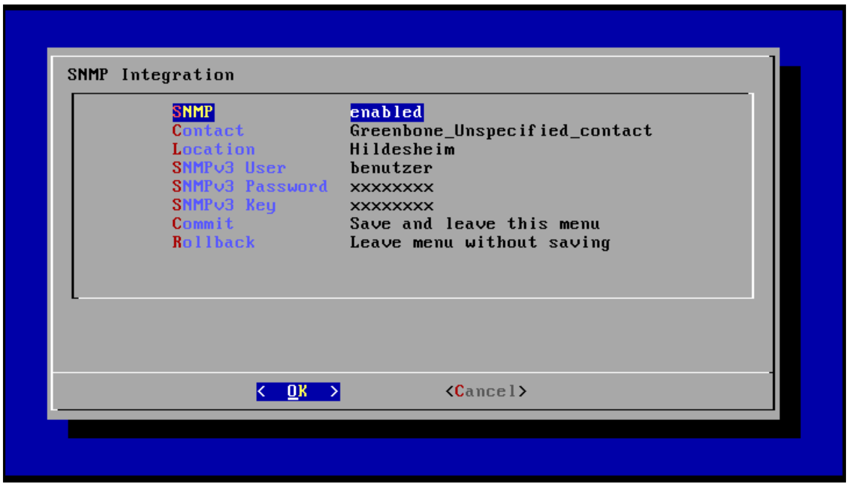
The GSM appliance supports SNMP. The SNMP support can both be used for sending of traps through alerts (see section Alerts (page 133)) as well as the monitoring of vital parameters of the appliance.

The supported parameters are specified in a Management Information Base (MIB) file. The current MIB is available from the Greenbone tech [doc] portal[5].

The GSM appliance supports SNMP version 3 for read access and SNMPv1 for traps.

The simplest way to configure the SNMPv3 is via the GOS-Admin-Menu under section *Remote* and *SNMP Configuration*. There is it also explained that the GSM will transfer the SNMPv3 user password with SHA-1 and use AES as encryption.

Sending traps is configured in the GOS-Admin-Menu under *Network* and *SNMP*.



SNMP Integration

```
SNMP             enabled
Contact          Greenbone_Unspecified_contact
Location         Hildesheim
SNMPv3 User      benutzer
SNMPv3 Password  xxxxxxxx
SNMPv3 Key       xxxxxxxx
Commit           Save and leave this menu
Rollback         Leave menu without saving
```

Fig. 5.4: SNMPv3 configuration

Alternatively the following variables allow for the configuration of the SNMP access:

- snmp
- snmp_key
- snmp_password
- snmp_user
- snmp_location
- snmp_contact
- snmp_trap
- snmp_trapcommunity
- snmp_trapreceiver

For sending alerts as SNMP traps use the following parameters.

```
gsm: set snmp_trap enabled
gsm *: set snmp_trapcommunity public
gsm *: commit
gsm: get snmp_trapreceiver
s snmp_trapreceiver 192.168.0.1
```

To configure read access for SNMP via CLI, use the respective variables snmp_key, snmp_password, and snmp_user.

[5] http://docs.greenbone.net/API/SNMP/snmp-gos-3.1.de.html

Afterwards test read access of the SNMP service under Linux/Unix with `snmpwalk`:

```
$ snmpwalk -v 3 -l authPriv -u user -a sha -A password -x aes -X key 192.168.155.180
iso .3.6.1.2.1.1.1.0 = STRING: "Greenbone Security Manager"
iso .3.6.1.2.1.1.5.0 = STRING: "gsm"
...
```

The following information may be gathered:

- Uptime
- Network interfaces
- Memory
- Harddisk
- Load
- CPU

5.5.3 Expert Network Configuration

The GOS-Admin-Menu and the variables currently only allow for simple network configuration. The configuration of VLANs or multiple static routes is not possible.

To make respective changes in the configuration an expert mode exists. It requires the input of all settings via script. The creation, editing and activation of this script is covered in this section.

Once the expert mode is used IP addresses can no longer be changed via the GOS-Admin-Menu or variables!

To use the expert mode it must be activated first. Execute the following command in the CLI (see section *Command line* (page 17)). Afterwards an reboot is required.

```
gsm: set netmode expert
gsm *: commit
gsm: reboot
Are you sure you want to reboot the system?
y/n? y
```

To revert back to normal mode at the later date use the command **`set netmode default`**.

Note that you need to execute `commit` to enable the **`set netmod`** command. After editing the file `expertnet.sh` a `reboot` is required to commit the settings.

Currently the command **`set netmode expert`** puts the appliance in a state whereby the user has to enter the entire configuration manually. To save them permanently the commands must be entered in within the `expertnet.sh` file and made executable (see below).

To edit the file change into shell mode. Enter the command `shell`:

```
gsm: shell
ATTENTION:
The shell command should only be used by expert users.
To leave the expert mode , type 'exit '.
admin@gsm :~$ ls -l expertnet.sh
-rwxr --r-- 1 admin admin 131 May 4 2012 expertnet.sh
admin@gsm :~$ _
```

Since you are in the Greenbone shell the files in the home directory can be displayed with the command **`ls`**. The file `expertnet.sh` is located here. The file can be customized with an editor. **`vi`**, **`vim`** or **`nano`** can be used for editing. If you are not familiar with the editor **`vi`** or **`vim`** please use **`nano`** as the editor. It displays help at the bottom of the window. The keyboard combinations listed all are executed with the Control key: `Ctrl-O` saves the file.

If the file has not been edited its content looks as follows:

```
# This script can be used to set custom network parameters like
# VLANS , source based routing and firewall restrictions on the GSM
```

Editing on a different system and copying the file afterwards with secure copy is not possible. The GSM does not support secure copying via SSH.

The first change in the file is to insert a first line so that the file looks as follows:

```
#!/bin/sh
# This script can be used to set custom network parameters like
# VLANS , source based routing and firewall restrictions on the GSM
```

The first line directs the Greenbone OS to interpret the file using the `/bin/sh` shell. Without this line the file will not be executed later. In order for the file to be able to be executed the file rights need to be configured directly. Enter the following command in the command line:

```
admin@gsm :~$ chmod 755 expertnet.sh
```

All network configurations require the command **`ip`**. The alternate commands **`ifconfig`**, **`route`** and **`vconfig`** should not be used. Their support can be limited in the future.

To avoid problems with the paths on the appliance the command **`ip`** should always be executed with the entire path: `/bin/ip`

Configuration of IP addresses

Configuration of IP addresses can easily be achieved with the **`ip`** command. The configuration is done in three steps:

1. Activation of the network adapter
2. Configuration of the first IP address
3. Configuration of optional additional IP addresses on the same network adapter

After activating the network adapter a delay of 10 second should be included to allow enough time for the network adapter to auto-negotiate. For consistency in the example this is also done for the loopback adapter.

```
/bin/ip link set lo up
sleep 10s
/bin/ip addr add 127.0.0.1/8 dev lo
/bin/ip link set eth0 up
sleep 10s
/bin/ip addr add 192.168.81.10/24 dev eth0
/bin/ip -f inet6 addr add 2607: f0d0 :2001::10/114 dev eth0
```

The first three lines activate and configure the loopback interface. This network adapter should not be forgotten in the script. Without the loopback interface the GSM will not work.

The command **`ip`** can activate multiple IP addresses on the same network adapter. **`ip addr add`** allows to add additional IP addresses. The do not replace the existing IP address. To delete an IP address **`ip addr del`** is required explicitly.

VLAN support

If switches are configured so that multiple VLANs with Tags (VLAN IDs [6] combined with an IEEE 802.1q [7] - trunk [8]) are transferred to the GSM they have to be disassembled on the GSM respectively. Sub-

[6] The 802.1q protocol with a 12bit VID field supports up to 4096 VLANs. Individual VLAN IDs are reserved however.

[7] Today the IEEE 802.1q protocol is the most common VLAN protocol. It has replaced proprietary protocols of individual manufacturers (such as Cisco's ISL).

[8] Multiple VLANs are marked with tags in a single connection transfer (single interconnect).

interfaces need to be configured on the physical network adapter. These sub-interfaces are also created with the **ip** command.

```
/bin/ip link set eth1 up
sleep 10
/bin/ip link add link eth1 name eth1 .91 type vlan id 91
/bin/ip link set eth1 .91 up
/bin/ip addr add 192.168.81.26/24 dev eth1 .91
```

The third command creates a sub-interface called *eth1.91* on network adapter *eth1*. The name can be freely chosen. For example, names like `ServerNet` or `MailDMZ` can be used. The flag `type vlan` instructs the command so that a tagged VLAN is disassembled respectively. `id 91` selects the actual VLAN ID.

The additional lines activate the sub-interface and configure the IP address. Multiple IPv4 and IPv6 addresses can be configured as well.

In case a VLAN trunk is a native VLAN the physical network adapter can be configured with an IP address. If no native VLAN was configured an IP address for the physical network adapter is not required. However, remember to activate the physical network adapter if this is the case!

Static Routing

Most networks only have one gateway. This gateway often is referred to as default gateway. Sometimes historically grown networks use different routers for different destinations. If these routers do not communicate data through dynamic routing protocols client systems often require static routes for those destinations. The expert configuration allows for configuration of unlimited static routes.

When using expert configuration the default gateway also needs to be configured in the `expertnet.sh` file. If IPv4 and IPv6 is used for each protocol a separate default gateway needs to be configured. If auto-configuration is used with IPv6 the default gateway can be omitted.

To set a route also use the **ip** command with the `route` argument:

```
/bin/ip route add default via 192.168.81.1
/bin/ip -f inet6 route add default via 2607: f0d0 :2001::1
```

The keyword `default` is dissolved into 0.0.0.0/0 or ::/0 respectively.

To add additional routes the following syntax can be used:

```
/bin/ip route add 192.168.0.0/24 via 192.168.81.5
```

A route for network 192.168.0.0/24 is set using the router 192.168.81.5.

5.6 Remote Access

To access the GSM appliance remotely basically four options are available

HTTPS This is the usual option for the creation, execution and analysis of the vulnerability scans. This option is activated by default and cannot be deactivated. Configuration is only possible for the timeout of the automatic logout when the HTTPS session is inactive.

SSH This option allows the possibility to access the command line, CLI and GOS-Admin-Menu of the GSM appliance. This access is deactivated by default and must be activated first. This can be done via serial console for example.

OMP (OpenVAS Management Protocol) The OpenVAS Management Protocol (OMP) allows for the communication with other Greenbone products (i.e. an additional GSM). It can also be used for the communication of in-house software with the appliance (see section OpenVAS Management Protocol (page 179)).

SNMP Read access of the GSM is possible via SNMPv3 (see section *SNMP* (page 26))

5.6.1 HTTPS Timeout

The timeout value can be set in the GOS-Admin-Menu (*Remote/HTTPS Timeout*) as well as the command line. In the CLI use the variable `webtimeout`:

```
gsm: get webtimeout
s webtimeout 15
gsm: set webtimeout 1
gsm *: commit
gsm: get webtimeout
s webtimeout 1
```

The value of the timeout can be between 1 and 1440 minutes (1 day).

5.6.2 SSH Access

SSH access can also be configured in the GOS-Admin-Menu (*Remote/SSH*) or the CLI. In the CLI use the variable `ssh`. It can have the value `enabled` or `disabled` Additionally the variable can be deleted:

```
gsm: get ssh
s ssh enabled
gsm: set ssh disabled
gsm *: commit
gsm: get ssh
s ssh disabled
```

In the GOS-Admin-Menu there is the additional possibility to display the fingerprint of the public key (host key)of the appliance.

5.6.3 OpenVAS Management Protocol (OMP)

The OpenVAS Management Protocol can be activated via the GOS-Admin-Menu (*Remote/OMP*) or the CLI. In the CLI use the variable `public_omp`:

```
gsm: get public_omp
s public_omp disabled
gsm: set public_omp enabled
gsm *: commit
gsm: get public_omp
s public_omp enabled
```

5.7 Upgrade and Feeds

On the command line system upgrades can be performed and feed synchronization can be configured. Commands and variables are available for these tasks.

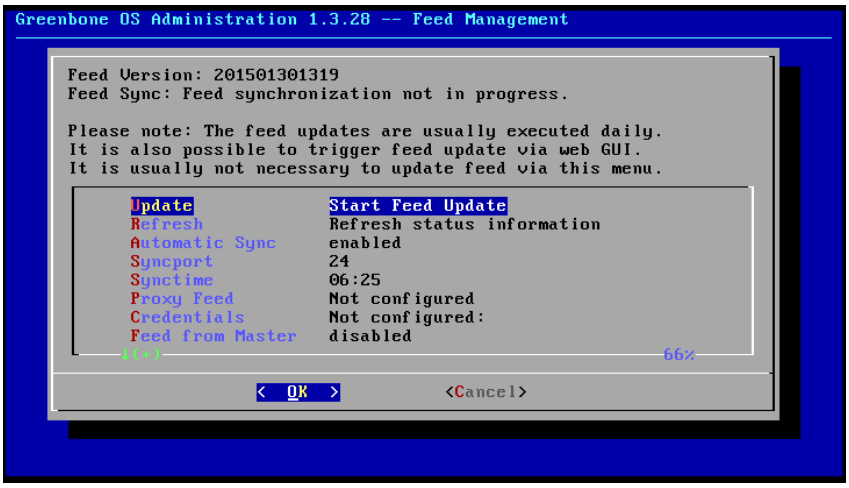
5.7.1 Upgrading the appliance

The command `systemupgrade` executes an upgrade. The status can be displayed with the command `systemupgradestatus` or `show schedule`.

Please take note of the *Upgrade* (page 39) section.

5.7.2 Feed Synchronization

To configure the synchronization feeds several variables are available: `feedsync`, `syncport` and `synctime`. Alternatively the configuration is possible via the GOS-Admin-Menu under *Feed*.



```
Greenbone OS Administration 1.3.28 -- Feed Management

Feed Version: 201501301319
Feed Sync: Feed synchronization not in progress.

Please note: The feed updates are usually executed daily.
It is also possible to trigger feed update via web GUI.
It is usually not necessary to update feed via this menu.

     Update                   Start Feed Update
     Refresh                  Refresh status information
     Automatic Sync           enabled
     Syncport                 24
     Synctime                 06:25
     Proxy Feed               Not configured
     Credentials              Not configured:
     Feed from Master         disabled
    ↓(+)                                                  66%

                  <  OK  >          <Cancel>
```

Fig. 5.5: Feed configuration

`feedsync` The automatic synchronization can be enabled or disabled.

`syncport` The port for the feed synchronization can be configured. By default the port is 24/tcp. Alternatively port 443/tcp can be used. Other ports cannot be used.

`synctime` The daily time for synchronization of the feed can be configured. This should be outside of regular business hours. The time of 10:00am-12:59am is the maintenance window of the feed and as such cannot be used. Times inside this window are rejected. These times are always UTC.

```
gsm: get synctime
s synctime 06:25
gsm: set synctime 11:30
syntax error in value
gsm: set synctime 13:30
gsm *: commit
gsm: get synctime
s synctime 13:30
```

Alternatively the feed can be started from the command line. Execute the command `feedstartsync`. The commands `feedsyncstatus` and `feedversion` can be used to monitor the current status.

5.7.3 Proxy configuration

Depending on the network environment, it might be necessary to use proxy for the feed and software updates. For both, the feed and software updates, the proxy is configured with this variable:

- `proxy_feed`

It expects a http proxy in the syntax of `http://proxy_ip[:port]`.

```
gsm: get proxy_feed
u proxy_feed
gsm: set proxy_feed http://1.2.3.4:3128
gsm *: commit
gsm: get proxy_feed
s proxy_feed http ://1.2.3.4:3128
```

Should the proxy require authentication it can be configured via the `proxy_credentials` variable. This variable expects a username and password separated by a colon:

```
gsm: get proxy_credentials
u proxy_credentials
gsm: set proxy_credentials user:password
gsm *: commit
gsm: get proxy_credentials
s proxy_credentials user:password
```

Note: In Windows environments, the credential is expressed as `domain\user:password`.

5.8 Database and Scanner Management

The *Advanced* options in the GOS-Admin-Menu provide access to the database management functions and the configuration of additional vulnerability scanners.

5.8.1 Database Management

The GSM uses the SQlite-Database for the internal storage of NVTs, scan results, configurations, etc. Using *Advanced/Database statistics* the admin can request database statistics. These statistics are logged and can be viewed using *Advanced/Database statistics log*.

Additionally the database may be optimized using the two commands VACUUM and ANALYZE. Both commands may take several hours to complete. The ANALYZE command gathers statistics about tables and indices. The collected information is stored in internal tables where the query optimizer can use it make better query planning choices. The VACUUM command rebuilds the whole database. This may speed up very fragmented databases.

The VACCUM command displays the results of the optimization after the successful termination:

```
Sep 28 14:56:22 gsm md main[18958]: Optimized: vacuum. Database file size reduced
by 85 MiB (55.9%)
```

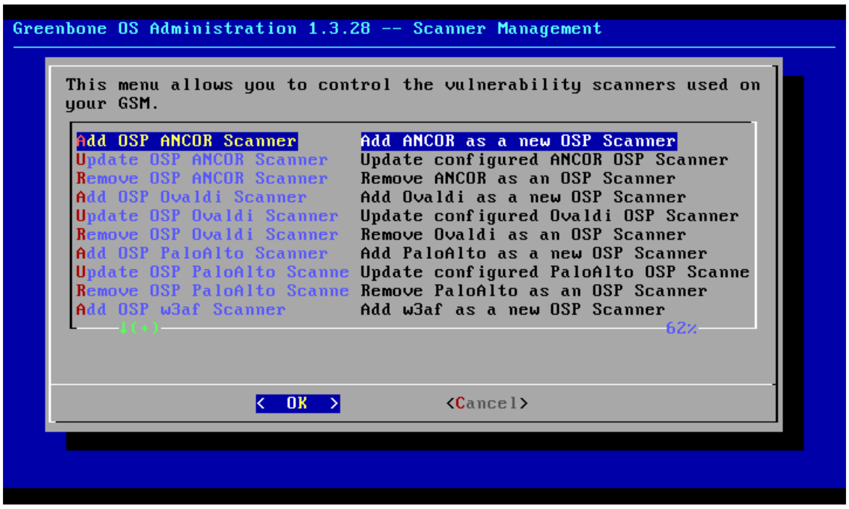
5.8.2 Additional Vulnerability Scanners

The *Advanced/Scanner Management* option currently (3.1.19) supports the listing of the currently supported vulnerability scanners. Future version will support the configuration of the following vulnerability Scanners:

- ANCOR
- Ovaldi
- Palo Alto
- w3af
- Fortinet

5.9 Monitoring and Debugging

Different tools for monitoring and debugging of the GSM appliance are available. The GSM-CLI offers access to some UNIX commands and files that can be useful when debugging.



Greenbone OS Administration 1.3.28 -- Scanner Management

This menu allows you to control the vulnerability scanners used on your GSM.

Add OSP ANCOR Scanner — Add ANCOR as a new OSP Scanner
Update OSP ANCOR Scanner — Update configured ANCOR OSP Scanner
Remove OSP ANCOR Scanner — Remove ANCOR as an OSP Scanner
Add OSP Ovaldi Scanner — Add Ovaldi as a new OSP Scanner
Update OSP Ovaldi Scanner — Update configured Ovaldi OSP Scanner
Remove OSP Ovaldi Scanner — Remove Ovaldi as an OSP Scanner
Add OSP PaloAlto Scanner — Add PaloAlto as a new OSP Scanner
Update OSP PaloAlto Scanne — Update configured PaloAlto OSP Scanne
Remove OSP PaloAlto Scanne — Remove PaloAlto as an OSP Scanner
Add OSP w3af Scanner — Add w3af as a new OSP Scanner
↓(+)
62%
< OK >
<Cancel>

Fig. 5.6: Configuration of additional OSP scanners

5.9.1 Monitoring and debugging of network functions

If the GSM is not reachable or cannot be reached by all client systems the network configuration must be checked. This is also the case should the GSM not be able to reach all of the target systems when performing a scan. Options of the GOS-Admin-Menu as well as some command line tools can be used to troubleshoot.

The following commands display the current network configuration:

getip This CLI specific command displays the current network configuration. Internally it uses the UNIX command **ip addr show**. By adding a specific network adapter the output can be limited:

```
gsm: getip dev eth0
2: eth0: <BROADCAST ,MULTICAST ,UP ,LOWER_UP > mtu 1500  qdisc pfifo_fast state
UP qlen 1000
link/ether 52:54:00:98:36:5 f brd ff:ff:ff:ff:ff:ff
inet 192.168.155.108/24 brd 192.168.155.255 scope global eth0
inet6 fe80 :: dead:beef /64 scope link
valid_lft forever preferred_lft forever
inet6 fe80 ::5054: ff:fe98 :365f/64 scope link
valid_lft forever preferred_lft forever
```

getroute This client specific command displays the current IPv4 routing table:

```
gsm: getroute
192.168.155.0/24 dev eth0 proto kernel scope link src&
192.168.155.108
default via 192.168.155.1 dev eth0
```

ntpq This command displays the configured NTP servers and their communication status:

```
gsm: ntpq
remote refid st t when poll reach delay offset jitter
===========================================================================
+ptbtime1.ptb.de .PTB. 1 u 602 1024 377 14.477 -0.319 9.907
*ptbtime2.ptb.de .PTB. 1 u 44 1024 177 13.580 0.143 0.150
LOCAL (0) .LOCL. 10 l 11d 64 0 0.000 0.000 0.000
```

The line with the asterisk (*) is the current preferred NTP server. The line with the plus (+) is the NTP backup server.

ip The command ip is also available in the CLI for the readable network properties. Different information can be displayed.

Display of the network adapters To display a list of network adapters use the command **`ip link show`**. This command displays the network adapters and MAC addresses:

```
gsm: ip link show
1: lo: <LOOPBACK ,UP ,LOWER_UP > mtu 16436 qdisc noqueue state UNKNOWN
         mode DEFAULT
         link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST ,MULTICAST ,UP ,LOWER_UP > mtu 1500 qdisc pfifo_fast
         state UP mode DEFAULT qlen 1000
         link/ether 52:54:00:98:36:5 f brd ff:ff:ff:ff:ff:ff
```

Display of the IP addresses To display the list of IP addresses use the command **`ip address show`**. The output reflects the command `getip`.

```
gsm: ip link show
1: lo: <LOOPBACK ,UP ,LOWER_UP > mtu 16436 qdisc noqueue state UNKNOWN
     link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
     inet 127.0.0.1/8 scope host lo
     inet6 ::1/128 scope host
     valid_lft forever preferred_lft forever
2: eth0: <BROADCAST ,MULTICAST ,UP ,LOWER_UP > mtu 1500 qdisc pfifo_fast
     state UP qlen 1000
     link/ether 52:54:00:98:36:5 f brd ff:ff:ff:ff:ff:ff
     inet 192.168.155.180/24 brd 192.168.155.255 scope global eth0
     inet6 fe80 ::5054: ff:fe98 :365f/64 scope link
     valid_lft forever preferred_lft forever
```

Display of the routes To display the routing table use the command **`ip route show`**. The output reflects the command `getroute`. To display the IPv6 routes enter **`ip -6 route show`**.

```
gsm: ip -6 route show
2001:4 dd0:ff00:d58 ::1 dev eth0 metric 0 cache
2001:4 dd0:ff00:d58 ::/64 dev eth0 proto kernel metric 256
fe80 ::/64 dev eth0 proto kernel metric 256
default via 2001:4 dd0:ff00:d58 ::1 dev eth0 metric 1024
```

ARP Cache and Neighbor Cache The ARP cache contains the MAC addresses of the systems the GSM communicated with directly in the LAN recently. The information can be useful when debugging if a system that is in the same LAN as the GSM is not reachable. The neighbor cache does the same for IPv6 addresses the ARP cache does for IPv4 addresses. On the GSM they are not differentiated and are displayed using the same command. By adding `-4` or `-6` the output can be limited:

```
gsm: ip neigh show
fe80 ::216:47 ff:fe7d :11c3 dev eth0 lladdr 00:16:47:7d:11: c3 router STALE
192.168.222.1 dev eth0 lladdr 00:16:47:7d:11: c3 REACHABLE
```

Monitoring of the IP stack With the command **`ip`** the changes in the routing table, the ARP cache and neighbor cache and the network adapters can be monitored. Use the command **`ip monitor all`**. Alternatively only individual sub systems (link, address, route, mroute, neigh., netconf) can be monitored. To cancel monitoring press `Ctrl-C`.

```
gsm: ip monitor all
[ROUTE]ff02 ::1 dev eth0 metric 0
               cache
[ROUTE ]2 a01 :198:5 a1 :201: d6ae :52ff:fe96:fe9b via 2001:4
               dd0:ff00:d58 ::1 dev eth0 metric 0
               cache
[ROUTE ]2001:4 dd0:ff00:d58 ::1 dev eth0 metric 0
               cache
[ROUTE]Deleted 2a01 :198:5 a1 :201: d6ae :52ff:fe96:fe9b via 2001:4
               dd0:ff00:d58::1 dev eth0 metric 0
               cache
```

```
[ROUTE ]2 a01 :198:5 a1 :255:5054: ff:fec3 :7266 via 2001:4
               dd0:ff00:d58 ::1 dev eth0 metric 0
               cache
[LINK ]4: eth1: <NO -CARRIER ,BROADCAST ,MULTICAST ,UP >
               link/ether
```

Link status of a network adapter To check the link status of a network adapter the GSM offers the command `ethtool`. This command expects additionally the name of the network adapter and can then display the current configuration and status. Interesting for debugging are the negotiated mode and speed and the current link status.

```
gsm: ethtool eth0
Settings for eth0:
              Supported ports: [ TP MII ]
              Supported link modes: 10 baseT/Half 10 baseT/Full
                                    100 baseT/Half 100 baseT/Full
              Supported pause frame use: No
              Supports auto - negotiation: Yes
              Advertised link modes: 10 baseT/Half 10 baseT/Full
                                     100 baseT/Half 100 baseT/Full
              Advertised pause frame use: Symmetric
              Advertised auto - negotiation: Yes
              Link partner advertised link modes: 10 baseT/Half 10 baseT/Full
                                    100 baseT/Half 100 baseT/Full
              Link partner advertised pause frame use: Symmetric
              Link partner advertised auto - negotiation: No
              Speed: 100Mb/s
              Duplex: Full
              Port: MII
              PHYAD: 32
              Transceiver : internal
              Auto - negotiation: on
              Supports Wake -on: pumbg
              Wake -on: d
              Current message level: 0x00000007 (7)
                                     drv probe link
              Link detected: yes
```

CHAPTER 6

Operation

This chapter covers the operation of the Greenbone Security Manager Appliance and looks at the most important aspects that could be encountered during operation. This chapter highlights first steps of user management. In addition, the upgrade of the appliance directly via the Internet as well as via Airgap mode are discussed. Finally, the backup and restoring of data are topics of this chapter.

6.1 User management

The Greenbone Security Manager user management allows for the definition and management of different users with different roles and permissions. When initializing the GSM appliance the first user (web/scan user respectively) is being set up via the GOS-Admin-Menu. This user allows the login and management of additional users.

The GSM user management supports a role based permission concept when accessing the web interface. Some roles are set up by default. However, other roles can be created and used by an administrator. The role defines which functions within the web interface a user is allowed to view and modify. The roles are not put in effect in the web interface rather than in the underlying OMP protocol and as such have an impact on all OMP clients. Read and modifying access can be assigned to roles separately.

Aside from roles the GSM user management supports groups as well. Groups allow the aggregation of users. This is mainly used for logical grouping. Aside from the management of permissions through roles, groups can also be assigned specific permissions.

Additionally, through user management every user can be assigned a range of IP addresses of which scanning is allowed or prohibited. The GSM appliance then denies a specific user the scanning of IP addresses other than the ones specified. Access to specific adapters of the GSM appliance can be allowed or denied.

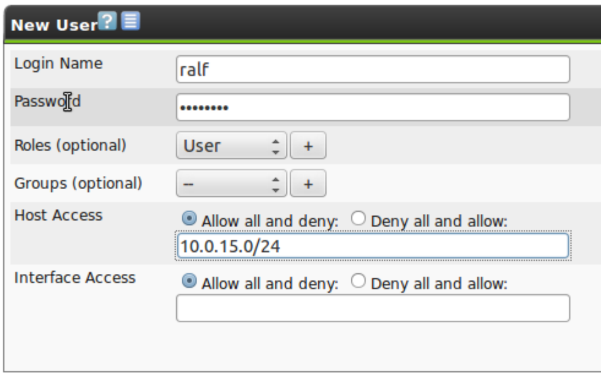
The Greenbone Security Manager offers its own user management for the management of the roles and specific permissions of the users. In order not to have to manage multiple passwords and to allow for password synchronization the Greenbone Security Manager allows for integration with a central LDAP server. It will only be used for the verification of the password of the user during log in. All other settings are performed in the user management of the GSM appliance.

The following sections cover the creation of individual users. The management of the permissions, groups and roles is covered in chapter User and Permission Management (page 165).

6.1.1 Creating and Managing Users

The dialog for creating and managing users can be accessed via the menu *Administration*. This menu is only visible to administrators since only they are allowed to create and manage users initially. Here the dialog for the creation of a new user can be started by clicking on the white star on blue background ★ or a user can be modified by clicking on the wrench icon.

When creating a user the following settings are possible:



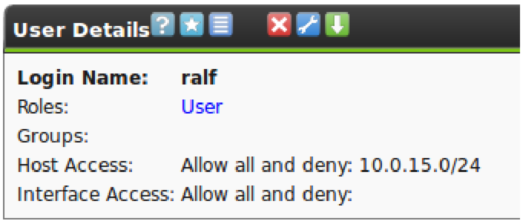
New User

Login Name	ralf
Password	••••••••
Roles (optional)	User +
Groups (optional)	– +
Host Access	● Allow all and deny: ○ Deny all and allow: 10.0.15.0/24
Interface Access	● Allow all and deny: ○ Deny all and allow:

Fig. 6.1: Creating a new user

- *Login Name*: This is the name the user logs in with. If an LDAP server is used for central password management, the user needs to be created with the identical name (rDN) as in the LDAP server. The name can be a maximum of 80 characters and can contain letters and numbers.
- *Password*: This is the password for the user. The password can be a maximum of 40 characters and can contain any type of character. Please note when using special characters that they are available on all keyboards and operating systems in use.
- *Roles (optional)*: Each user can have multiple roles. The roles define the permissions of a user when using the OMP protocol. Since the Greenbone Security Assistance utilized the OMP protocol the roles define directly the features in the web interface. While it is possible to add and configure additional roles, at the beginning some default roles are available. These roles are discussed in more detail in section *User Roles* (page 167).
- *Groups (optional)*: Each user can be a member of multiple groups. Permissions management can be performed via groups as well (see section *Permissions* (page 173)).
- *Host Access*: Here it can be defined which systems a specific user can analyze in a scan and which systems should not be considered in a scan. These restrictions can also be set up for administrators. They can, however, remove these restrictions again themselves. This is why this function is simply a self-protection for administrators. Normal users (*User*) and roles without access to the user management respectively cannot circumvent this restriction. Basically it can be chosen between a whitelist (deny all and allow) and a blacklist (allow all and deny). In the first case the scanning of all systems is denied in general and only explicitly listed systems are allowed to be scanned. In the latter case the scanning of all systems is allowed except the listed systems. System names as well as IPv4 and IPv6 addresses can be entered. Furthermore individual IP addresses as well as address ranges and network segments can be specified. The following listing shows some examples:
  - 192.168.15.5 (IPv4 address)
  - 192.168.15.5-192.168.15.27 (IPv4 range long form)
  - 192.168.15.5-27 (IPv4 range short form)
  - 192.168.15.128/25 (CIDR notation)
  - 2001:db8::1 (IPv6 address)
  - 2001:db8::1-2001:db8::15 (IPv6 range long form)
  - 2001:db8::1-15 (IPv6 range short form)
  - 2001:db8::/120 (CIDR notation)

  All options can be mixed and matched and entered as a comma separated list. The netmask in the CIDR notation is restricted however to a maximum of 20 for IPv4 and 116 for IPv6. In both cases the result is a maximum of 4096 IP addresses



Login Name: ralf
Roles: User
Groups:
Host Access: Allow all and deny: 10.0.15.0/24
Interface Access: Allow all and deny:

Fig. 6.2: Displaying a user

- *Interface Access*: Here it can be specified which network adapter a user can run a scan on. A comma separated list of network adapters can be entered and similar to the Host Access it can be chosen between a whitelist and blacklist methodology.

Tip: In general the whitelist methodology should be used and scans of systems denied except for the chosen systems. This is to ensure that users do not scan systems by accident or unknowingly that are outside of their responsibility, are located somewhere on the Internet or react critical to a scan.

After creating the user the user's properties are displayed. The display should be verified to ensure that the user does not have too many permissions assigned to him.

6.2 Upgrade

As part of your subscription Greenbone provides upgrades for the GSM appliance. The upgrades are provided regularly. Users can decide if an upgrade should be applied. The given numbers are based on the release data from the last 5 years as well as based on experience of the Support Team when helping customers to execute an upgrade. There are three different kinds of updates:

- Patch-Level upgrade (i.e. from version 3.0.16 to 3.0.17)
  - ca. 1 per month
  - some recommended, some critical (security)
  - 10 min per Master-GSM
- Release upgrade (i.e. from version 3.0.16 to 3.1.0)
  - ca. 1-2 per year
  - upon preference or due to End-of-Life
  - 2-6 hours (depending on whether it is necessary to adjust configuration due to functionality changes and whether users need to be trained about the changes)
- LTS Release upgrade
  - ca. 1 per 2 years
  - required due to End-of-Life
  - ca. 1-2 days (depending on whether it is necessary to adjust configuration due to functionality changes and whether users need to be trained about the changes)
- Generation Upgrade (i.e. from version 2.2.9 to 3.1.0)
  - ca. 1 per 2 years
  - upon preference or due to End-of-Life
  - ca. 1-2 days (depending on whether it is necessary to adjust configuration due to functionality changes and whether users need to be trained about the changes)

These upgrades are not being performed automatically. The user has to invoke the upgrades manually.

The upgrade steps are also explained in a video at http://docs.greenbone.net/Videos/gos/en/GSM-Upgrade-en-20150703.mp4.

If there are Master-GSMs as well as Slave-GSMs in the environment the following information is important:

- Sensors are being updated automatically by the master.
- Slaves must be updated manually. The masters should be updated first and then the slaves. It works this way under Airgap operation as well.
- Two GSMs with different patch levels can work together. However, this is not supported.
- Different release versions on master and slave are not possible!

6.2.1 Checking the Current Version

To check the current version all that is required is to connect to the GSM appliance. A log in is not even required. The welcome message of the GSM lists the current version in its banner. Alternatively executing the command `softwareversion` produces the same output.

```
Welcome to the Greenbone OS 3.1.6 running on a Greenbone Security Manager

Web Interface available at : https ://192.168.155.100

gsm login :
```

The log in screen of the web interface can also be checked. The version is displayed at the bottom right as well.

Alternatively after logging in using the command line via SSH for example, the version can be checked in the GOS-Admin-Menu. Under *Upgrade* it can be checked directly if an newer version is available. The current installed version can be displayed with *Current*. *Available* displays the latest version downloaded from the Greenbone feed server during last feed synchronisation. Under menu option *Sync* available versions on the Greenbone servers can be checked and a possible installation can be downloaded.

6.2.2 Performing Patch-Level upgrades

Before performing an upgrade it is recommended to inform yourself of the changes resulting from an upgrade. Greenbone is documenting all changes that are performed by an update on http://www.greenbone.net/technology/gos_release_history.html.

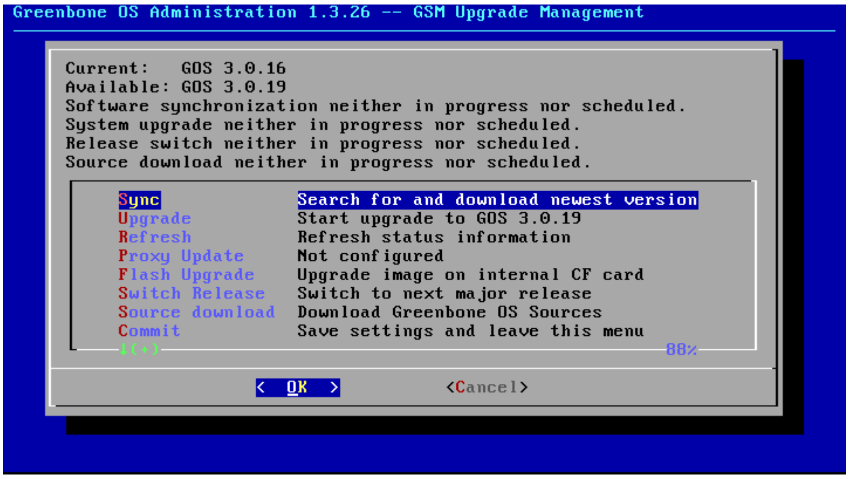
Before an upgrade a backup of the GSM should be performed also. The backup procedures are covered in section *Backup and Restore* (page 43). It makes sense to backup the entire appliance on the internal backup partition if supported by the appliance.

Furthermore the timing of the backup should be chosen so that no scans are actively run or started. Possibly individual system services will be restarted. This could cause scan results to get lost and limit the speed of an upgrade.

A Patch-Level upgrade usually completes after a couple of minutes. Afterwards a reboot is not required but recommended.

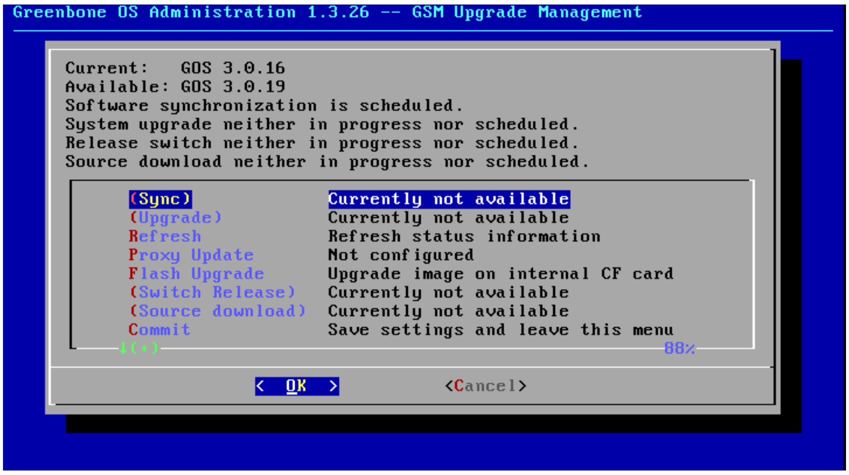
The upgrade is started via the GSM-Admin-Menu. Start the GSM-Admin-Menu and then select menu option *Upgrade*.

With the menu option *Sync* the availability of new versions can be checked anytime. It starts a new software synchronization in the background. The upgrade functions will then be disabled temporarily.



```
Greenbone OS Administration 1.3.26 -- GSM Upgrade Management

  Current:   GOS 3.0.16
  Available: GOS 3.0.19
  Software synchronization neither in progress nor scheduled.
  System upgrade neither in progress nor scheduled.
  Release switch neither in progress nor scheduled.
  Source download neither in progress nor scheduled.

      Sync              Search for and download newest version
      Upgrade           Start upgrade to GOS 3.0.19
      Refresh           Refresh status information
      Proxy Update      Not configured
      Flash Upgrade     Upgrade image on internal CF card
      Switch Release    Switch to next major release
      Source download   Download Greenbone OS Sources
      Commit            Save settings and leave this menu
      ↓(+)                                                 88%

                   <  OK  >          <Cancel>
```

Fig. 6.3: The GOS-Admin-Menu displays the availability of new versions



```
Greenbone OS Administration 1.3.26 -- GSM Upgrade Management

  Current:   GOS 3.0.16
  Available: GOS 3.0.19
  Software synchronization is scheduled.
  System upgrade neither in progress nor scheduled.
  Release switch neither in progress nor scheduled.
  Source download neither in progress nor scheduled.

       (Sync)              Currently not available
       (Upgrade)           Currently not available
       Refresh             Refresh status information
       Proxy Update        Not configured
       Flash Upgrade       Upgrade image on internal CF card
       (Switch Release)    Currently not available
       (Source download)   Currently not available
       Commit              Save settings and leave this menu
      ↓(+)                                                 88%

                   <  OK  >          <Cancel>
```

Fig. 6.4: The search for updates can be started at anytime.

By selecting the menu option *Refresh* the display can be updated. Synchronizing available upgrades can take several minutes as the required data for a possible upgrade is downloaded.

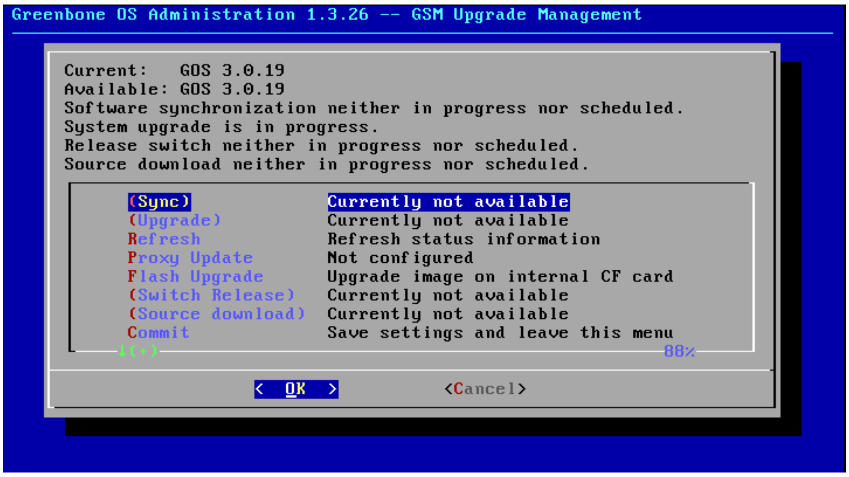
Afterwards the upgrade can be performed via the menu option *Upgrade*. Normally this process takes only a couple minutes, if a jump over multiple patch levels is performed it can take several minutes more. The upgrade is also requested in the background. For the actual start of the upgrade it can still take several minutes. All the while the GOS-Admin-Menu displays the message `System upgrade is scheduled`. As soon as the upgrade is performed the message in the GOS-Admin-Menu changes to `System-Upgrade is in process`. A couple of minutes later the message of the current version changes. The upgrade is not completed, however, until the message shows the system upgrade.

After completion a system reboot should be performed.

6.2.3 Release Upgrade

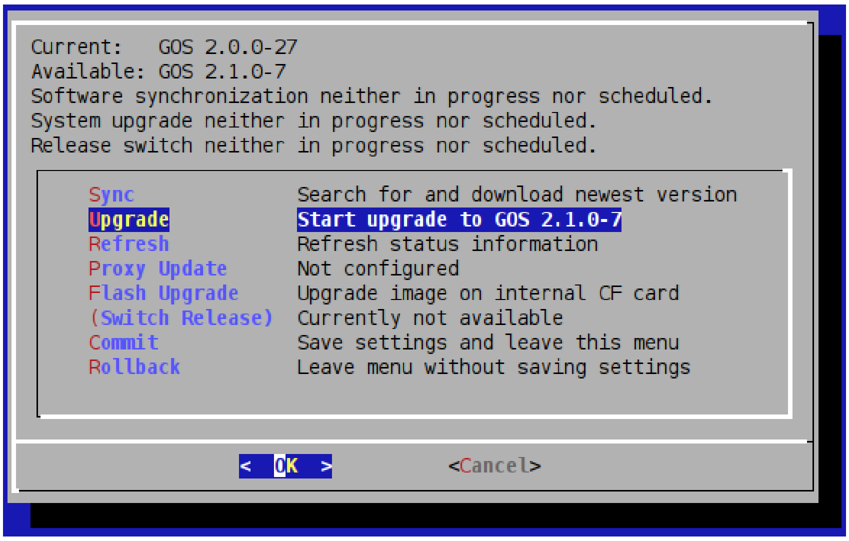
A release change is not being indicated in the GOS-Admin-Menu. A release change is announced by Greenbone via Newsletter and on the web site. Select the menu option *Switch Release* in the GOS-Admin-Menu. After a warning message the available release is displayed and is being downloaded from the Greenbone Feed servers. This process can take up to an hour depending on the Internet connection. Afterwards a new version for upgrade is being offered in the GOS-Admin-Menu and the release change is preformed along the same lines as a Patch-Level upgrade.

To complete a reboot is required. The upgrade can also take a couple of hours. While upgrading no



```
Greenbone OS Administration 1.3.26 -- GSM Upgrade Management

Current:   GOS 3.0.19
Available: GOS 3.0.19
Software synchronization neither in progress nor scheduled.
System upgrade is in progress.
Release switch neither in progress nor scheduled.
Source download neither in progress nor scheduled.

      (Sync)              Currently not available
      (Upgrade)           Currently not available
      Refresh             Refresh status information
      Proxy Update        Not configured
      Flash Upgrade       Upgrade image on internal CF card
      (Switch Release)    Currently not available
      (Source download)   Currently not available
      Commit              Save settings and leave this menu
    ↓(+)                                                  88%

                 <  OK  >             <Cancel>
```

Fig. 6.5: System upgrade in progress



```
Current:   GOS 2.0.0-27
Available: GOS 2.1.0-7
Software synchronization neither in progress nor scheduled.
System upgrade neither in progress nor scheduled.
Release switch neither in progress nor scheduled.

     Sync                Search for and download newest version
     Upgrade             Start upgrade to GOS 2.1.0-7
     Refresh             Refresh status information
     Proxy Update        Not configured
     Flash Upgrade       Upgrade image on internal CF card
     (Switch Release)    Currently not available
     Commit              Save settings and leave this menu
     Rollback            Leave menu without saving settings

                 <  OK  >             <Cancel>
```

Fig. 6.6: Release upgrade

scans should be running or being started.

6.2.4 Use of Proxies

In case the GSM appliance cannot access the Internet directly and requires the use of a proxy, it must be stored on the GSM appliance. Start the GOS-Admin-Menu and select the *Feed* option. Then select the option *Proxy Feed*. Here the proxy can be entered. Make sure that a valid HTTP-URL is used. Names as well as IP address can be used.

```
http://proxy.mycompany.com:3128
http://192.168.15.5:3128
```

To enter proxy credentials select *Credentials* in the same menu.

This proxy configuration will be used for the feed updates as well as for the software updates.

6.3 Backup and Restore

Regularly backing up the GSM appliance and the created data ensures fast restoration of operation of a new appliance, should the appliance have to be replaced by Greenbone after a failure of the appliance. Moreover, to be safe a backup of the system should be done prior to every update. Three different ways of backup are available:

- Backup of the entire system (SystemBackup)
- Snapshot of the entire system (SystemSnapshot)
- Backup of the created and changed data (user data). This includes all created scan configurations, users, overrides and so on.

A backup of the entire system prior to every update of the GSM appliance is recommended. This ensures the GSM appliance can be returned to its original state should the update fail.

A backup of the user data should be performed regularly. With this backup it is possible to restore your configurations after an exchange by Greenbone should the appliance have failed. Additionally this backup is recommended prior to every update.

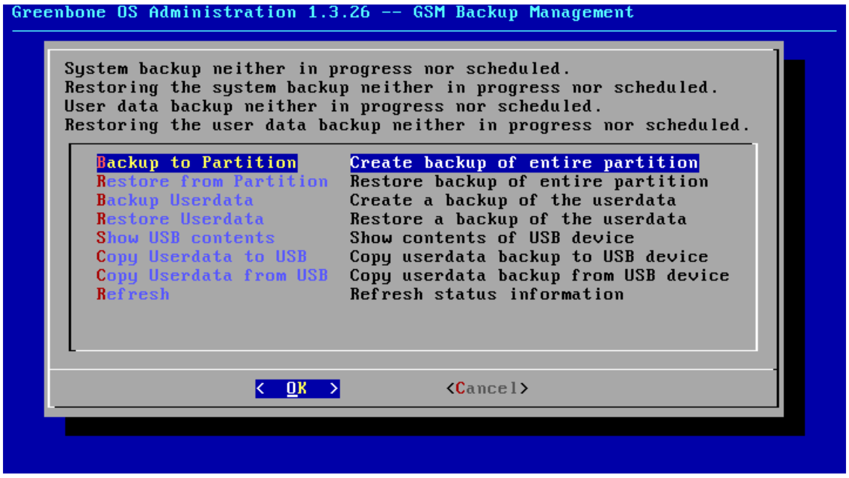
The following sections cover the individual steps.

6.3.1 Backup of the entire system

The way the backup of the entire system is performed depends on the appliance in use. The GSM ONE and GSM 25V are virtual appliances. It is very simple to utilize the backup functionalities of the hypervisor. The hypervisor, for example, supports the snapshot functionality that allows to backup and if needed the restoring, of the current state of the running system. The GSM 25 and GSM 100 do not support the backup of the entire system.

All other appliances (GSM 500 and up) come with a backup partition. The backup partition can store exactly one complete backup of the appliance. An incremental backup or the provisioning of other types is not supported.

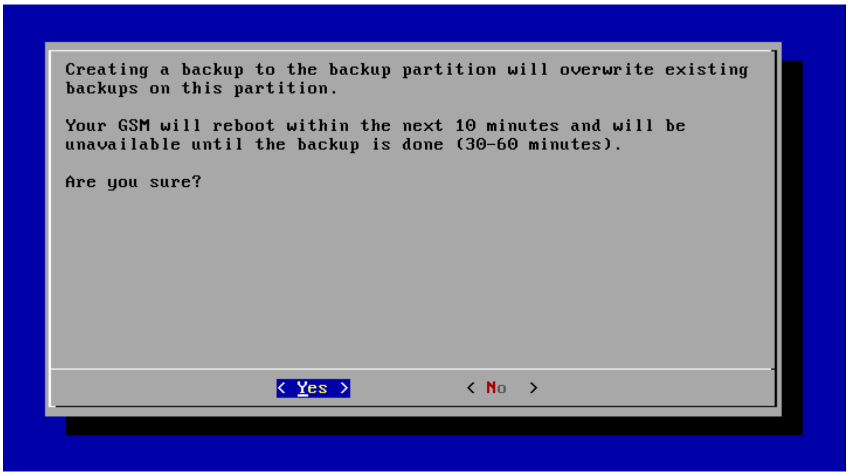
To perform a complete backup start the GOS-Admin-Menu from the console. Select the menu option *Backup*. The menu being displayed has the options *Create System Backup* and *Restore System Backup*.



```
Greenbone OS Administration 1.3.26 -- GSM Backup Management

System backup neither in progress nor scheduled.
Restoring the system backup neither in progress nor scheduled.
User data backup neither in progress nor scheduled.
Restoring the user data backup neither in progress nor scheduled.

  Backup to Partition     Create backup of entire partition
  Restore from Partition  Restore backup of entire partition
  Backup Userdata         Create a backup of the userdata
  Restore Userdata        Restore a backup of the userdata
  Show USB contents       Show contents of USB device
  Copy Userdata to USB    Copy userdata backup to USB device
  Copy Userdata from USB  Copy userdata backup from USB device
  Refresh                 Refresh status information

              <  OK  >            <Cancel>
```

Fig. 6.7: The complete backup is being started from the GOS-Admin-Menu

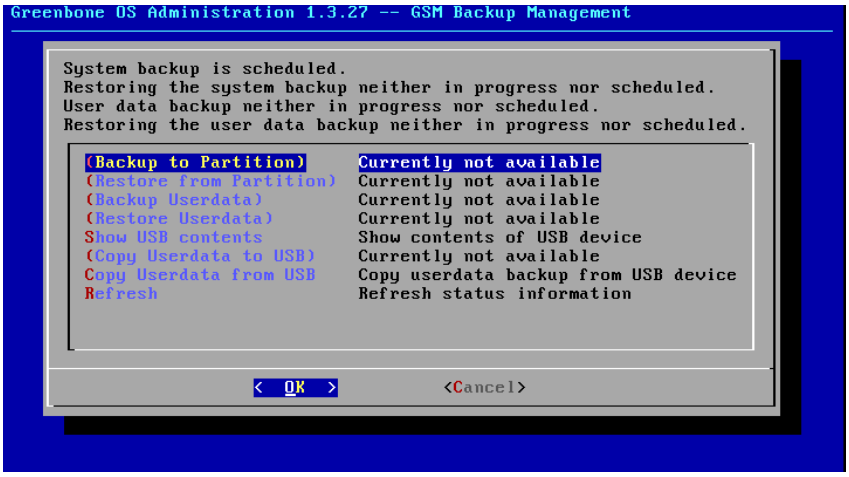
Create System Backup start the backup process. Afterwards the GSM appliance will reboot within the next 10 minutes (often immediately) and the system is backed up to the backup partition. This process can take about 30-60 minutes. A respective maintenance window is required and before starting the backup the process has to be confirmed.



```
Creating a backup to the backup partition will overwrite existing
backups on this partition.

Your GSM will reboot within the next 10 minutes and will be
unavailable until the backup is done (30-60 minutes).

Are you sure?
```

Fig. 6.8: The backup requires some time.

While the appliance waits to reboot other menu options in the backup menu are no longer available.



```
Greenbone OS Administration 1.3.27 -- GSM Backup Management

System backup is scheduled.
Restoring the system backup neither in progress nor scheduled.
User data backup neither in progress nor scheduled.
Restoring the user data backup neither in progress nor scheduled.

(Backup to Partition)      Currently not available
(Restore from Partition)   Currently not available
(Backup Userdata)          Currently not available
(Restore Userdata)         Currently not available
Show USB contents          Show contents of USB device
(Copy Userdata to USB)     Currently not available
Copy Userdata from USB     Copy userdata backup from USB device
Refresh                    Refresh status information
```

Fig. 6.9: After scheduling a backup, until reboot, other options are no longer available.

Restoring the GSM appliance from a complete backup is also performed with the assistance of the GOS-Admin-Menu. Select the menu option *Restore from Partition*. A maintenance window of 30-60 minutes is also required and the appliance performs a reboot. The process needs to be confirmed as it could cause data loss.

Note: If, since the last backup, there have been changes to user data, new scan configurations, tasks or overrides, they will be overridden. If in doubt user data should be backed up before restoring!

6.3.2 Snapshot of the System

The snapshot backup is another alternative to backing up the entire system. The system snapshot is only available with certain appliances (i.e. 5xx but not 6xx). Both the system backup as well as the system snapshot creates a complete backup of the partition. However both of the backups don't override each other. This means that practically two (backup) states can be stored (with one GSM 5xx). A GSM 600 only the system backup is possible for example.

To start the creation of a snapshot change to the command line and enter the command `systemsnapshot`. Afterwards the GSM appliance will boot and create the snapshot.

With the GSM 5xx a snapshot backup as well as a system backup can be created.

Restoring of a system snapshot backup is done via the Grub boot menu. Connect to the system vie serial port or a VGA monitor.

Perform a reboot. In the grub menu (before the GOS boot) a menu option *Snapshot Backup* should be displayed. Select this option. The system now boots into the snapshot.

6.3.3 Backup of User Data via USB-Stick

Backing up of user data is performed on all GSM appliances in the same way. The GSM appliance supports first of all the backup of the user data to the GSM appliance itself. The file created can be copied to a USB key or a separate SSH server afterwards. This way the data will still be available when the appliance fails. To save the data to an external USB key two steps are always required:

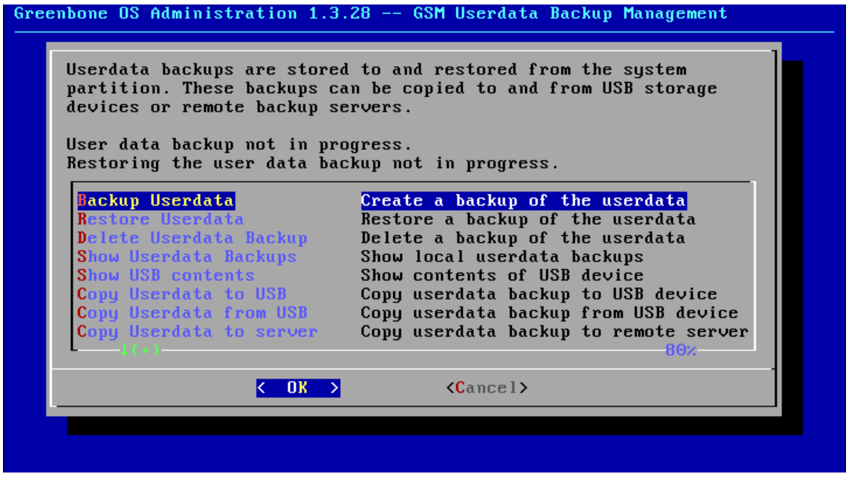
1. Backup of the user data
2. Copying of the backup to the USB key

The same process is performed backwards when restoring the user data. First the user data is copied from the USB key or the SSH server to the appliance. Then the data can be restored.

The following covers the individual steps.

These backup steps are also explained within the following video covering upgrades: http://docs.greenbone.net/Videos/gos/en/GSM-Upgrade-en-20150703.mp4.

First, log into the appliance, for example, via SSH. The start the GOS-Admin-Menu and select the menu option *Backup*. After selecting the option *Userdata Backup* the menu options concerning the Userdata Backup are available. While the actual Userdata backup is in progress the other options will be blocked until the backup is complete. Otherwise the system can be used as usual. A maintenance window is not required. A reboot is not performed either.



```
Greenbone OS Administration 1.3.28 -- GSM Userdata Backup Management

Userdata backups are stored to and restored from the system
partition. These backups can be copied to and from USB storage
devices or remote backup servers.

User data backup not in progress.
Restoring the user data backup not in progress.

Backup Userdata            Create a backup of the userdata
Restore Userdata           Restore a backup of the userdata
Delete Userdata Backup     Delete a backup of the userdata
Show Userdata Backups      Show local userdata backups
Show USB contents          Show contents of USB device
Copy Userdata to USB       Copy userdata backup to USB device
Copy Userdata from USB     Copy userdata backup from USB device
Copy Userdata to server    Copy userdata backup to remote server
    ↓(+)                                                     80%

                 <  OK  >             <Cancel>
```

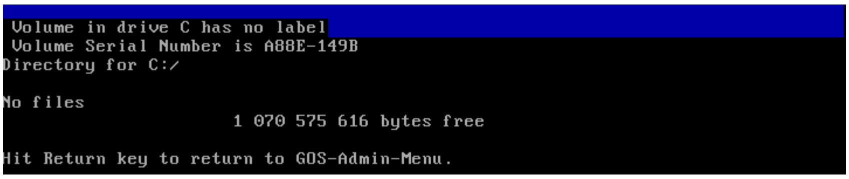
Fig. 6.10: The backup of user data can be done during regular operation.

Opposite to the complete backup multiple versions of user data backups can be stored on the appliance. They are being saved by name with the following pattern:

```
<gsf-number>-<date><time>.gsmb
201309161-201406180807.gsmb
```

On the appliance the backups are stored in the folder `/var/gsm/backups/userdata/`.

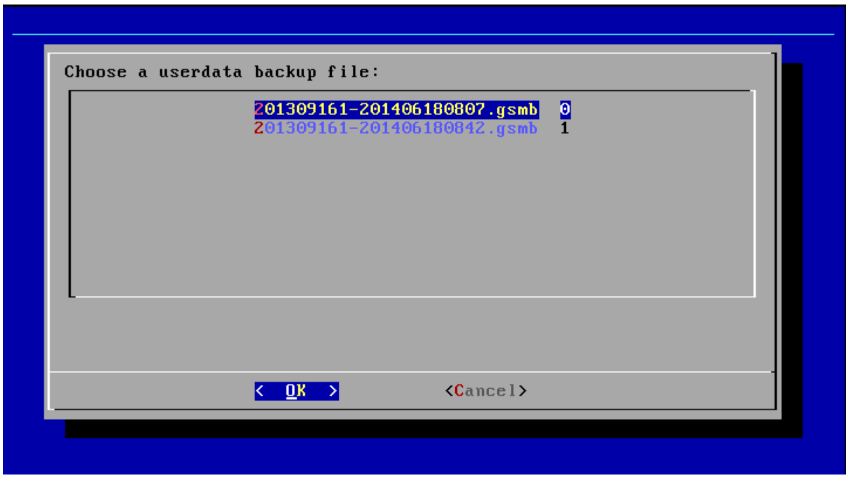
The stored user data can now be copied to a USB key or a SSH server. The USB key has to be partitioned and contain exactly one primary partition formatted in VFAT file system. This is the factory default with most USB keys. After inserting the USB key wait for a couple of seconds until the GSM appliance recognized the USB key. Then you can display the contents of the USB key with the menu option *Show USB contents*. The execution of the command can take a couple of seconds.



```
 Volume in drive C has no label
 Volume Serial Number is A88E-149B
Directory for C:/

No files
                      1 070 575 616 bytes free

Hit Return key to return to GOS-Admin-Menu.
```

Fig. 6.11: An empty USB key does not contain any files.

Now the user data can be copied to the USB key. Select the menu option *Copy Userdata to USB*. Afterwards you can select the backup to be copied.



```
Choose a userdata backup file:

                 201309161-201406180807.gsmb  0
                 201309161-201406180842.gsmb  1
```

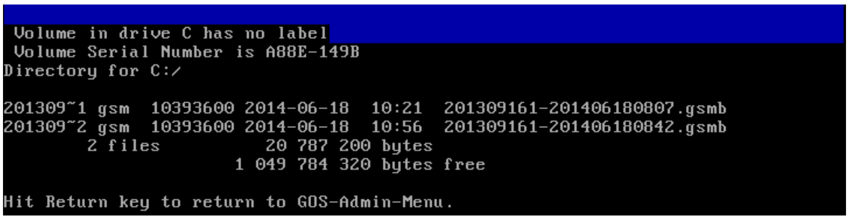
Fig. 6.12: Select the backup to be copied.

Should the file already exist in the USB key, you will be asked if the file should be renamed, overridden or skipped:

```
Long file name "201309161 -201406180807. gsmb " already exists .
a) utorenmae A) utorename - all r) rename R) ename - all o) verwrite O) verwrite - all
s) kip S) kip q) uit ( aArRoOsSq ):
```

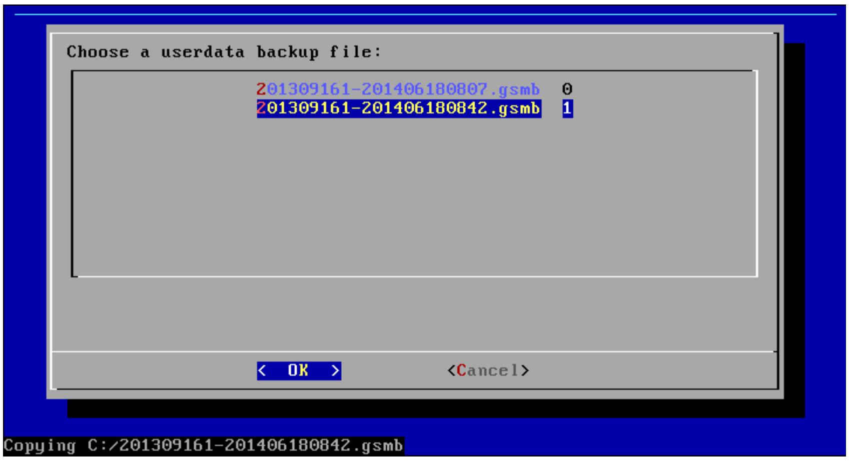
After the files are copied to the USB key the contents can be displayed again (see *After the copy process the data was transferred.* (page 46)). Afterwards the USB key can be unplugged.

To restore the data from the USB key, in the GOS-Admin-Menu select the menu option *Backup* followed by the option *Copy Userdata from USB*. After a couple of seconds the selection of available backups on the USB key is displayed. After confirming a version with OK, it will be copied to the GSM appliance.



```
 Volume in drive C has no label
 Volume Serial Number is A88E-149B
Directory for C:/

201309~1 gsm  10393600 2014-06-18  10:21  201309161-201406180807.gsmb
201309~2 gsm  10393600 2014-06-18  10:56  201309161-201406180842.gsmb
        2 files            20 787 200 bytes
                        1 049 784 320 bytes free

Hit Return key to return to GOS-Admin-Menu.
```

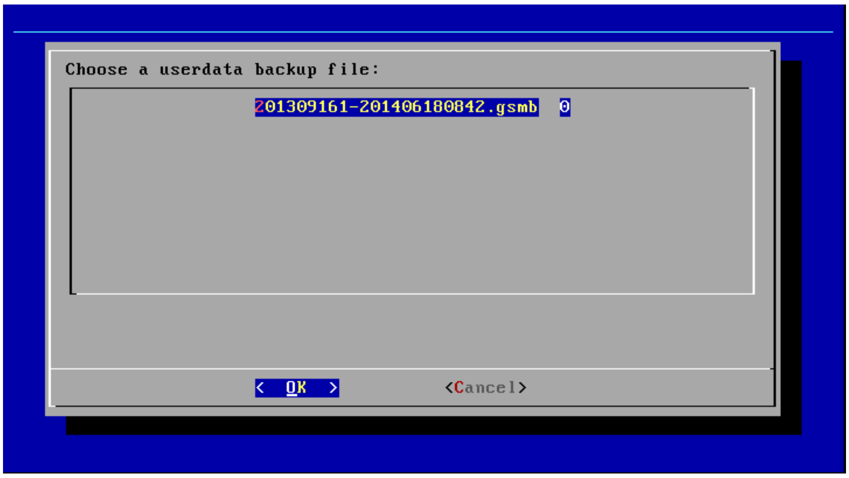
Fig. 6.13: After the copy process the data was transferred.



```
Choose a userdata backup file:

201309161-201406180807.gsmb   0
201309161-201406180842.gsmb   1

Copying C:/201309161-201406180842.gsmb
```

Fig. 6.14: User data backups can be copied from the USB key to the appliance.

Afterwards the user data can be restored with *Restore Userdata*. There will be a warning message that when restoring the old data the current data will be erased. This is possible if you want to backup it up. However, merging of user data backups is not possible.



```
Choose a userdata backup file:

201309161-201406180842.gsmb   0
```

Fig. 6.15: After copying the user data backups can be restored from USB key again.

Tip: If you want to backup only individual information such as a scan configuration you can export it via the web interface and import it onto another appliance as well!

6.3.4 Backup of User Data via SSH

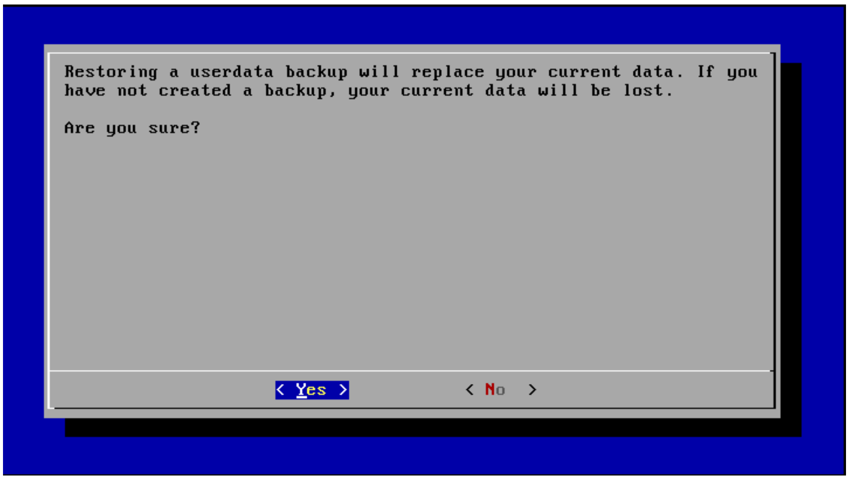
Backing up of user data can also be performed via SSH. This requires a SSH access on a remote system. To configure the remote backup via SSH you need to use gos-admin-menu and access menu *Backup* and there *Configure Server*. There you need configure the following items:

Backup server user This is the username to be used to log into the remote system and transfer the backup.

Backup server password This is the password for the specified user.

Backup server address This is the IP address of the backup server.

Backup server fingerprint Here you have to enter the MD5 checksum of the hostkey of the backup server. You can find out about the MD5 checksum by executing the following command on the



Restoring a userdata backup will replace your current data. If you have not created a backup, your current data will be lost.

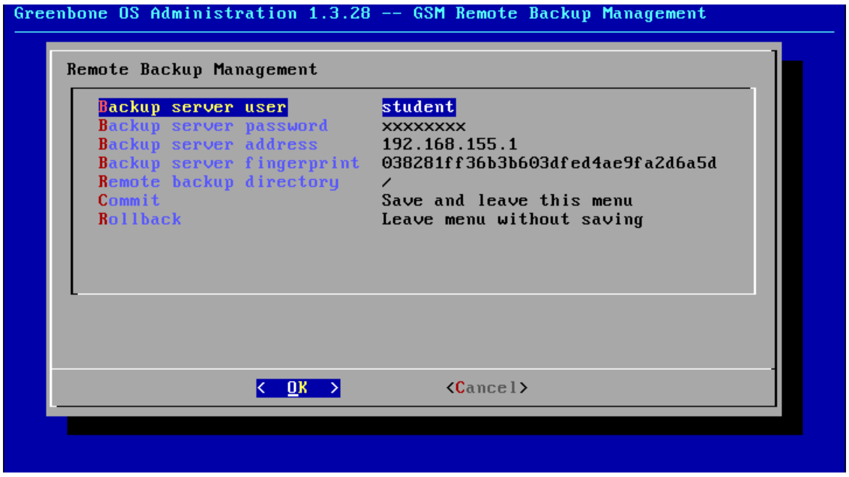
Are you sure?

Fig. 6.16: After copying the user data backups can be restored from USB key again.

backup server. This fingerprint must be entered without colons (see figure *The identify of the backup server is checked via the fingerprint of the hostkey.* (page 48)).

```
ssh-keygen -l -f /etc/ssh/ssh_host_rsa_key.pub
2048 03:82:81:ff:36:b3:b6:03:df:ed:4a:e9:fa:2d:6a:5d  root@station100 (RSA)
```

Remote backup directory Here you can change the directory where the backup will be stored on the remote system.



Greenbone OS Administration 1.3.28 -- GSM Remote Backup Management

Remote Backup Management

```
Backup server user          student
Backup server password      xxxxxxxx
Backup server address       192.168.155.1
Backup server fingerprint   038281ff36b3b603dfed4ae9fa2d6a5d
Remote backup directory     /
Commit                      Save and leave this menu
Rollback                    Leave menu without saving
```

Fig. 6.17: The identify of the backup server is checked via the fingerprint of the hostkey.

Now you have to create and copy a user data backup with *Userdata Backup*.

An automatic execution of the remote backup is not yet possible.

6.4 Airgap Update

The Airgap function allows a GSM appliance that is not directly connected to the Internet with updates of feeds and updates nonetheless. Two GSM appliances are required. One of these appliances is situated in a secured area and does not have any connectivity to the Internet. The second appliance has to be connected to the Internet.

For the Airgap function two options are available:

- Greenbone Airgap USB key

- Airgap FTP Server

Both options are covered in the following sections.

Note: Please refer to the GSM model overview (*GSM Overview* (page 3)), section GSM Networks to check which models support the Airgap feature.

6.4.1 Airgap via USB key

The feeds and updates are loaded from an appliance that is connected to the Internet and copied to a USB key. It then can be used to update the second appliance. The USB key can be checked for malware by a security gateway beforehand.

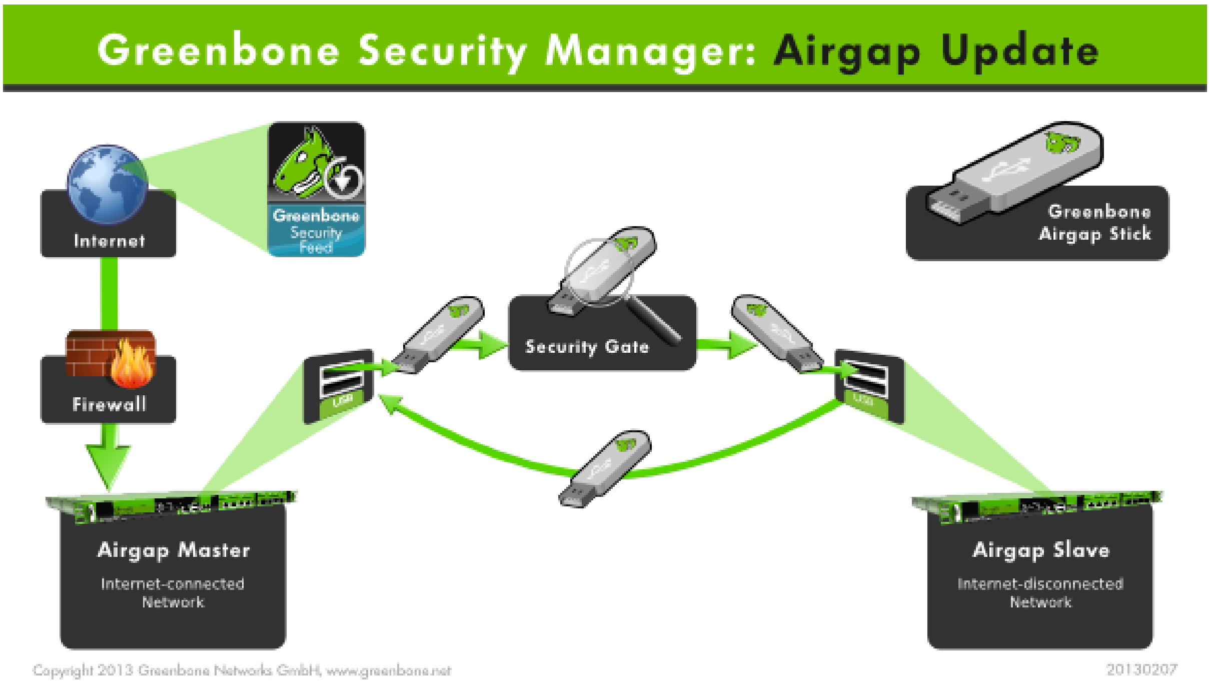

Greenbone Security Manager: Airgap Update
Internet
Greenbone Security Feed
Greenbone Airgap Stick
Security Gate
Firewall
USB
USB
Airgap Master
Internet-connected Network
Airgap Slave
Internet-disconnected Network
Copyright 2013 Greenbone Networks GmbH, www.greenbone.net
20130207

Fig. 6.18: The Airgap function allows for the update of GSM that are not connected to the Internet.

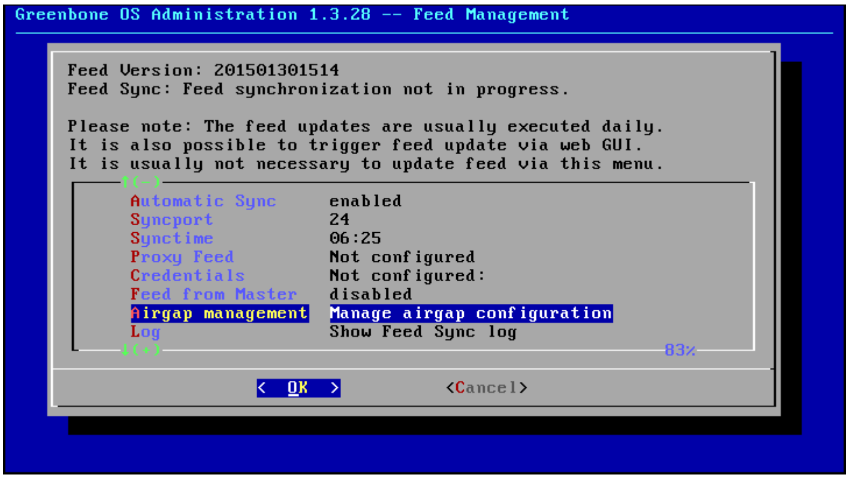
After setting up the of the Airgap functionality no log in onto the appliances is required. The communication happens entirely through the LCD display and can be performed by any personnel. Once a day they only have to remove the USB key from the Airgap master and insert it into the airgap slave. After a few minutes they will be asked on the display to remove the USB key from the Airgap slave again and insert it into the Airgap master.

The Airgap function can only be used with special USB keys provided by Greenbone. Contact Greenbone providing your customer number to request a respective USB key.

To use the Airgap function with the respective key, the GSM appliance needs to be configured respectively and the roles of Airgap master and Airgap slave need to be assigned. Start the GOS-Admin-Menu and change into the menu *Feed*. Scroll to the menu option *Airgap management* and select it.

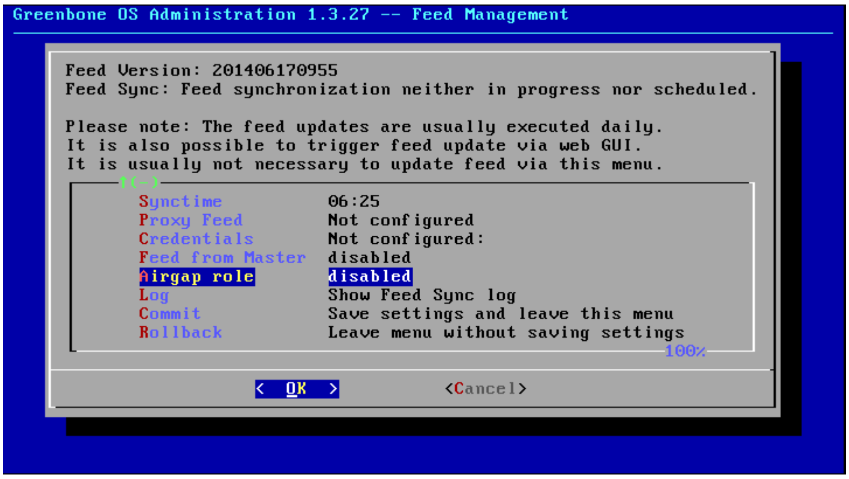
Enter in the role the respective role in the process either `master` or `slave`. The master is now building a special update package during every daily update and will save it to the USB key. The process can be followed on the display.

When the master is updating, it will display the messages **Airgap Master U1 updating USB...** and **Airgap Master U2 USB stick ready.** one after the other. A soon as the master displays **USB MEM PRESENT ok to remove!.** the USB key can be removed and transferred to the slave.



```
Greenbone OS Administration 1.3.28 -- Feed Management

 Feed Version: 201501301514
 Feed Sync: Feed synchronization not in progress.

 Please note: The feed updates are usually executed daily.
 It is also possible to trigger feed update via web GUI.
 It is usually not necessary to update feed via this menu.
        ↑(-)
        Automatic Sync       enabled
        Syncport             24
        Synctime             06:25
        Proxy Feed           Not configured
        Credentials          Not configured:
        Feed from Master     disabled
        Airgap management    Manage airgap configuration
        Log                  Show Feed Sync log
        ↓(+)                                              83%

              <  OK  >            <Cancel>
```

Fig. 6.19: The Airgap management can be found in its own submenu.



```
Greenbone OS Administration 1.3.27 -- Feed Management

 Feed Version: 201406170955
 Feed Sync: Feed synchronization neither in progress nor scheduled.

 Please note: The feed updates are usually executed daily.
 It is also possible to trigger feed update via web GUI.
 It is usually not necessary to update feed via this menu.
        ↑(-)
        Synctime             06:25
        Proxy Feed           Not configured
        Credentials          Not configured:
        Feed from Master     disabled
        Airgap role          disabled
        Log                  Show Feed Sync log
        Commit               Save settings and leave this menu
        Rollback             Leave menu without saving settings
                                                          100%

              <  OK  >            <Cancel>
```

Fig. 6.20: The Airgap role identified the function of the GSM appliance in the Airgap process.

The slave recognizes the USB key automatically and loads the update from the USB key. The display displays the message **Airgap Slave DL1 updating from USB.** and **Airgap Slave S0 ……..**. As soon as the message **USB MEM PRESENT ok to remove!.** is being displayed also, the USB key can be removed and inserted back into the master.

6.4.2 Airgap via FTP

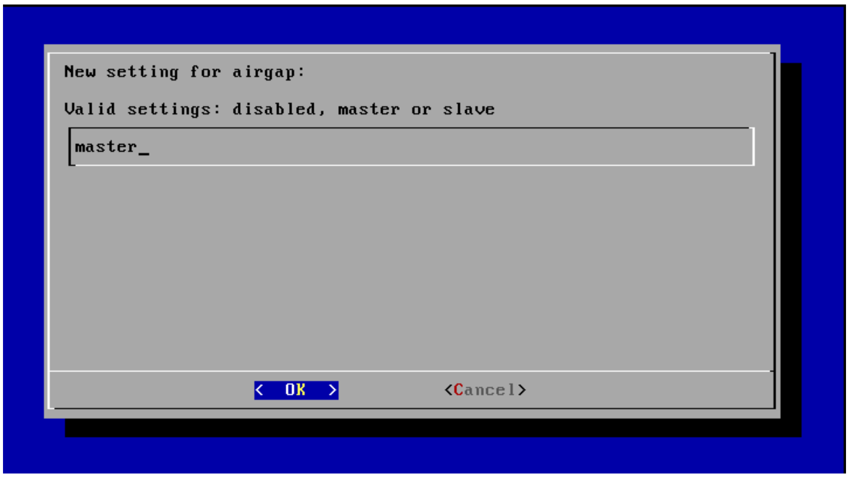
Alternatively the feed updates can be provided via their own FTP server. The FTP server takes on the function of the USB key. Two GSMs are required as well:

- The master picks up the feed from the Internet and writes it to the FTP server.
- The slave downloads the feed from the FTP server.

On the master change into the menu *Airgap management* (see figure *The Airgap management can be found in its own submenu.* (page 50)). Afterwards change the *Airgap type* to the value `ftp` and the *Airgap role* to `master`. Afterwards you will get a new parameter in the menu.

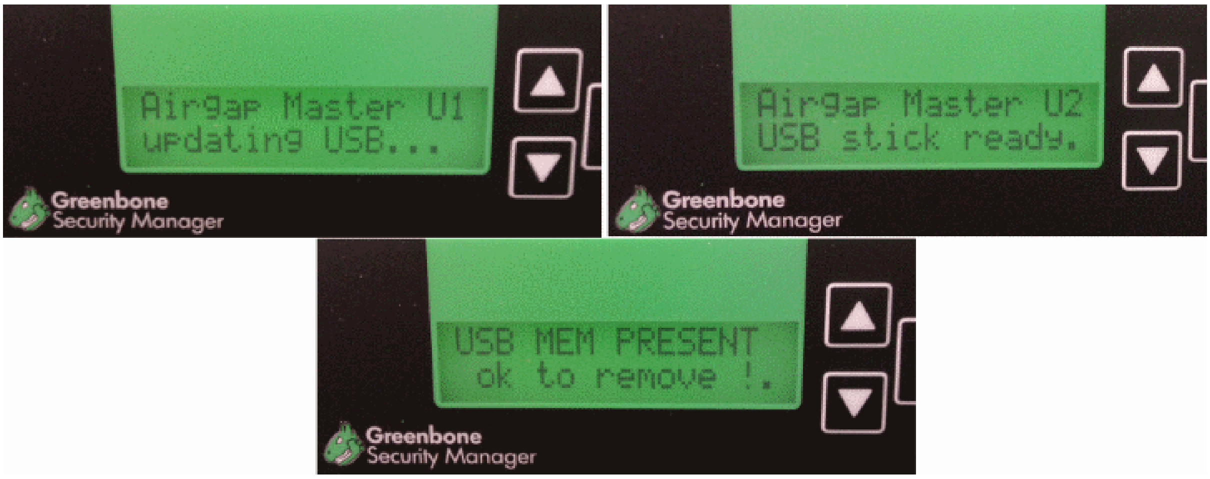
Enter the respective values:

- *FTP location*: This is the FTP server with folder as complete path.
- *FTP user*: This is the FTP user with which to log in.
- *FTP password*: This is the password for the log in.



```
New setting for airgap:

Valid settings: disabled, master or slave

master_
```

Fig. 6.21: Possible Values are `master` and `slave`.



```
Airgap Master U1
updating USB...
```

```
Airgap Master U2
USB stick ready.
```

```
USB MEM PRESENT
 ok to remove !.
```

Fig. 6.22: The Airgap master displays the steps during the creation of the update package on its display.

- *Test FTP*: You can verify the data entered. The test verifies if a log in works with the data supplied.

On the slave perform the same set up. Here only select the *Airgap role* to `slave`.

In order for the synchronization to work flawlessly the synchronization times of the master and slave must be synchronized. Ensure that the master is allowed enough time for the upload of the feeds so that the slave does not load the feed before the master completed the upload. The *Synctime* can be adjusted respectively.

So that the FTP server really displays the function of a diode it should be ensured that the uploaded files are verified after upload. This can be achieved with the pure-ftpd for example. This FTP server allows the possibility to run a script after the upload of a file. It first executes a virus scanner. After the successful verification the script moves the feed files to anther folder to which the slave has access and downloads the feed from.

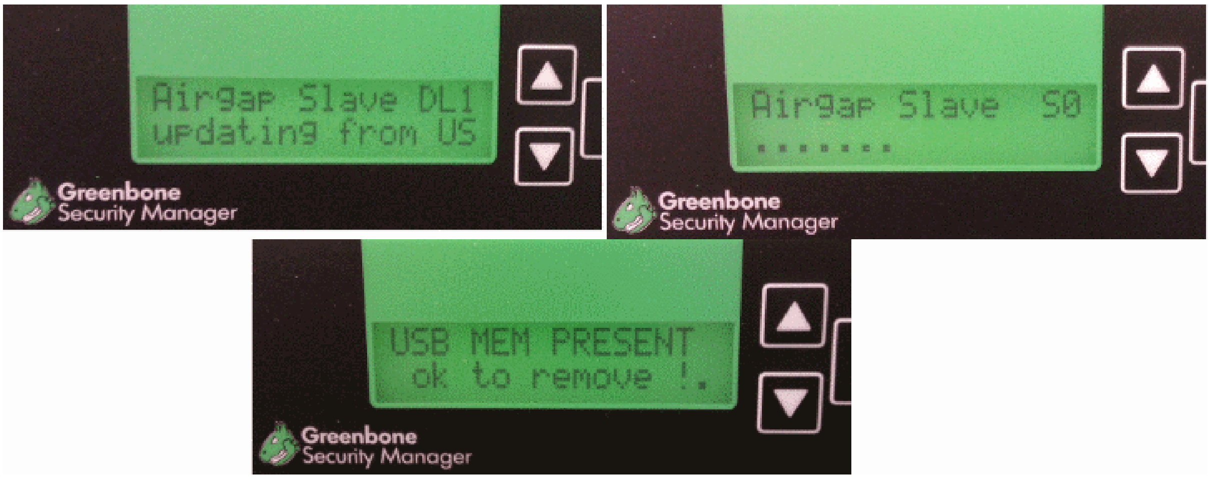
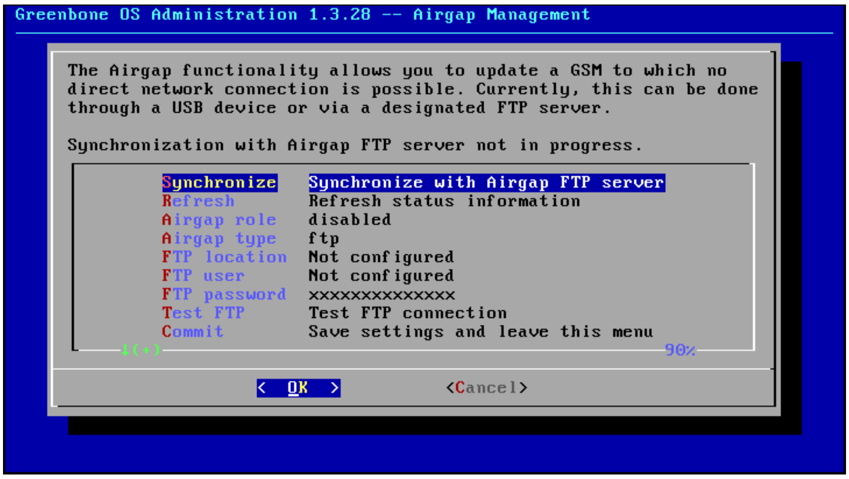


Fig. 6.23: The Airgap slave displays the steps as well.



```
Greenbone OS Administration 1.3.28 -- Airgap Management

  The Airgap functionality allows you to update a GSM to which no
  direct network connection is possible. Currently, this can be done
  through a USB device or via a designated FTP server.

  Synchronization with Airgap FTP server not in progress.

            Synchronize    Synchronize with Airgap FTP server
            Refresh        Refresh status information
            Airgap role    disabled
            Airgap type    ftp
            FTP location   Not configured
            FTP user       Not configured
            FTP password   xxxxxxxxxxxxxx
            Test FTP       Test FTP connection
            Commit         Save settings and leave this menu
       ↓(+)                                                   90%

                    <  OK  >              <Cancel>
```

Fig. 6.24: After activating of FTP new parameters for the configuration are available.

CHAPTER 7

Scanning

This chapter covers the set up and execution of the actual scans of your systems for vulnerability management. The chapter describes basic first steps. Later sections show the more detailed use and configuration of scan configurations and the analysis of the results.

7.1 Simple Scan

This first section describes the first steps of the configuration of the first scan. Basically two options are available. The web interface of the GSM appliance, the Greenbone Security Assistant, provides a wizard that creates all required configurations for a first scan with only very little input. Alternatively these configurations can be created manually step by step. The following two sections cover both options. Ideally the individual steps should be followed directly on a GSM appliance.

These steps are also explained in a video at http://docs.greenbone.net/Videos/gos-3.1/en/GSM-FirstScan-GOS-3.1-en-20150716.mp4.

7.1.1 Wizard

When logging into the web interface of the GSM appliance for the first time after initial set up a wizard will be displayed immediately. By default, this will happen as long as less than four scan tasks were created. Afterwards the wizard can be started at any time by clicking the icon.

To scan a system using the wizard directly it is enough to enter the IP address or system name. However, it is a requirement that the GSM appliance is able to resolve the system name.

The task wizard then automatically performs the following steps:

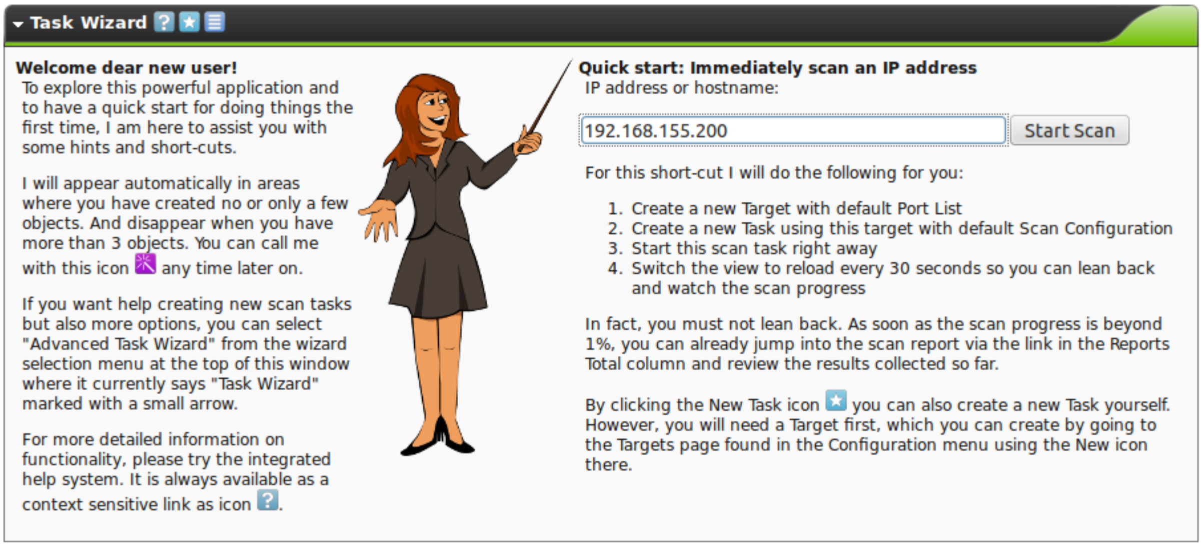
1. Creates a new scan target (Target) in the GSM.
2. Creates a new scan task (Task) in the GSM.
3. Starts the scan task immediately.
4. Changes the view and reloads it every 30 seconds in order to monitor the progress of the task.

After the task is started the progress can be monitored. The Greenbone Security Assistant displays the overview page. The new task can be seen there as well.

The colours and the fill level of the status bar notifies about the status of the scan (see also section *Starting a Task* (page 61)).

As soon as the scan is completed the column Severity notifies about the criticality of the vulnerabilities found. The prior column Solution Type shows the type of solution available. The most common type here is the VendorFix.

The task can be managed via the actions in the right column:



Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.

If you want help creating new scan tasks but also more options, you can select "Advanced Task Wizard" from the wizard selection menu at the top of this window where it currently says "Task Wizard" marked with a small arrow.

For more detailed information on functionality, please try the integrated help system. It is always available as a context sensitive link as icon ?.

Quick start: Immediately scan an IP address
IP address or hostname:

192.168.155.200 Start Scan

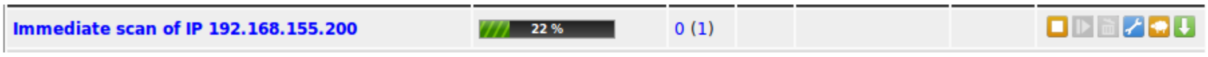
For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

By clicking the New Task icon you can also create a new Task yourself. However, you will need a Target first, which you can create by going to the Targets page found in the Configuration menu using the New icon there.

Fig. 7.1: The task wizard simplifies the first steps



Immediate scan of IP 192.168.155.200 | 22 % | 0 (1)

Fig. 7.2: After the start the progress is being displayed.

- ▶ Starting of a currently not running task.
- ■ Stopping of a currently running task. All discovered results will be written to the database.
- ▷ Resuming of a stopped task.
- 🗑 Moving of a task to the trashcan.
- 🔧 Editing of a task.
- ⧉ Cloning of a task.
- ⬇ Exporting of a task as xml object. The object can be imported again on another GSM.

Even before the scan is completed the results can be viewed (see figure *The results are already available before the scan is completed.* (page 55)). With the mouse simply click on the progress bar. The now displayed results are not complete yet of course. The progress can be continued to be monitored at the top right via the progress bar. This page, however, is not reloaded automatically.

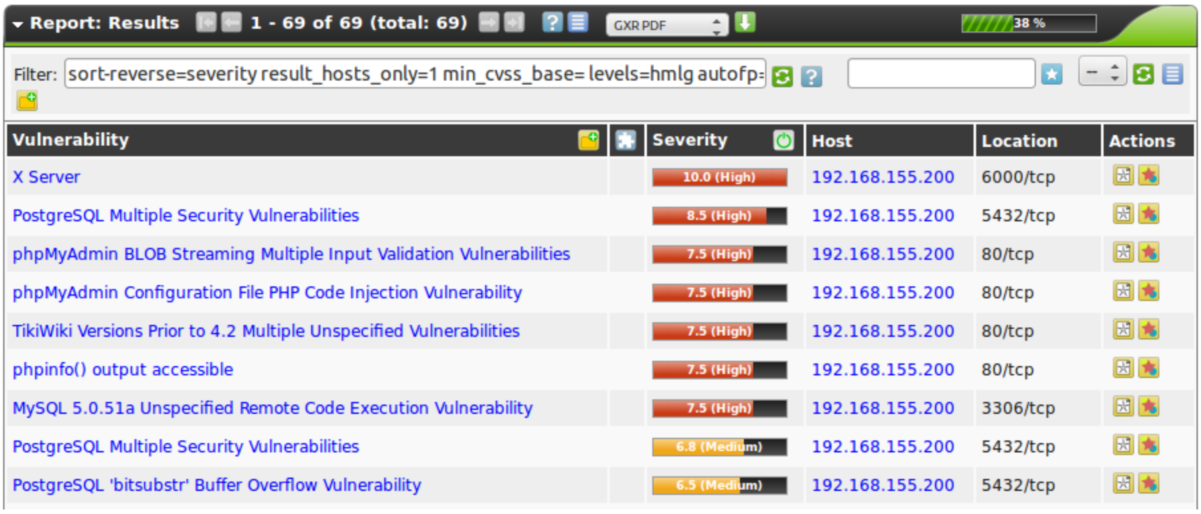
In order to obtain different representations of the results, you can move the mouse over the title bar. It opens a pull-down menu where you can choose different representation formats.

Furthermore the report can be exported in various different formats as well. The export formats are selected in the title bar as well. Afterwards the report can be downloaded by clicking the ⬇ button. Reports and report formats are discussed in more detail in section *Reports* (page 63).

7.1.2 Advanced Wizard

Next to the simple wizard the GSM also provides an advanced wizard that allows for more configuration options. This wizard allows for shortcutting the manual configuration of the individual parameters and still allows for a more granular configuration.

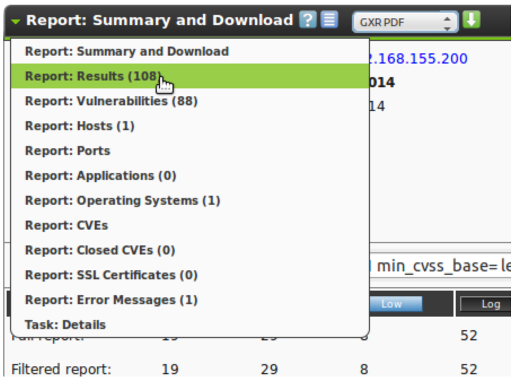
This wizard can be started by clicking on the wizard icon in the context menu. Here a wizard can be executed that allows for the modification of a task (Modify Task Wizard).



Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= levels=hmlg autofp=

Vulnerability		Severity	Host	Location	Actions
X Server		10.0 (High)	192.168.155.200	6000/tcp	
PostgreSQL Multiple Security Vulnerabilities		8.5 (High)	192.168.155.200	5432/tcp	
phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities		7.5 (High)	192.168.155.200	80/tcp	
phpMyAdmin Configuration File PHP Code Injection Vulnerability		7.5 (High)	192.168.155.200	80/tcp	
TikiWiki Versions Prior to 4.2 Multiple Unspecified Vulnerabilities		7.5 (High)	192.168.155.200	80/tcp	
phpinfo() output accessible		7.5 (High)	192.168.155.200	80/tcp	
MySQL 5.0.51a Unspecified Remote Code Execution Vulnerability		7.5 (High)	192.168.155.200	3306/tcp	
PostgreSQL Multiple Security Vulnerabilities		6.8 (Medium)	192.168.155.200	5432/tcp	
PostgreSQL 'bitsubstr' Buffer Overflow Vulnerability		6.5 (Medium)	192.168.155.200	5432/tcp	

Fig. 7.3: The results are already available before the scan is completed.



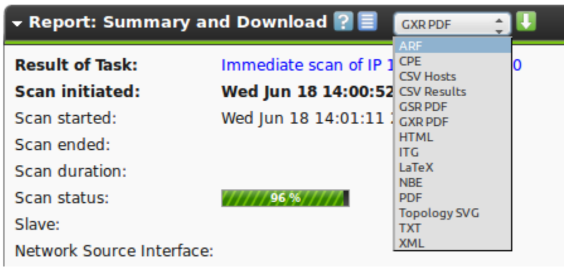
Filtered report:	19	29	8	52

Fig. 7.4: A report can be displayed in different ways.

7.1.3 Manual Configuration

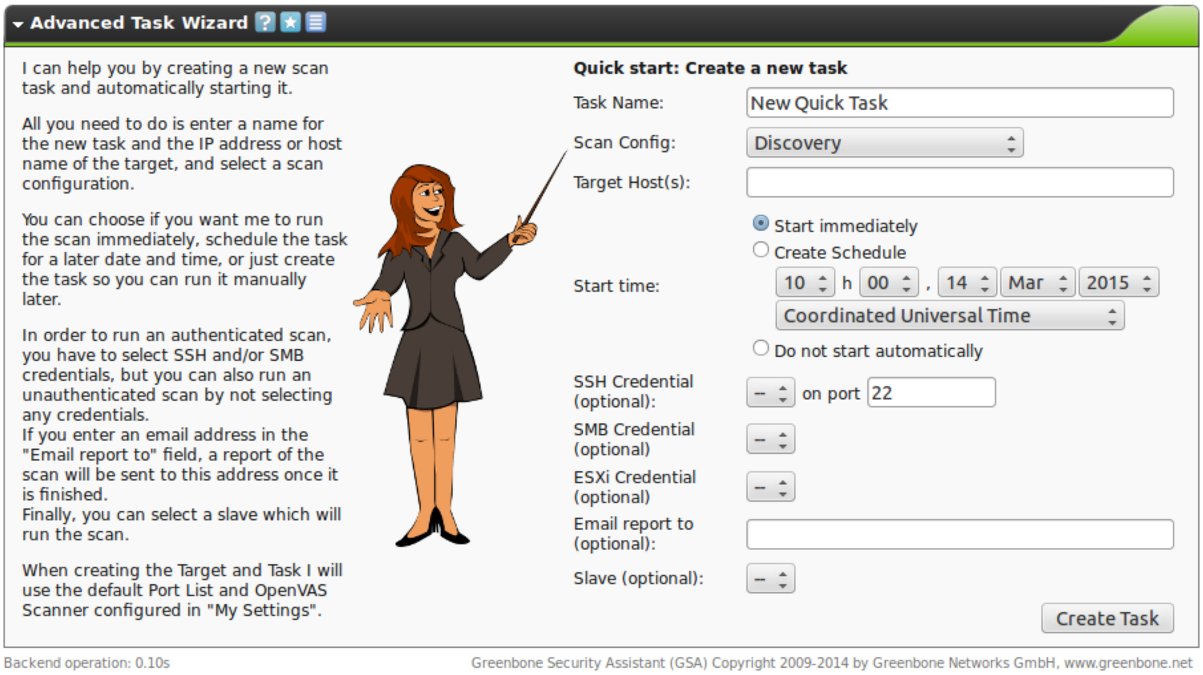
The upcoming section covers the creation of a simple scan with its individual steps that the wizard performs as well. You can chose your own names that make sense for the scan targets (Targets) and the scan task (Task).

These steps are also explained in a video at http://docs.greenbone.net/Videos/gos-3.1/en/GSM-FirstScan-GOS-3.1-en-20150716.mp4.



Result of Task: Immediate scan of IP 1
Scan initiated: **Wed Jun 18 14:00:52**
Scan started: Wed Jun 18 14:01:11
Scan ended:
Scan duration:
Scan status:
Slave:
Network Source Interface:

Fig. 7.5: Furthermore a report can be downloaded in various different formats.



Advanced Task Wizard

I can help you by creating a new scan task and automatically starting it.

All you need to do is enter a name for the new task and the IP address or host name of the target, and select a scan configuration.

You can choose if you want me to run the scan immediately, schedule the task for a later date and time, or just create the task so you can run it manually later.

In order to run an authenticated scan, you have to select SSH and/or SMB credentials, but you can also run an unauthenticated scan by not selecting any credentials.
If you enter an email address in the "Email report to" field, a report of the scan will be sent to this address once it is finished.
Finally, you can select a slave which will run the scan.

When creating the Target and Task I will use the default Port List and OpenVAS Scanner configured in "My Settings".

Quick start: Create a new task

Task Name: New Quick Task

Scan Config: Discovery

Target Host(s):

Start time:
● Start immediately
○ Create Schedule
10 h 00 , 14 Mar 2015
Coordinated Universal Time
○ Do not start automatically

SSH Credential (optional): – on port 22

SMB Credential (optional): –

ESXi Credential (optional): –

Email report to (optional):

Slave (optional): –

Create Task

Backend operation: 0.10s

Greenbone Security Assistant (GSA) Copyright 2009-2014 by Greenbone Networks GmbH, www.greenbone.net

Fig. 7.6: The advanced wizard offers more options.

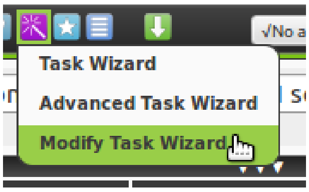


Fig. 7.7: The wizard context menu allows the execution.

Creating a Target

The first step is to define a scan target. This is called Target by the Greenbone Security Assistant.

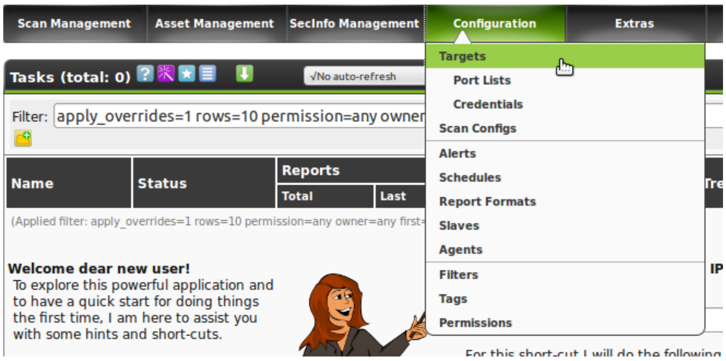
First chose one or more systems in your network you want to scan. The IP address or DNS name is required. In both cases it is necessary that the GSM can reach the system. When using the DNS name the GSM appliance must be able to resolve the name.

Choose *Targets* from the menu *Configuration*. Select the *New Target* icon (the white star on blue background: ★). This icon can be found in many places. It always stands for the creation of a new object within its respective context.

A new window, in which the target can be configured in more detail, will open.

Enter the following information:

- Name The name can be freely chosen. A very descriptive name should be chosen if possible. Possibilities are Mailserver, ClientNetwork, Webserverfarm, DMZ or the like, describing the entered systems in more detail.
- **Comment** The optional comment allows to specify background information. It simplifies understanding the configured targets later.
- **Hosts** Manual entry of the system or importing of a list of systems. When entering manually the following options are available:
  - Single IP address, i.e. 192.168.15.5



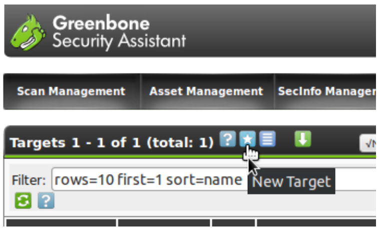
Filter: apply_overrides=1 rows=10 permission=any owner

(Applied filter: apply_overrides=1 rows=10 permission=any owner=any first=

Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

For this short-cut I will do the following

Fig. 7.8: Selecting the targets.



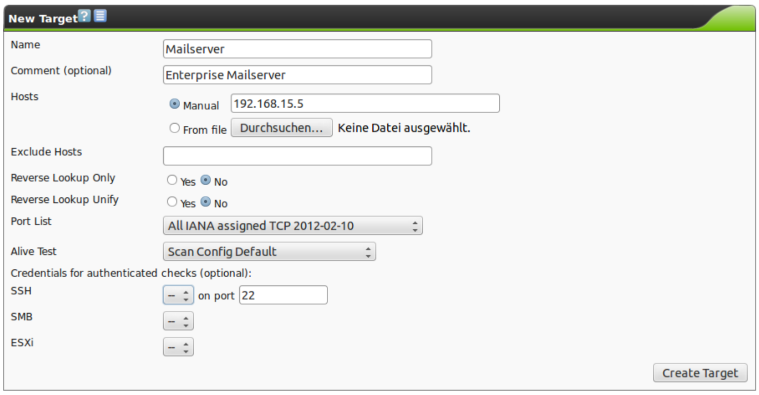
Filter: rows=10 first=1 sort=name

Fig. 7.9: Creating a new target.

- System name, i.e. mail.example.com
- IPv4 address range, i.e. 192.168.15.5-192.168.15.27 or 192.168.55.5-27
- IPv4 network in CIDR notation, i.e. 192.168.15.0/24 [9]
- Single IPv6 address
- IPv6 address range in long format, i.e. ::12:fe5:fb50-::12:fe6:100
- IPv6 address range in short format, i.e. ::13:fe5:fb50-fb80
- IPv6 address range in CIDR notation, i.e. fe80::222:64ff:fe76:4cea/120
- multiple entries can be entered separated with commas

When importing from a file the same syntax can be used. The entries can be stored in the file on multiple lines. When using long lists of systems to be scanned this way is usually the simpler one.

[9] The maximum netmask is /20. This equals 4096 addresses.


New Target

Name	Mailserver
Comment (optional)	Enterprise Mailserver
Hosts	● Manual 192.168.15.5 ○ From file Durchsuchen... Keine Datei ausgewählt.
Exclude Hosts	
Reverse Lookup Only	○ Yes ● No
Reverse Lookup Unify	○ Yes ● No
Port List	All IANA assigned TCP 2012-02-10
Alive Test	Scan Config Default
Credentials for authenticated checks (optional):	
SSH	-- on port 22
SMB	--
ESXi	--

Fig. 7.10: Enter the details for the target.

- **Exclude Hosts** Systems that should be excluded from the lists mentioned above.
- **Reverse Lookup Only** Only scan IP addresses that can be resolved into a DNS name.
- **Reverse Lookup Unify** Should the reverse lookups get unified. If multiple IP addresses resolve to the same DNS name the DNS name will only get scanned once.
- **Port list** The TCP and UDP protocols support 65535 ports respectively. Scanning all ports in many cases takes too long. Many ports are normally not being used. A manufacturer developing a new application often reserves the respective port with the IANA (Internet Assigned Numbers Association). For most scans it is often enough to scan the ports registered with the IANA. The registered ports differentiate from the privileged ports. Privileged ports are ports smaller than 1024 [10]. At the IANA, for example, ports 1433/tcp (MS-SQL) and 3306/tcp (MySQL) are also included in the list. Nmap uses a different list also and doesn't check all ports either. OpenVAS uses a different default as well.

  The scan of TCP ports can be performed simply and fast. Operating system always reply to a TCP request and as such advertise a port as being open (TCP-ACK) or closed (TCP-RST). With UDP this is not the case. The operating system only responds reliably when the port is closed (ICMP-Port-Unreachable). An open port is deducted by the scanner by a missing response. This is why the scanner has to wait for an internal timeout. This behaviour is only true for systems not protected by a firewall. When a firewall exists the discovery of open or closed ports is much more difficult.

  If applications run on unusual ports and they should be monitored and tested with the GSM, the default port lists should be verified under *Configuration* submenu *Port Lists*. If necessary create your own list that includes your port. The default port lists can not be modified.
- **Alive Test** Should the scan check if a target (Targets) is reachable. Options are:
  - ICMP Ping
  - TCP Service Ping
  - ARP Ping
  - ICMP & TCP Service Ping
  - ICMP & ARP Ping
  - TCP Service & ARP Ping
  - ICMP, TCP Service & ARP Ping

In the real world there are problems with this test from time to time. In some environments routers and firewall systems respond to a TCP Service Ping with a TCP-RST even though the host is actually not alive.

Network components also exist that support a Proxy-ARP and respond to an ARP-Ping. This is why this test requires local customization to your environment.

- **SSH Credential** Selection of a user that can log into the target system of a scan if it is a Linux or UNIX system. This allows for an *Authorized Scan* (see section *Authenticated Scan* (page 67)).
- **SMB Credential** Selection of a user that can log into the target system of a scan if it is a Microsoft Windows system. This allows for an *Authorized Scan* (see section *Authenticated Scan* (page 67)).
- **ESXi Credential** Selection of a user that can log into the target system of a scan if it is a VMWare ESXi system. This allows for an *Authorized Scan* (see section *Authenticated Scan* (page 67)).

[10] In UNIX access to these privileged ports is only allowed for privileged users (i.e. root). Ports starting at 1024 are also available to unprivileged users.

Creating a Task

The GSM controls the execution of a scan as Tasks. These tasks can be repeated regularly or run at specific times. The control is discussed in more detail in section *Scheduled Scan* (page 76). For now the basic creation of a task is covered in this section.

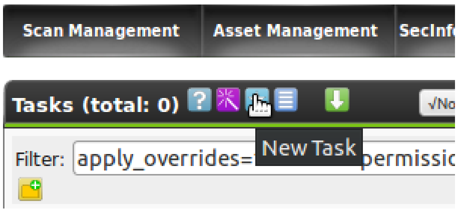
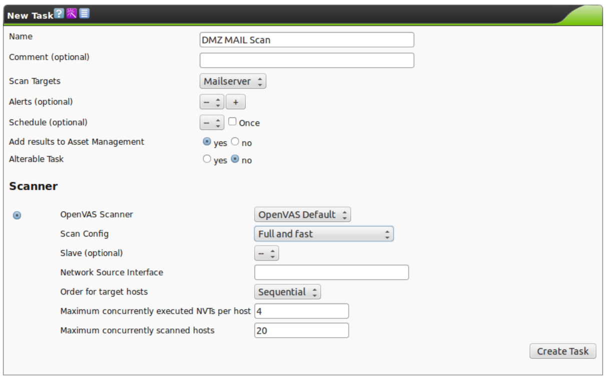


Fig. 7.11: Creation of tasks.

To access the tasks select menu option *Scan Management* from the menu bar. From there select the *Tasks*. On the following page select the white star ☆ on blue background to create a new task. A web page opens on which you can configure the additional options of the task.



Name	DMZ MAIL Scan
Comment (optional)	
Scan Targets	Mailserver
Alerts (optional)	-- +
Schedule (optional)	-- □ Once
Add results to Asset Management	● yes ○ no
Alterable Task	○ yes ● no

Scanner

●	OpenVAS Scanner	OpenVAS Default
	Scan Config	Full and fast
	Slave (optional)	--
	Network Source Interface	
	Order for target hosts	Sequential
	Maximum concurrently executed NVTs per host	4
	Maximum concurrently scanned hosts	20

Fig. 7.12: Creation of a new task.

The following information can be entered:

- **Name** The name can be chosen freely. A descriptive name should be used if possible. Possibilities to describe the entered task are *Scan Mailserver*, *Test ClientNetwork*, *Check DMZ for new ports and systems* or the like.
- **Comment** The optional comment allows for the entry of background information. It simplifies understanding the configured task later.
- **Scan Targets** Select a previously configured Target from the drop down menu.
- **Alerts** Select a previously configured Alert. Status changes of a task can be communicated to the world via email, Syslog, HTTP or a connector.
- **Schedule** Select a previously configured Schedule. The task can be run once or repeatedly at a predetermined time. It is possible to scan the network every Monday morning at 6:00 am for example.
- **Add results to Asset Management** Selecting this option will make the systems available to the Asset Management of the GSM automatically (see chapter Asset Management (page 197)). This selection can be changed at a later point as well.
- **Alterable Task** Allow for modification of the task even though reports were already created. The consistency between reports can no longer be guaranteed if tasks are altered.
- Scanner

- **OpenVAS Scanner** By default only the OpenVAS scanning engine is supported. Additional scanning engines are the Palo Alto and W3AF scanning engines.
- **Scan Config** The GSM comes by default with seven pre-configured scan configurations.
  - **Discovery** Only NVTs are used that provide the most possible information of the target system. No vulnerabilities are being detected.
  - **Host Discovery** Only NVTs are used that discover target systems. This scan only reports the list of systems discovered.
  - **System Discovery** Only NVTs are used that discover target systems including installed operating systems and hardware in use.
  - **Full and Fast** This is the default and for many environments the best option to start with. This configuration is based on the information gathered in the prior port scan and uses almost all NVTs. Only NVTs are used that will not damage the target system. Plugins are optimized in the best possible way to keep the potential false negative rate especially low. The other configurations only provide more value only in rare cases but with much more required effort.
  - **Full and fast ultimate** This configuration expands the first configuration with NVTs that could disrupt services or systems or even cause shut downs.
  - **Full and very deep** This configuration differs from the **Full and Fast** configuration in the results of the port scan not having an impact on the selection of the NVTs. Therefore NVTs will be used that will have to wait for a timeout. This scan is very slow.
  - **Full and very deep ultimate** This configuration adds the dangerous NVTs that could cause possible service or system disruptions to the **Full and very deep** configuration.
- **Slave** Selection of a previously created slave that will be used by the performing scan. The scan can be delegated to another system which has better access to the target system.
- **Network Source Interface** Here you can choose the source interface for the scan.
- **Order for target hosts** Select how the specified network area should be searched. Options available are:
  - Sequential
  - Random
  - Reverse

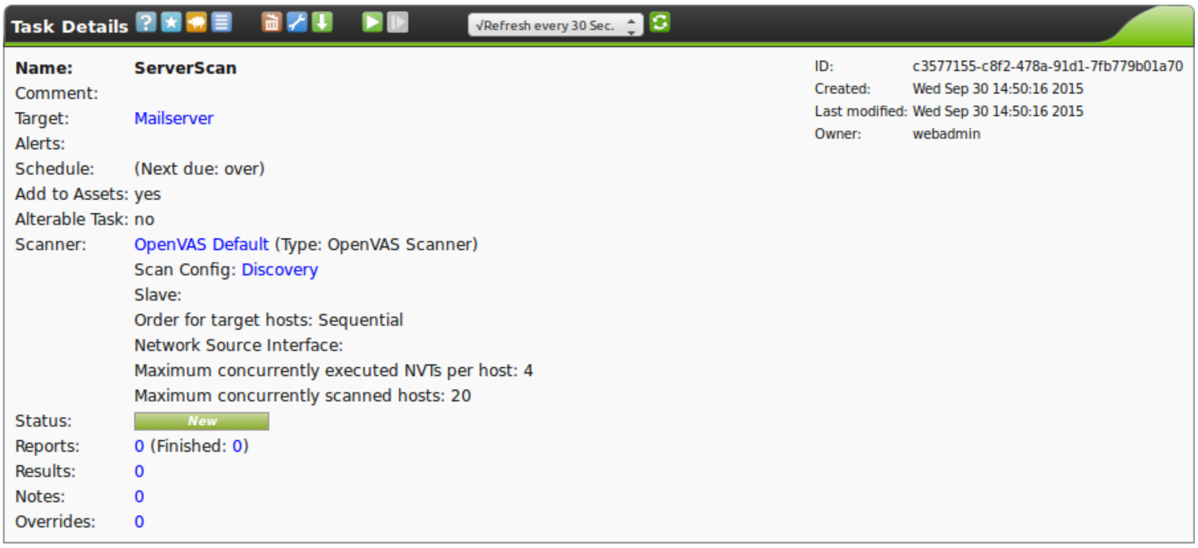
  This is interesting if for example a network, i.e. 192.168.0.0/24, is being scanned that has lots of systems at the beginning or end of the IP address range. With the selection of the `Random` mode the progress view is more meaningful.
- **Scan Intensity** Select the speed of the scan. The default values are chosen sensibly. If more NVTs run simultaneously on a system or more systems are scanned at the same time, there is the danger that a scan has a negative impact on the performance of the systems or network.

Permissions

Once the task is saved it will be displayed next (see figure *A newly created task.* (page 62)).

When scrolling the window further down the permissions for the task can be managed.

Note: By default normal users can not create permissions for other users as they do not have read permission to the user database. To do this a user must specifically have the *get_users* permission. It



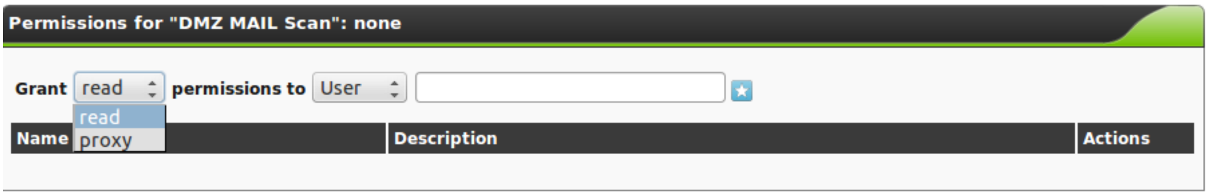
Task Details

√Refresh every 30 Sec.

Name: ServerScan
Comment:
Target: Mailserver
Alerts:
Schedule: (Next due: over)
Add to Assets: yes
Alterable Task: no
Scanner: OpenVAS Default (Type: OpenVAS Scanner)
Scan Config: Discovery
Slave:
Order for target hosts: Sequential
Network Source Interface:
Maximum concurrently executed NVTs per host: 4
Maximum concurrently scanned hosts: 20
Status: New
Reports: 0 (Finished: 0)
Results: 0
Notes: 0
Overrides: 0

ID: c3577155-c8f2-478a-91d1-7fb779b01a70
Created: Wed Sep 30 14:50:16 2015
Last modified: Wed Sep 30 14:50:16 2015
Owner: webadmin

Fig. 7.13: A new task after it is created.



Permissions for "DMZ MAIL Scan": none

Grant read permissions to User

read
proxy

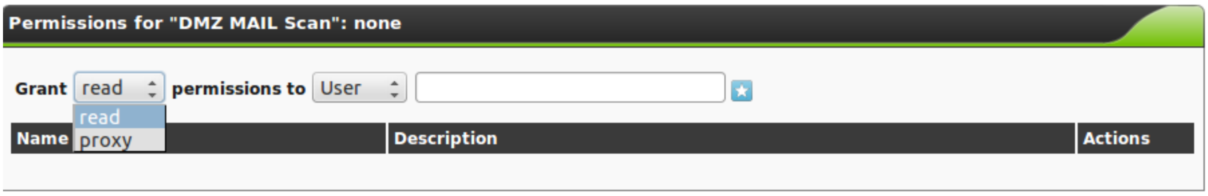
Name	Description	Actions

Fig. 7.14: Read permissions can be managed directly in the task.

makes most sense to create an additional role (see section *GetUsers Role for Observers* (page 172)).

Select *User*, *Group* or *Role* respectively and enter the respective name. After clicking on ★ the permissions are entered.

This is now displayed in the task overview.



Permissions for "DMZ MAIL Scan": none

Grant read permissions to User

read
proxy

Name	Description	Actions

Fig. 7.15: The read permissions of a task are displayed in the overview.

After logging in the user can see those tasks and can access the respective reports.

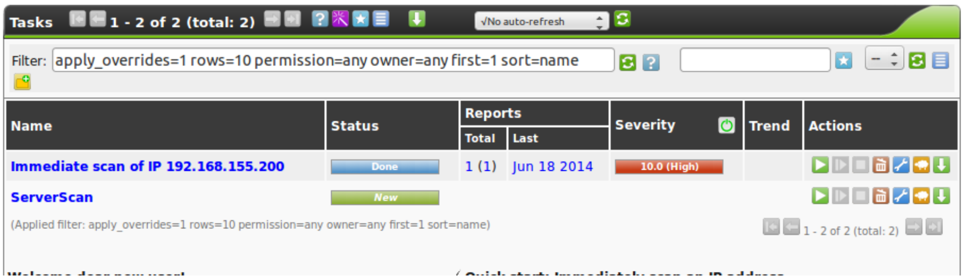
This is now displayed in the task overview.

Starting a Task

Once a task is saved it will be displayed next (see figure *A newly created task.* (page 62)).

The task can be managed via the action icons in the title bar:

- ▶ Starting of a currently not running task.
- ■ Stopping of a currently running task. All discovered results will be written to the database.



Tasks 1 - 2 of 2 (total: 2) √No auto-refresh

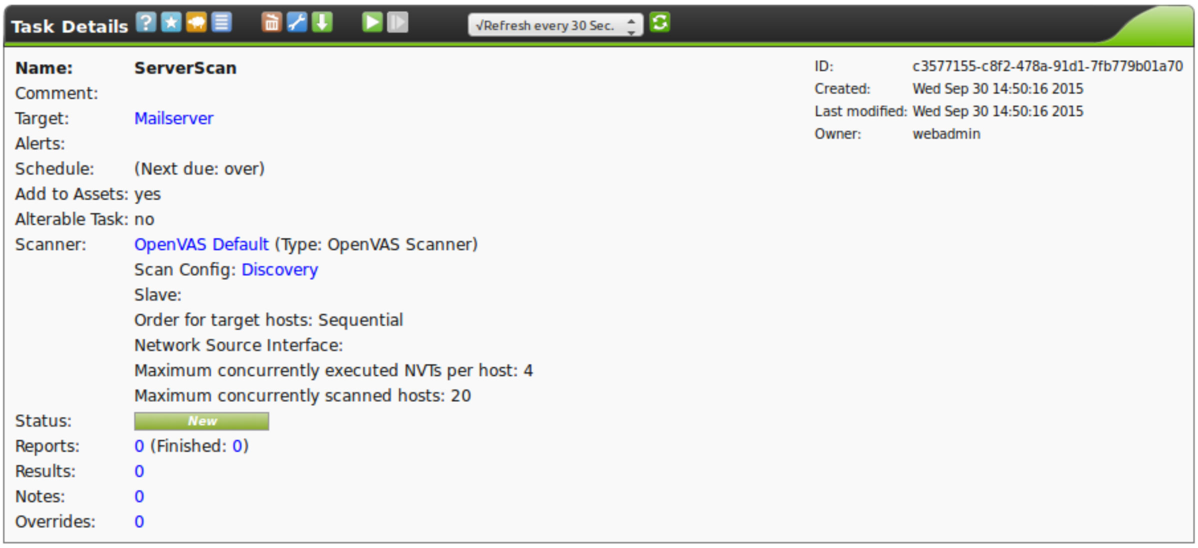
Filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=name

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 192.168.155.200	Done	1 (1)	Jun 18 2014	10.0 (High)		
ServerScan	New					

(Applied filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=name)

1 - 2 of 2 (total: 2)

Fig. 7.16: After logging in the observer can view the tasks but cannot change them.



Task Details √Refresh every 30 Sec.

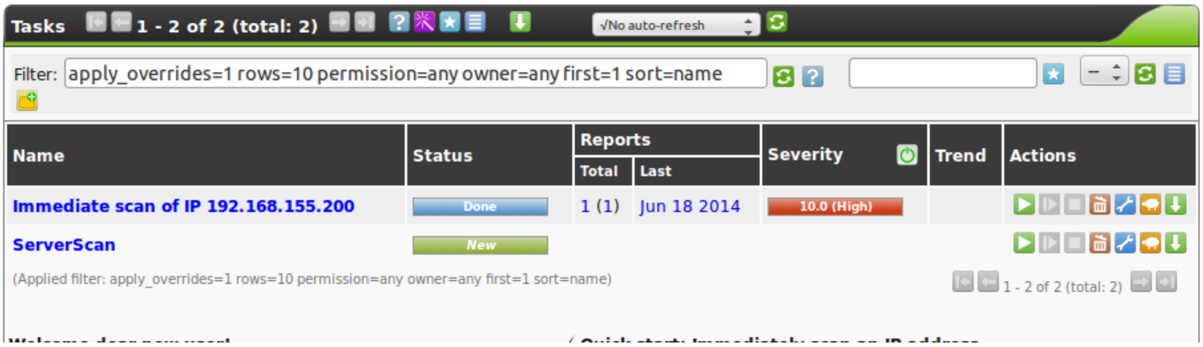
Name: ServerScan
Comment:
Target: Mailserver
Alerts:
Schedule: (Next due: over)
Add to Assets: yes
Alterable Task: no
Scanner: OpenVAS Default (Type: OpenVAS Scanner)
Scan Config: Discovery
Slave:
Order for target hosts: Sequential
Network Source Interface:
Maximum concurrently executed NVTs per host: 4
Maximum concurrently scanned hosts: 20
Status: New
Reports: 0 (Finished: 0)
Results: 0
Notes: 0
Overrides: 0

ID: c3577155-c8f2-478a-91d1-7fb779b01a70
Created: Wed Sep 30 14:50:16 2015
Last modified: Wed Sep 30 14:50:16 2015
Owner: webadmin

Fig. 7.17: A newly created task.

- ⏵ Resuming of a stopped task.
- 🗑 Moving of a task to the trashcan.
- 🔧 Editing of a task.
- ⧉ Cloning of a task.
- ⬇ Exporting of a task as xml object. The object can be imported again on another GSM.

Alternatively starting a task can be performed via the overview page that can be accessed by selecting *Scan Management* and then *Tasks* (see figure *The control of the task is performed in the right column of the overview.* (page 62)).



Tasks 1 - 2 of 2 (total: 2) √No auto-refresh

Filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=name

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 192.168.155.200	Done	1 (1)	Jun 18 2014	10.0 (High)		
ServerScan	New					

(Applied filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=name)

1 - 2 of 2 (total: 2)

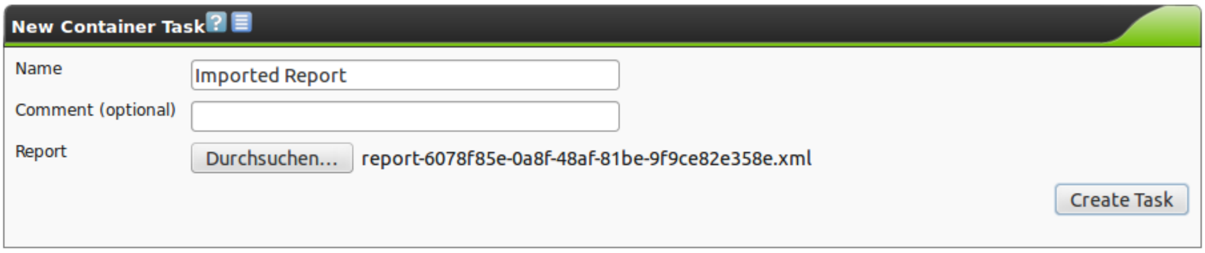
Fig. 7.18: The control of the task is performed in the right column of the overview.

The status bar shows information about the status of a scan. The following colours and states are possible:

- New The task has not been run since it was created.
- 42 % The task is currently running and 42% completed. The information is based on the number of NVTs executed on the selected hosts. For this reason the information does not necessarily correlate with the time spent.
- Requested The task was just started. The GSM is preparing the scan.
- Delete Requested The task was deleted. The actual deletion process can take some time as reports need to be deleted as well.
- Stop Requested The task was stopped recently. However, the scan engine has not reacted respectively yet.
- Stopped at 15 % The last scan was stopped by the user at 15%. The latest report is possibly not yet complete. Other reasons for this status could be the reboot of the GSM or a power outage. After restarting the scanner the task will be resumed automatically.
- Internal Error An error has occurred. The latest report is possibly not yet complete or is missing completely.
- Done The task has been completed successfully.
- Container The task is a container task.

Container Task

A Container Task can be used to import and provide reports created on other GSMs. When creating the *Container Task* the first report needs to be imported right away. Afterwards additional reports can be imported and, like in this example, be compared with a delta report as well.



New Container Task

Name	Imported Report
Comment (optional)	
Report	Durchsuchen... report-6078f85e-0a8f-48af-81be-9f9ce82e358e.xml

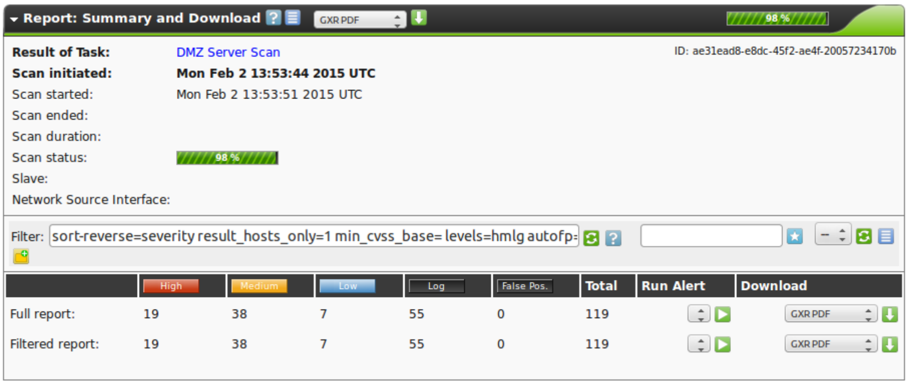
Fig. 7.19: Container tasks are used to import external reports.

The reports need to be in the GSM xml report format.

7.2 Reports

The results of a scan are summarized in a report. Reports can be viewed with a browser and downloaded from the GSM in different formats. Once a scan has been started the report of the results found so far, can be viewed. Once a scan is complete its status changed to `Done`. From now on no additional results will get added. For more information on reports please refer to the Reports (page 87) chapter as well.

The report summary gives a quick overview over the current state. It shows if a scan is complete and how many vulnerabilities have already been found. From the summery a report can be downloaded directly in many different formats. The following formats are supported (see also section *Report Plugins* (page 88))



Result of Task: DMZ Server Scan
ID: ae31ead8-e8dc-45f2-ae4f-20057234170b
Scan initiated: **Mon Feb 2 13:53:44 2015 UTC**
Scan started: Mon Feb 2 13:53:51 2015 UTC
Scan ended:
Scan duration:
Scan status: 98 %
Slave:
Network Source Interface:

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= levels=hmlg autofp=

	High	Medium	Low	Log	False Pos.	Total	Run Alert	Download
Full report:	19	38	7	55	0	119		GXR PDF
Filtered report:	19	38	7	55	0	119		GXR PDF

Fig. 7.20: The report summary gives an overview over vulnerabilities found.

ARF: Asset Reporting Format v1.0.0 This format creates a report that represents the NIST Asset Reporting Format.

CPE - Common Enumeration CSV Table This report selects all CPE tables and creates a single comma separated file.

CSV hosts This report creates a comma separated file containing the systems discovered.

CSV Results This report creates a comma separated file with the results of a scan.

GSR PDF - Greenbone Security Report (recommended) This is the complete Greenbone Security report with all vulnerabilities.

GXR PDF - Greenbone Executive Report (recommended) This is a shortened report for management.

HTML This report is in HTML format.

ITG - IT-Grundschutz catalogue This report is guided by the BSI IT-Grundschutz catalogue.

LaTeX This report is offered as LaTeX source text.

NBE This is the old OpenVAS/Nessus report format.

Details of a report can be viewed in the web UI as well.

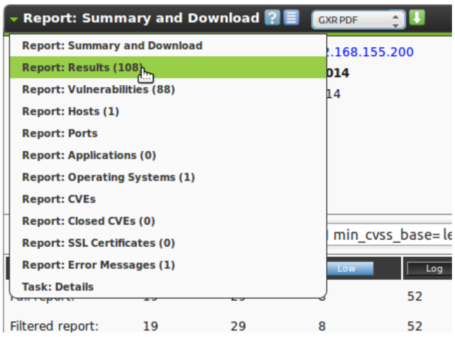
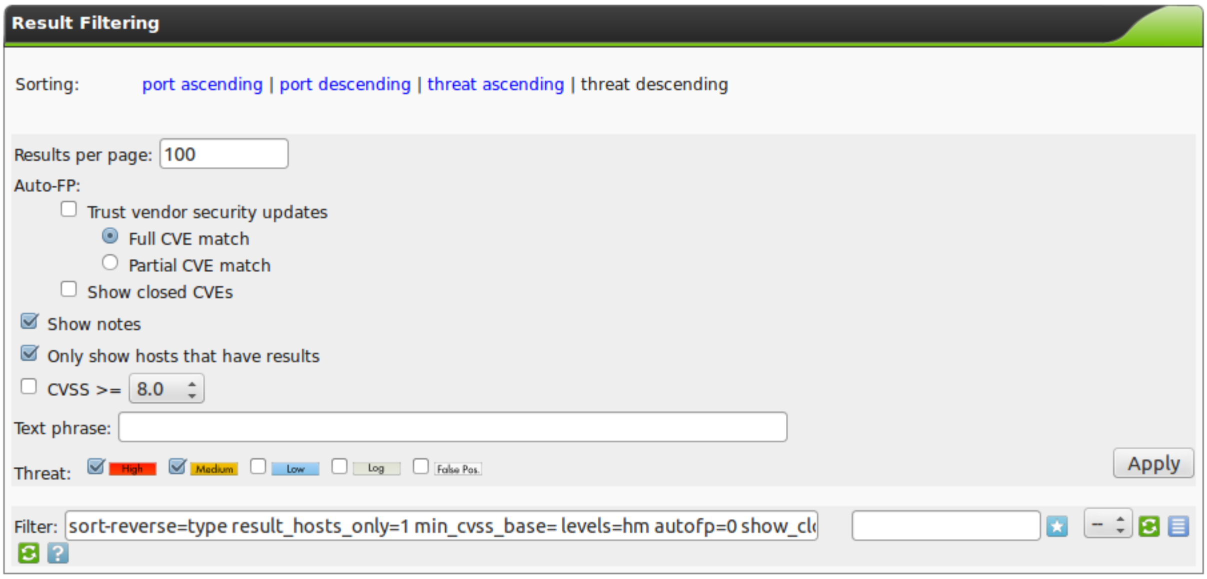


Fig. 7.21: Different views of the same report.

Since a report often contains a lot of findings, the complete report as well as only filtered results can be viewed and downloaded. In the default setting only the `High` and `Medium` risks are being displayed. This can be changed very easily.

In the Filtered Results section shows the filtered results. As long as the scan is still running can cause rearrangements here.

To interpret the results please note the following information:



Result Filtering

Sorting: port ascending | port descending | threat ascending | threat descending

Results per page: 100

Auto-FP:

- □ Trust vendor security updates
  - ● Full CVE match
  - ○ Partial CVE match
- □ Show closed CVEs

☑ Show notes

☑ Only show hosts that have results

□ CVSS >= 8.0

Text phrase:

Threat: ☑ High ☑ Medium □ Low □ Log □ False Pos.

Filter: sort-reverse=type result_hosts_only=1 min_cvss_base= levels=hm autofp=0 show_cl

Fig. 7.22: Report Filtering.

- False Positives False Pos.

  A false positive is a finding that describes a problem that does not exists in reality. Vulnerability scanners often find evidence that point at a vulnerability. However, a final judgment cannot be made. There are two options available:

  - Reporting of a potentially nonexistent vulnerability (False Positive).
  - Ignoring reporting of a potentially existing vulnerability (False Negative).

  Since a user can identify, manage and as such deal with false positives compared to false negatives, the GSM Vulnerability Scanner reports all potentially existing vulnerabilities. The GSM assists with several automatic and semi-automatic to categorize them.

  This problem is very common with Enterprise Linux distributions. If, for example, a SSH service in version 4.4 is installed and the software reports this version during a connection attempt, a vulnerability scanner, that knows of a vulnerability in this version, will report this as such. The vendor potentially already addressed the vulnerability and released version 4.4-p1 that is already installed. This version still reports to the outside version 4.4 so that the vulnerability scanner cannot differentiate. If the user knows of this circumstance an Override can be configured (see section *Overrides and False Positives* (page 81)). The AutoFP function (see section *Automatic False Positives* (page 83)) can assist here as well.

Note: Consider the new concept of Quality of Detection (see sections *Reading of the Reports* (page 66) and *Network Vulnerability Tests* (page 188)).

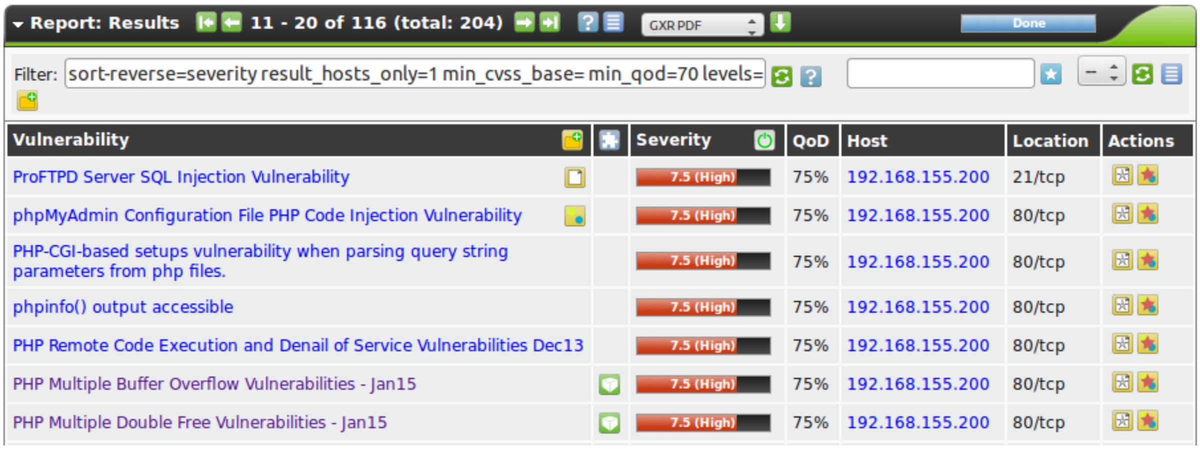
- Multiple findings can have the same cause. Is an especially old software package installed often multiple vulnerabilities exist. Each of these vulnerabilities is tested by an individual NVT and causes an alert. The installation of a current package will then remove a lot of vulnerabilities at once.
- Important are findings of the levels High High and Medium Medium. Address these findings in order of priority. Before addressing medium level findings, high level findings should get addressed. Only in exceptional cases, when it is known that the high alerts need to be less considered (because the service cannot be reached through the firewall) should this approach be deviated from.
- Low Low and Log Log are mostly interesting for detail understanding. This is why these findings are filtered out by default. These findings can hold very interesting information how-

ever and considering them will increase the security of your network and systems. For their understanding often a deeper knowledge of the applications is required. Typical for an alert at the log level is that a service uses a banner with its name and version number. This could be useful for an attacker during an attack if this version has a known vulnerability.

- To simplify the remediation of vulnerabilities every alert offers a solution for problems directly. In most cases it will be referred to the latest vendor software package. In some cases a configuration change will be mentioned.
- References explain the vulnerabilities further. Even though the alerts contain a lot of information external references are always listed. These refer to web sites on which the vulnerability was already discussed. Additional background information is available such as who discovered the vulnerability, what effects it could have and how the vulnerability can be remediated.

7.2.1 Reading of the Reports

The report contains a list of all of the vulnerabilities detected by the GSM (see figure *List of discovered vulnerabilities* (page 66))



Report: Results 11 - 20 of 116 (total: 204)

GXR PDF

Done

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= min_qod=70 levels=

Vulnerability		Severity	QoD	Host	Location	Actions
ProFTPD Server SQL Injection Vulnerability		7.5 (High)	75%	192.168.155.200	21/tcp	
phpMyAdmin Configuration File PHP Code Injection Vulnerability		7.5 (High)	75%	192.168.155.200	80/tcp	
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.		7.5 (High)	75%	192.168.155.200	80/tcp	
phpinfo() output accessible		7.5 (High)	75%	192.168.155.200	80/tcp	
PHP Remote Code Execution and Denail of Service Vulnerabilities Dec13		7.5 (High)	75%	192.168.155.200	80/tcp	
PHP Multiple Buffer Overflow Vulnerabilities - Jan15		7.5 (High)	75%	192.168.155.200	80/tcp	
PHP Multiple Double Free Vulnerabilities - Jan15		7.5 (High)	75%	192.168.155.200	80/tcp	

Fig. 7.23: List of discovered vulnerabilities

To support the administrator with the analysis of the results the severity of a vulnerability (CVSS, see also section *CVSS* (page 193))is displayed directly as a bar.

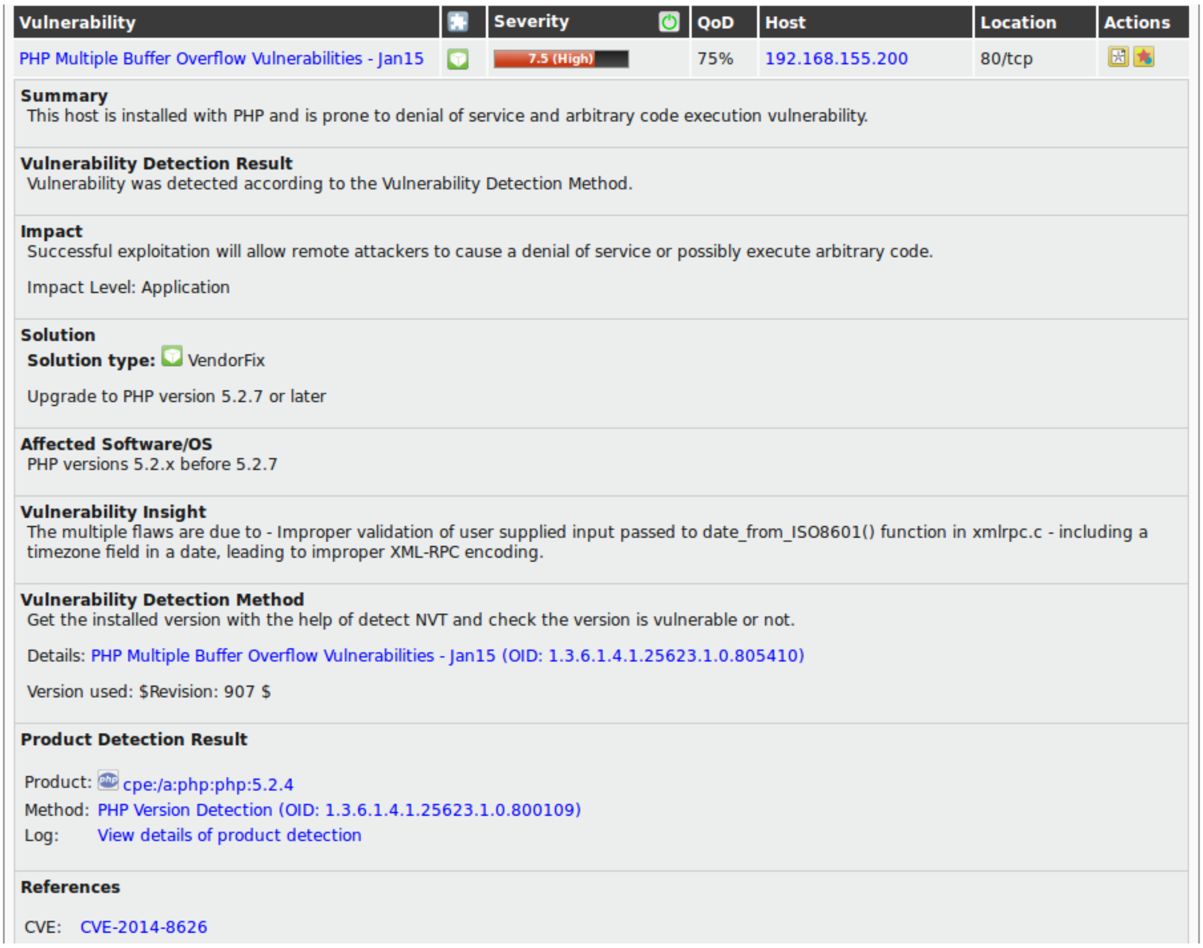
To point the administrator to a simple solution the column Solution-Type displays the existence of a solution. The column will display if a vendor patch exists or a workaround is available. It will also be displayed if no solution for a vulnerability exists. If the column of the respective vulnerability still appears empty then the respective NVT has not been updated yet.

The column Quality of Detection (QoD) provides information in regards to the reliability of the successful detection of a vulnerability. This assessment is implemented into all existing NVTs step by step (see section *Network Vulnerability Tests* (page 188)). This column allows to be filtered as well. You can use the *min_qod* in the Powerfilter. By default only NVTs with a QoD of 70% are displayed. Vulnerabilities with a lower reliability of detection are not displayed in the report. The possibility of false positives is thereby lower.

In the respective vulnerability view, additional, more detailed information is available.

7.3 Results

While the reports only contain the results of one single run of a task all results are saved in the internal database and can be viewed using *Scan Managment/Results*.



Vulnerability		Severity	QoD	Host	Location	Actions
PHP Multiple Buffer Overflow Vulnerabilities - Jan15		7.5 (High)	75%	192.168.155.200	80/tcp	

Summary
This host is installed with PHP and is prone to denial of service and arbitrary code execution vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to cause a denial of service or possibly execute arbitrary code.

Impact Level: Application

Solution
Solution type: VendorFix

Upgrade to PHP version 5.2.7 or later

Affected Software/OS
PHP versions 5.2.x before 5.2.7

Vulnerability Insight
The multiple flaws are due to - Improper validation of user supplied input passed to date_from_ISO8601() function in xmlrpc.c - including a timezone field in a date, leading to improper XML-RPC encoding.

Vulnerability Detection Method
Get the installed version with the help of detect NVT and check the version is vulnerable or not.

Details: PHP Multiple Buffer Overflow Vulnerabilities - Jan15 (OID: 1.3.6.1.4.1.25623.1.0.805410)

Version used: $Revision: 907 $

Product Detection Result

Product: cpe:/a:php:php:5.2.4
Method: PHP Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800109)
Log: View details of product detection

References

CVE: CVE-2014-8626

Fig. 7.24: Detailed information about the vulnerability and solution options.

By default the view is sorted by the creation time of the results. But the results may be sorted by severity, QoD, solution type or host as well. Additionally powerfilters (see section *Powerfilter* (page 139)) may be used to view just the interesting results.

7.4 Authenticated Scan

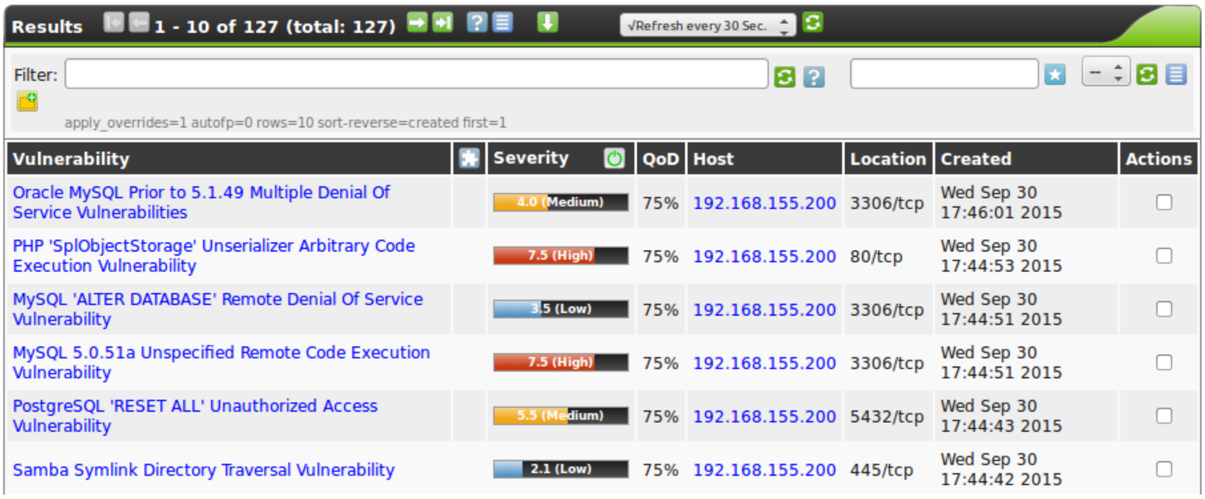
An authenticated scan logs into a target system in order to test it. The scan uses credentials the scan user has saved on the GSM previously. These credentials are used to authenticate with different services on the target system. In some circumstances the results could be limited by the permissions of the users used.

A scan is minimally invasive. It means that the GSM only determines the risk level but does not make any changes on the target system. However the log in by the GSM is being logged in the protocols of the target system.

The GSM can use the credentials for different services. However, the most important ones are:

- **SMB** On Windows systems the GSM can check the patch level and locally installed software such as Adobe Acrobat Reader or the Java suite.
- **SSH** This access is used to check the patch level on UNIX and Linux systems.
- **ESXi** This access is used for testing of VMWare ESXi servers locally.

The extent and success of the testing routines for authenticated scans depends on the heavily on the permissions of the account used for access. Especially on Windows systems unprivileged users are



Results 1 - 10 of 127 (total: 127) √Refresh every 30 Sec.

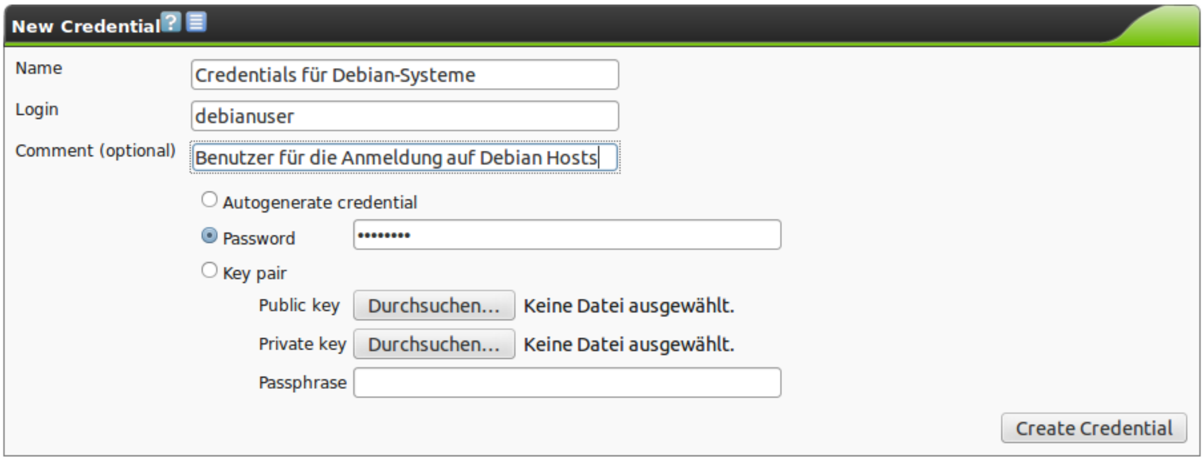
Filter:

apply_overrides=1 autofp=0 rows=10 sort-reverse=created first=1

Vulnerability	Severity	QoD	Host	Location	Created	Actions
Oracle MySQL Prior to 5.1.49 Multiple Denial Of Service Vulnerabilities	4.0 (Medium)	75%	192.168.155.200	3306/tcp	Wed Sep 30 17:46:01 2015	□
PHP 'SplObjectStorage' Unserializer Arbitrary Code Execution Vulnerability	7.5 (High)	75%	192.168.155.200	80/tcp	Wed Sep 30 17:44:53 2015	□
MySQL 'ALTER DATABASE' Remote Denial Of Service Vulnerability	3.5 (Low)	75%	192.168.155.200	3306/tcp	Wed Sep 30 17:44:51 2015	□
MySQL 5.0.51a Unspecified Remote Code Execution Vulnerability	7.5 (High)	75%	192.168.155.200	3306/tcp	Wed Sep 30 17:44:51 2015	□
PostgreSQL 'RESET ALL' Unauthorized Access Vulnerability	5.5 (Medium)	75%	192.168.155.200	5432/tcp	Wed Sep 30 17:44:43 2015	□
Samba Symlink Directory Traversal Vulnerability	2.1 (Low)	75%	192.168.155.200	445/tcp	Wed Sep 30 17:44:42 2015	□

very restricted.

To create credentials access the submenu *Credentials* from the *Configuration* menu. The following information can be entered:



New Credential

Name	Credentials für Debian-Systeme
Login	debianuser
Comment (optional)	Benutzer für die Anmeldung auf Debian Hosts

○ Autogenerate credential

● Password ••••••••

○ Key pair

Public key Durchsuchen... Keine Datei ausgewählt.

Private key Durchsuchen... Keine Datei ausgewählt.

Passphrase

Fig. 7.25: SSH keys can be utilized with credentials as well.

- **Name** An arbitrary name for the credentials.
- **Login** The log in name with which the GSM authenticates on the system that is to be scanned.
- **Comment** A freely selectable comment.
- **Autogenerate Credentials** The GSM itself is creating a random password.
- **Password** The password can be entered.
- **Key Pair** If authentication is performed via SSH the private keys can be uploaded. Additionally an optional passphrase of the private key can be entered.

7.4.1 Requirements on Target Systems with Windows

General notes on configuration

- The remote registry service must be started in order to access the registry

  You can achieve this by configuring the service to automatically start up. If you do not prefer the automatic start, you could configure manual start up. In that case the service will be started while the system is scanned by GSM and afterwards it will be disabled again. To ensure this behaviour the following item about LocalAccountTokenFilterPolicy must be considered.

- It is necessary that for all scanned systems the file and printer sharing is activated. When using Windows XP, take care to disable the setting "Use Simple File Sharing".
- For individual systems not attached to a domain the following registry key must be set:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\DWORD:
LocalAccountTokenFilterPolicy = 1
```

- On systems with domain controller the user account in use must be a member of the group **Domain Administrators** to achieve the best possible results. Due to the permission concept it is not possible to discover all vulnerabilities using the **Local Administrator** or the administrators assigned by the domain. Alternatively follow the instructions below under *Configuring a domain account for authenticated scans* (page 69).
- Should a **Local Administrator** be selected – which we explicitly do not recommend – it is mandatory to set the following registry key as well:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system\DWORD:
LocalAccountTokenFilterPolicy = 1
```

- Generated install package for credentials: The installer sets the `Remote Registry` service to auto start. If the installer is executed on a Domain Controller the user account will be assigned to the Group **Domain Administrators** (`SID S-1-5-32-544`).
- An exception rule for the GSM on the Windows firewall must be created. Additionally on XP systems the **File and Printer Sharing** must be set to `enabled`.
- Generated install package for credentials: During the installation the installer offers a dialog to enter the IP address of the GSM. If the entry is confirmed the firewall rule is configured. The **File and Printer Sharing** service will be enabled in the firewall rules.

Configuring a domain account for authenticated scans

In order to use a domain account for host based remote audits on a windows target this must be performed under Windows XP Professional, Windows Vista, Windows 2003, Windows 2008, Windows 2012 Windows 7, Windows 8 or Windows 8.1 and also be part of a domain.

Taking security into consideration the following eight steps should be implemented to create these scans.

Step 1: Create a security group

First create a security group called `Greenbone Local Scan`:

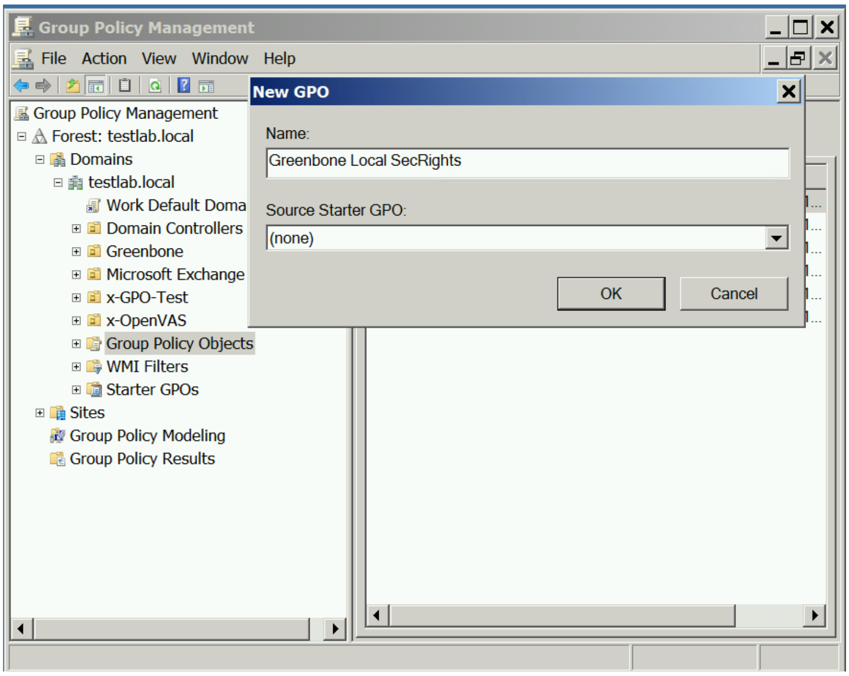
- Log into a domain controller and open `Active Directory Users and Computers`.
- Now create the security group in the menu. Select *Action* > *New* > *Group*.
- Call the group `Greenbone Local Scan`. It is important that the Global is selected for the Group Scope and Security as the Group Type.
- Add the account, that is being used for the local authenticated scans under Windows by the Greenbone Appliance, to the group `Greenbone Local Scan`.

Step 2: Create a Group Policy

Now create a group policy with called `Greenbone Local SecRights`.

- Open the Group Policy Management console.

- Right click on Group Policy Objects and select New.
- Enter `Greenbone Local SecRights` as the name of the policy.



New GPO

Name: Greenbone Local SecRights

Source Starter GPO: (none)

Fig. 7.26: A new Windows Group Policy Object for Greenbone scans.

Step 3: Configuration of the Policy

Add the group `Greenbone Local Scan` to the `Greenbone Local SecRIghts` policy and insert local administrators to the groups.

Please note that this setting still exists after the GPO has been removed (*Tattooing GPO*).

- Click on the policy `Greenbone Local SecRights` and select `Edit`.
- Open:

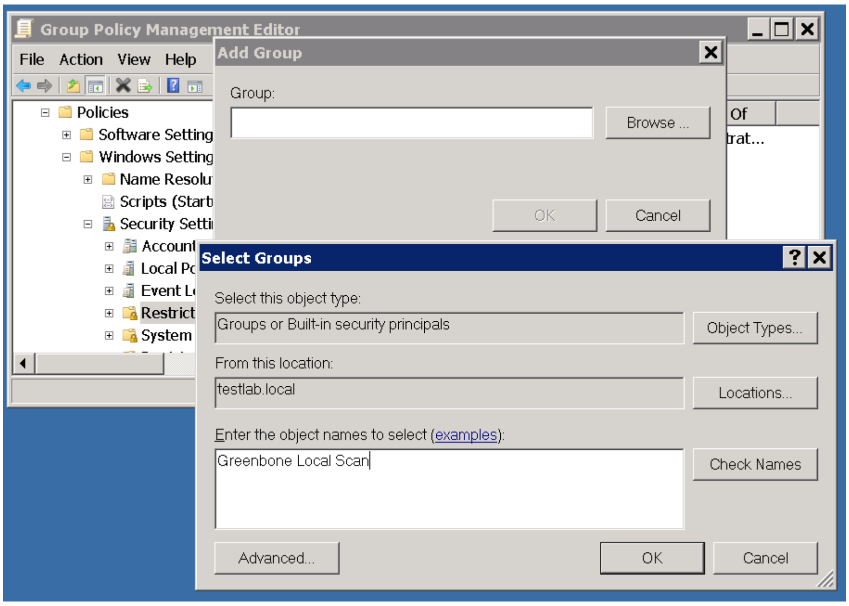
```
Computer Configuration\Policies\Windows Settings\
Security Settings\Restricted Groups
```

- In the left pane right click on Restricted Groups and select `Add Group`
- Now select `Browse` in the `Add Group` dialog, enter `Greenbone Local Scan`, afterwards click `Check Names`.
- Click OK twice to close the opened dialog.
- Under `This group is member of:` click on `Add`.
- Add the group `Administrators`. Additionally on non-English systems enter the respective name of the local administrator group.
- Click OK twice.

Step 4: Configuration of the policy, to deny local log on systems of the `Greenbone Local Scan` **group**

Add the `Greenbone Local Scan` to the `Greenbone Local SecRights` group and deny the local log in of group members.

- Click on the `Greenbone Local SecRights` and then select `Edit`.



Group:

Select this object type: Groups or Built-in security principals

From this location: testlab.local

Enter the object names to select (examples): Greenbone Local Scan

Fig. 7.27: Check Windows Group Name.

- Open:

```
Computer Configuration\Policies\Windows Settings\Security Settings\
Local Policies\User Rights Assignment
```

- In the right pane double click on `Deny log on locally`
- Set the checkmark in `Define these policy settings:`
- Click on `Add User or Group`
- Now select `Browse`, enter `Greenbone Local Scan` and then click on `Check Names`.
- Now click twice on OK to close the opened dialog.
- Click OK.

Step 5: Configure the policy to deny the group `Greenbone Local Scan` logging into systems remotely

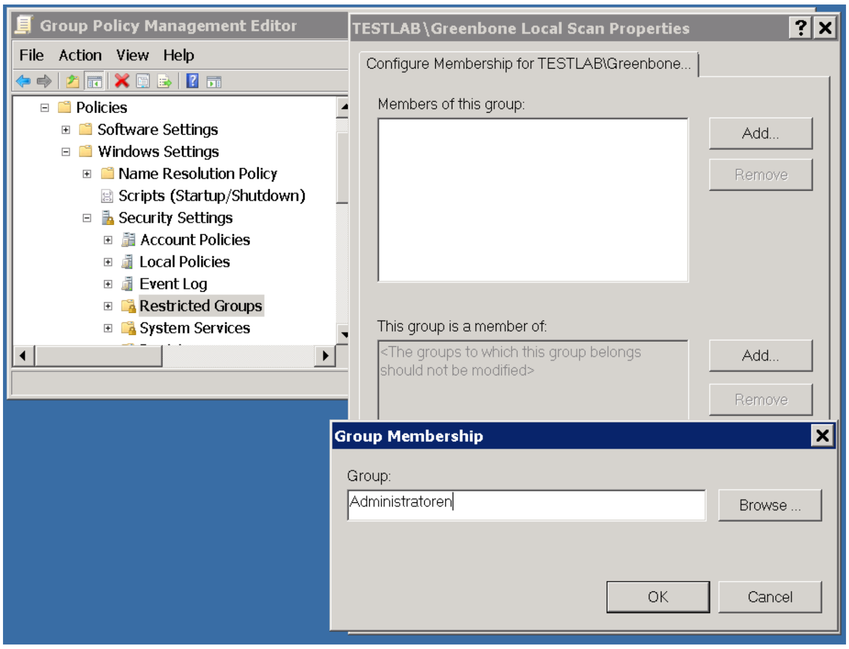
Add the `Greenbone Local Scan` to the `Greenbone Local SecRights` group and deny group members logging in via RDP.

- Click the policy `Greenbone Local SecRights` and then select `Edit`.
- Open:

```
Computer Configuration\Polices\Windows Settings\Security Settings\
Local Policies\User Rights Assignment
```

- In the right pane double click on `Deny log on through Remote Desktop Services`.
- Set the checkmark in `Define these policy settings:`
- Click on `Add User or Group`
- Now select `Browse` in the dialog, enter `Greenbone Local Scan`, then click on `Check Names`.
- Now click twice on OK to close the opened dialog.
- Click OK.

Step 6 (Optional): Configure the policy to give only read permissions to the local drive for the `Greenbone Local Scan` group.



Group: Administratoren

Fig. 7.28: Add Group Membership.

Restrict the permissions to the system drive in the `Greenbone Local SecRights` policy for the `Greenbone Local Scan` group. Please note that this setting still exists after the GPO has been removed (`Tattooing GPO`).

- Click on the `Greenbone Local Sec Rights` policy and then select `Edit`.
- Open:

```
Computer Configuration\Polices\Windows Settings\Security Settings\File Systems
```

- In the left pane right click on File System and select `Add File...`.
- In the Folder field enter: `%SystemDrive%` and click OK.
- Click on Add under `Group or user names:`
- In the dialog that opens enter `Greenbone Local Scan` and click OK.
- Now select the user `Greenbone Local Scan`.
- Deactivate all checkmarks under `Allow` and activate the checkmarks under *Deny* > *Write*.
- Afterwards click on OK and confirm the warning message with `Yes`.
- Now select `Configure this file or folder then` and `Propagate inheritable permissions to all subfolders and files` and then click on OK.

Step 7 (Optional): Configure the policy to give only read permissions to the registry for the `Greenbone Local Scan` group.

To achieve complete restriction is very difficult and possible with a lot of effort. If necessary critical branches can be secured additionally by adding the branches manually.

Please note that this setting still exists after the GPO has been removed (*Tattooing GPO*).

- In the left pane right click `Registry` and select `Add Key`.
- Select `Users` and click OK
- Click on Advanced and then Add.
- Enter `Greenbone Local Scan` in the dialog that opens and click on OK.

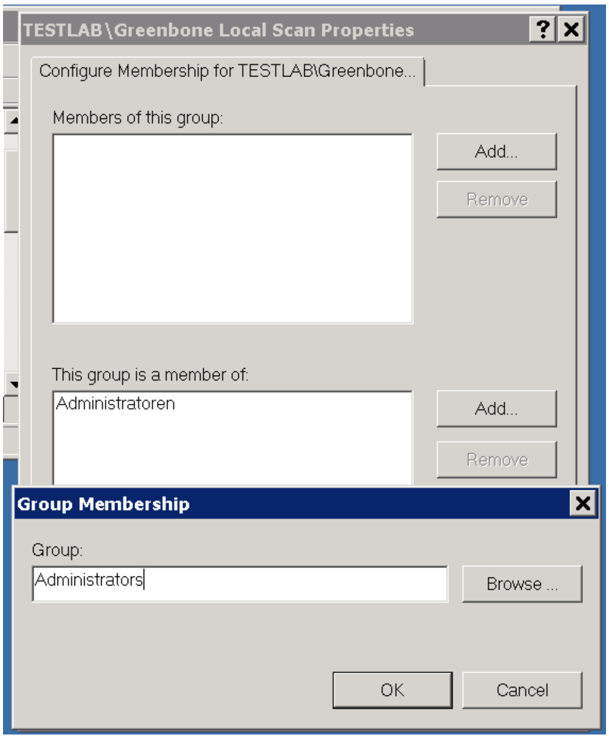


Fig. 7.29: Add another Group Membership.

- In the following dialog select for `Apply to: This object and child objects`
- Under Permissions select Deny for `Set Value`, `Create Subkey`, `Create Link`, `Delete`, `Change Permissions` and `Take Ownership`.
- Do not select anything under `Allow`!
- Afterwards click OK twice and confirm the warning message with `Yes`.
- Click OK again.
- Now select `Configure this key then` and `Propagate inheritable permissions to all subkeys` and then click OK.
- Repeat the above mentioned steps also for MACHINE and CLASSES_ROOT by clicking on Registry in the right pane and then select `Add key...`.

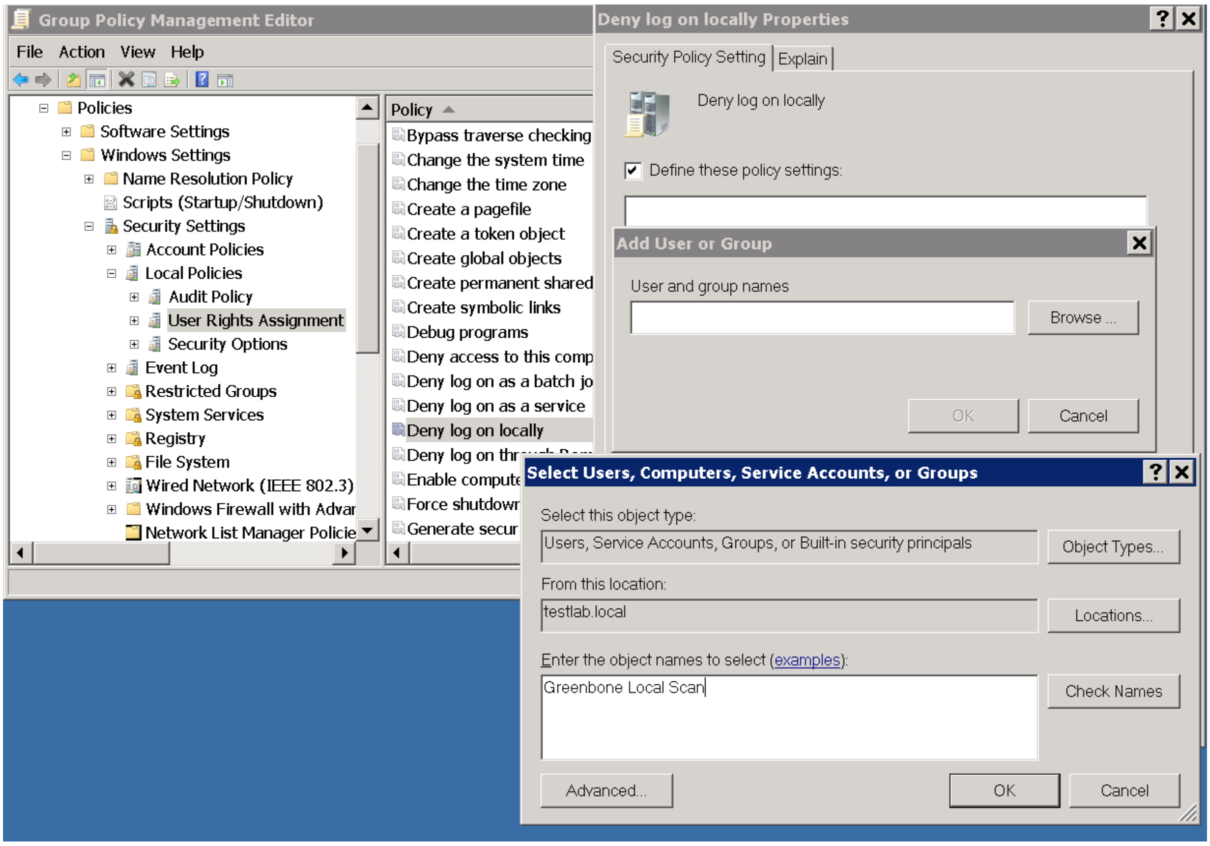
Step 8 (Optional): Linking of the Group Policy Object

- On the right pane in the Group Policy Management console right click on the domain or Organizational Unit `Link an Existing GPO` and select `Link an Existing GPO`....
- Now select the group policy object `Greenbone Local SecRights`.

Restrictions

Based on the fact that write permissions to the registry and system drive have been removed, the following two tests will no longer work:

- **`Leave information on scanned Windows hosts` OID 1.3.6.1.4.1.25623.1.0.96171** This test, if desired, creates information about the start and end of a scan under HKLMSoftwareVulScanInfo. Due to denying write access to HKLM this is no longer possible. If you continue to desire this the GPO must be adjusted here respectively.



☑ Define these policy settings:

Select this object type:
Users, Service Accounts, Groups, or Built-in security principals

From this location:
testlab.local

Enter the object names to select (examples):
Greenbone Local Scan

Fig. 7.30: Edit the policy for local log on.

- **Windows file Checksums OID 1.3.6.1.4.1.25623.1.0.96180** This test, if desired, when executed saves the tool ReHash under C:\Windows\system32 (for 32-bit systems) or c:\Windows\SysWOW64 (for 64-bit systems). Due to denying write access this is no longer possible. The tool must be saved separately or the GPO must be adjusted respectively.

  More information can be found in section *File Checksums* (page 98).

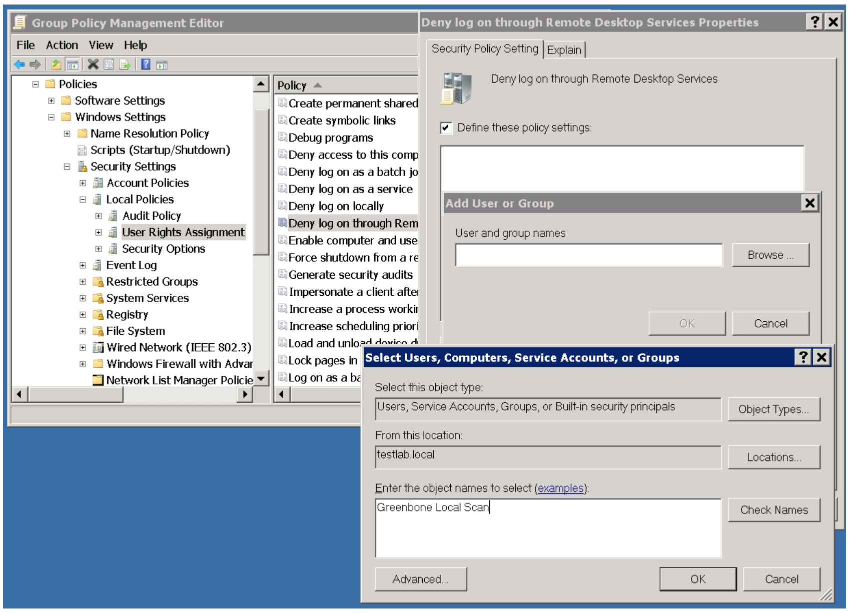
Scanning without domain admin and local admin permissions

Theoretically it is possible to build a GPO in which the user also does not have any local admin permissions. But the effort to add respective read permissions to each registry branch and folder as well, is enormous. Unfortunately inheriting of permissions is deactivated for many folders and branches. Additionally these changes can be set by GPO but cannot be removed again (Tattooing GPO). Also specific permissions could possibly be overwritten so that additional problems could occur.

To go this route does not make a lot of sense from a technical and administrative perspective.

7.4.2 Requirements on Target Systems with Linux/UNIX

- For authenticated scans on Linux or UNIX systems regular user access is usually enough. The log in is performed via SSH. The authentication is done wither with passwords or an SSH key stored on the GSM.
- Generated install package for credentials: The install package for Linux Debian or Linux RedHat is a `.deb` or a `.rpm` respectively, creating a new user without any specific permissions. A SSH Key that is created on the GSM is stored in the users home folder. For users of other Linux distributions or UNIX derivatives the key is offered for download. The creation of a user and saving the key with the proper file permissions is the responsibility of the user.



Deny log on through Remote Desktop Services

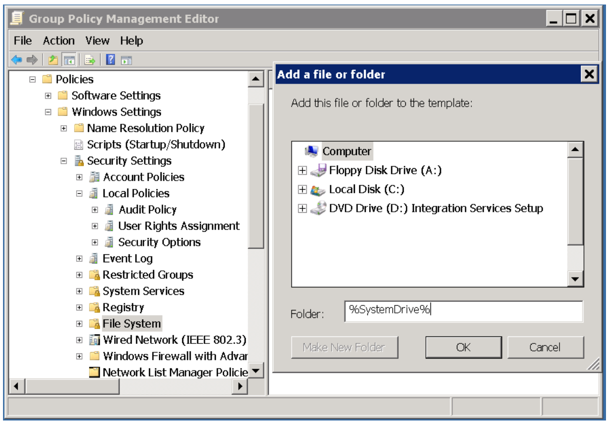
☑ Define these policy settings:

Select this object type: Users, Service Accounts, Groups, or Built-in security principals

From this location: testlab.local

Enter the object names to select: Greenbone Local Scan

Fig. 7.31: Edit Policy for remote log in.



Folder: %SystemDrive%

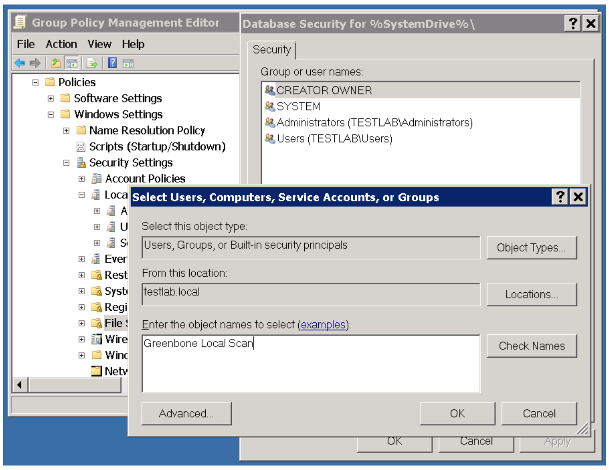
Fig. 7.32: Specifying the `%SystemDrive%` folder.

- In both cases it needs to be made sure that Public Key authentication is not prohibited by the SSH daemon. The line `PubkeyAuthentication no` can not be present.
- Already existing SSH keys protected by an optional passphrase can be used as well. It is recommended to use the RSA and DSA formats as created by the command **ssh-keygen**.
- For scans that include policy testing root permission or the membership in specific groups (often `wheel`) might be necessary. For security reasons many configuration files are only readable by super user or members of specific groups.

7.4.3 Requirements on Target Systems with ESXi

By default, local ESXi users are limited to read-only roles. Either an administrative account or a read-only role with permission to global settings must be used.

To avoid using a administrative account, clone the `Read-Only` role and then select `Global > Settings`. Finally the scan user account must be assigned with this new role.



Group or user names:

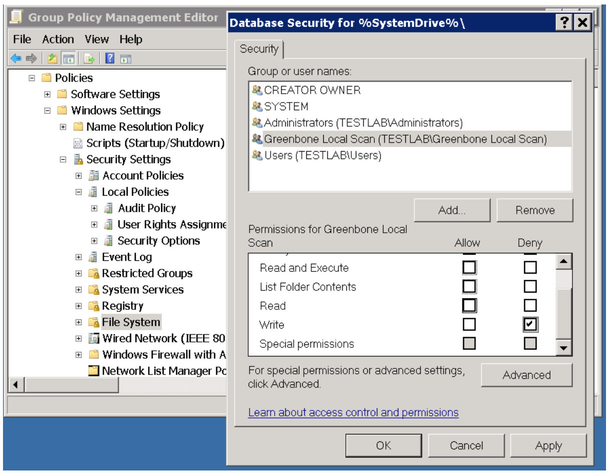
- CREATOR OWNER
- SYSTEM
- Administrators (TESTLAB\Administrators)
- Users (TESTLAB\Users)

Select this object type: Users, Groups, or Built-in security principals

From this location: testlab.local

Enter the object names to select (examples): Greenbone Local Scan

Fig. 7.33: Select the `Greenbone Local Scan` group.



Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (TESTLAB\Administrators)
- Greenbone Local Scan (TESTLAB\Greenbone Local Scan)
- Users (TESTLAB\Users)

Permissions for Greenbone Local Scan	Allow	Deny
Read and Execute	□	□
List Folder Contents	□	□
Read	□	□
Write	□	☑
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

Fig. 7.34: Deny Write access to the group.

7.4.4 Autogenerate Credentials

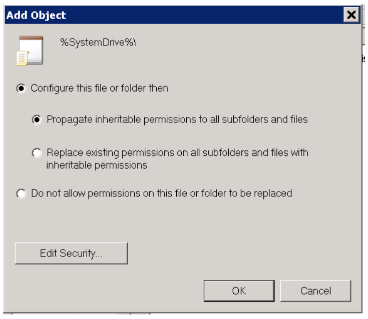
To simplify the installation and creation of accounts for authenticated scans the GSM option *Autogenerate Credential* offers an install package for the respective target system. This package creates the user and the most important permissions for the authenticated scan and re-sets them again during uninstallation.

The install package is provided for:

- Debian based systems
- RPM based systems
- Windows
- Public Key

7.5 Scheduled Scan

Once tasks are created executing them manually can be annoying. The GSM offers the possibility to automate different tasks. This is done via *Schedules*. It can be found in the *Configuration* menu.


Add Object

%SystemDrive%\

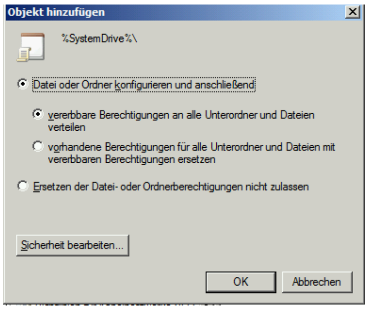
● Configure this file or folder then

● Propagate inheritable permissions to all subfolders and files

○ Replace existing permissions on all subfolders and files with inheritable permissions

○ Do not allow permissions on this file or folder to be replaced

Fig. 7.35: Make the permissions recursive.


Objekt hinzufügen

%SystemDrive%\

● Datei oder Ordner konfigurieren und anschließend

● vererbbare Berechtigungen an alle Unterordner und Dateien verteilen

○ vorhandene Berechtigungen für alle Unterordner und Dateien mit vererbbaren Berechtigungen ersetzen

○ Ersetzen der Datei- oder Ordnerberechtigungen nicht zulassen

Fig. 7.36: Policy for read permissions on the system drive.

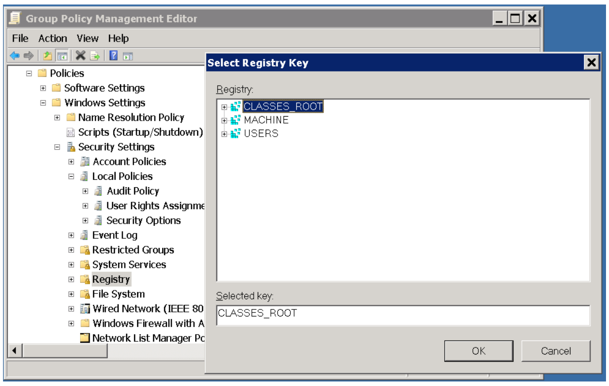
Directly after start up no schedule is pre-configured. The first schedule needs to be created by you. To do so select the ★ button.

The Greenbone Security Manager refers to Schedules as automatic scans at a specific time. They can be run once or repeatedly. The intervals can be configured in much detail:

- hourly
- daily
- weekly
- monthly

The time zone is very important in a schedule. It can be selected from a drop down menu. For Eastern Standard Time (EST) you will likely choose `America/New York`. Finally the maximum duration of the scan can be limited. If the scan takes longer it will aborted. This way it can be ensured that the scan will always run with a specific time window.

Now the schedule can be defined and the following data can be entered:



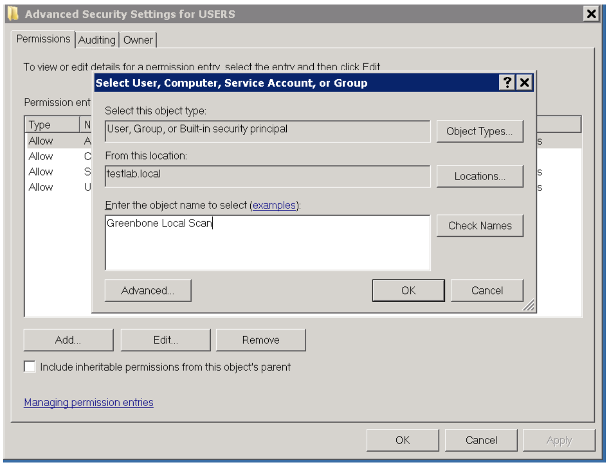
Select Registry Key

Registry:

CLASSES_ROOT
MACHINE
USERS

Selected key: CLASSES_ROOT

Fig. 7.37: Select the `USERS` registry key.



Advanced Security Settings for USERS

Permissions | Auditing | Owner

To view or edit details for a permission entry, select the entry and then click Edit.

Select User, Computer, Service Account, or Group

Select this object type:
User, Group, or Built-in security principal

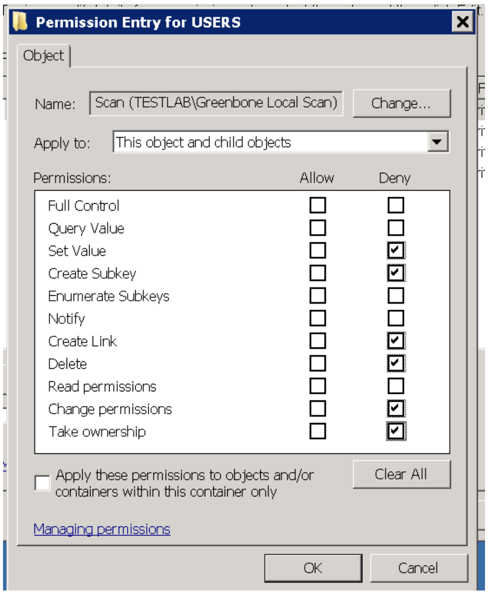
From this location:
testlab.local

Enter the object name to select (examples):
Greenbone Local Scan

☐ Include inheritable permissions from this object's parent

Managing permission entries

Fig. 7.38: Select the `Greenbone Local Scan` group.



Permission Entry for USERS

Object

Name: Scan (TESTLAB\Greenbone Local Scan)

Apply to: This object and child objects

Permissions:	Allow	Deny
Full Control	☐	☐
Query Value	☐	☐
Set Value	☐	☑
Create Subkey	☐	☑
Enumerate Subkeys	☐	☐
Notify	☐	☐
Create Link	☐	☑
Delete	☐	☑
Read permissions	☐	☐
Change permissions	☐	☑
Take ownership	☐	☑

☐ Apply these permissions to objects and/or containers within this container only

Managing permissions

Fig. 7.39: Disallow edition of the registry.

Name This is a descriptive name. Meaningful are entries such as `Daily 5:15pm` or `Every 2nd monthly 4:15am`.

Comment Enter a comment again.

First Time Enter the time of the first run.

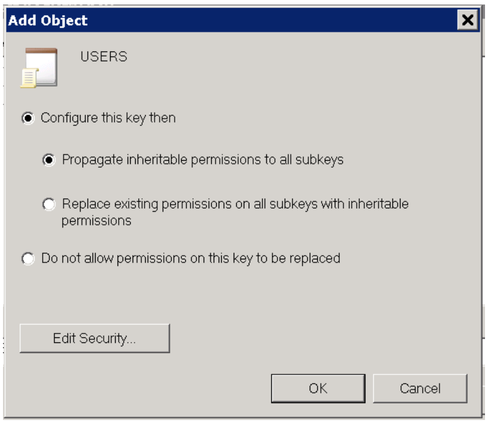
Period This is the interval between two runs. It can be selected between hourly, daily, weekly and monthly. If left blank the interval is a single instance.

Timezone Select the time zone. UTC is standard.

Duration This is the maximum duration a task can take for its execution. After expiration of the of the time allotted the task is aborted.

7.6 Notes

Notes allow adding comments to a Network Vulnerability Test (NVT). They will also be displayed in the reports. A Note can be added to a specific result, a specific task, a risk level, port or host and as such



Add Object

USERS

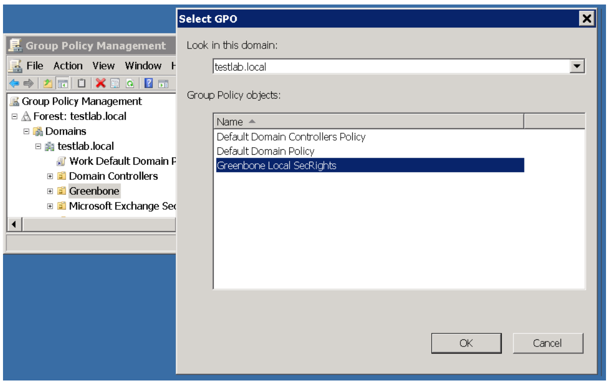
● Configure this key then

● Propagate inheritable permissions to all subkeys

○ Replace existing permissions on all subkeys with inheritable permissions

○ Do not allow permissions on this key to be replaced

Fig. 7.40: Propagate the new settings recursively.



Select GPO

Look in this domain: testlab.local

Group Policy objects:

Name
Default Domain Controllers Policy
Default Domain Policy
Greenbone Local SecRights

Fig. 7.41: Linking the policy.

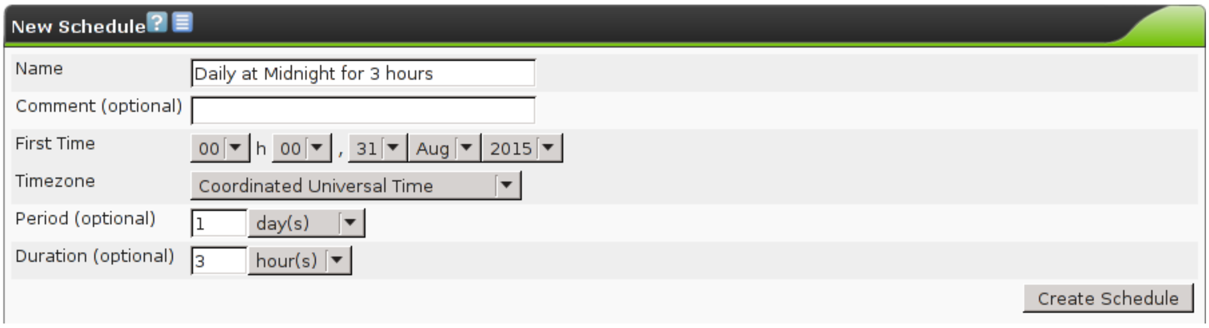
will only appear in specific reports. A Note can be generalized just as well so that it will be displayed in all reports.

7.6.1 Creating notes

To create a new note select the finding in the report you want to add a note to and click *New Note* ⭐. Alternatively you can create a note without relation to a finding. However, the GSM can not suggest any meaningful values for the different fields in the following dialogue.

A new window opens in which exactly those criteria of the selected vulnerability are pre-set.

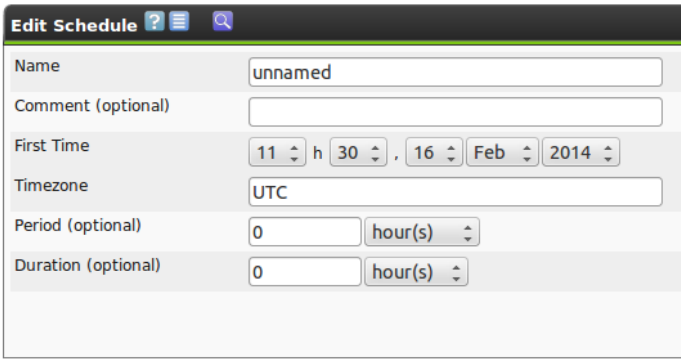
Individual values can be selected and unselected to generalize or the note even further or make it more specific. Additionally the note can be activated for a specific period of time. This allows adding



New Schedule

Name	Daily at Midnight for 3 hours
Comment (optional)	
First Time	00 h 00 , 31 Aug 2015
Timezone	Coordinated Universal Time
Period (optional)	1 day(s)
Duration (optional)	3 hour(s)

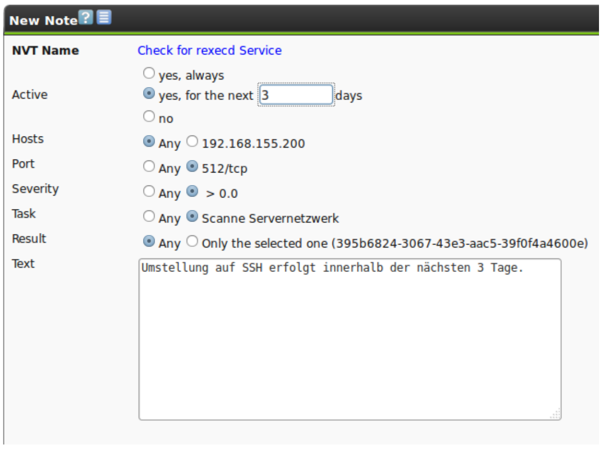
Fig. 7.42: Schedules allow time controlled scans.



Edit Schedule

Name	unnamed
Comment (optional)	
First Time	11 h 30 , 16 Feb 2014
Timezone	UTC
Period (optional)	0 hour(s)
Duration (optional)	0 hour(s)

Fig. 7.43: When creating a schedule various information must is required.



New Note

NVT Name	Check for rexecd Service
Active	○ yes, always ● yes, for the next 3 days ○ no
Hosts	● Any ○ 192.168.155.200
Port	○ Any ● 512/tcp
Severity	○ Any ● > 0.0
Task	○ Any ● Scanne Servernetzwerk
Result	● Any ○ Only the selected one (395b6824-3067-43e3-aac5-39f0f4a4600e)
Text	Umstellung auf SSH erfolgt innerhalb der nächsten 3 Tage.

Fig. 7.44: A new note

of information to a note that a security update is uploaded in the next seven days. For the next seven days the note will be displayed in the report that the vulnerability is being worked on.

7.6.2 Generalizing Notes

Any note can be generalized. In this example a quite extensive generalization is configured, matching any target host, port and task.

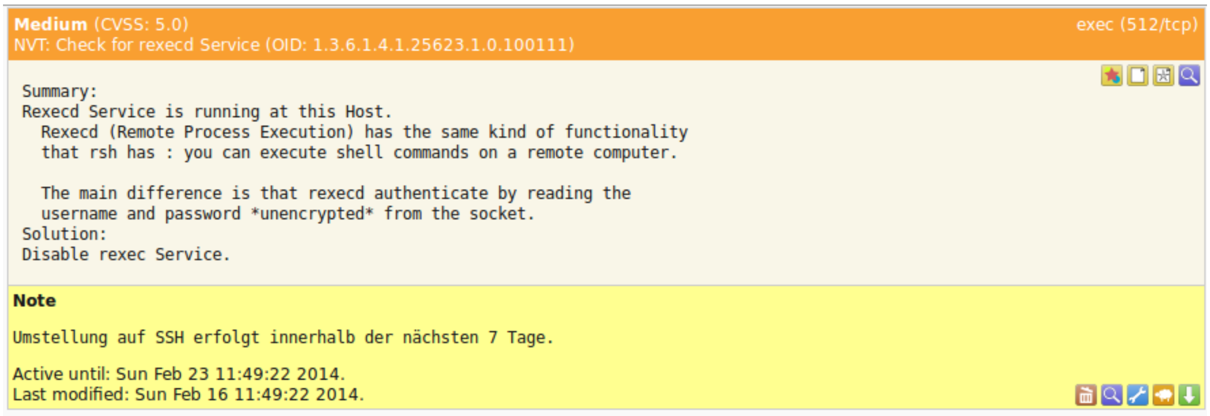
From this moment on the note is always shown in the results view if this NVT matches.

This applies for all previously created scan reports and for all future scan reports until the note is deleted.

7.6.3 Managing Notes

The created notes can be displayed under *Scan Management* and *Notes*. Here completely new notes can be added as well.

Among others it is being displayed if created notes are currently active. Additionally notes can be edited 🔧. To search for a specific note a search filter can be used respectively. This will make it easier to find a specific note when especially a great deal of notes is available. The search filter can be opened respectively end text entered appropriately or it can be entered directly into the filter window at the top. These filters can, of course, be saved for later use as well.



Medium (CVSS: 5.0) exec (512/tcp)
NVT: Check for rexecd Service (OID: 1.3.6.1.4.1.25623.1.0.100111)

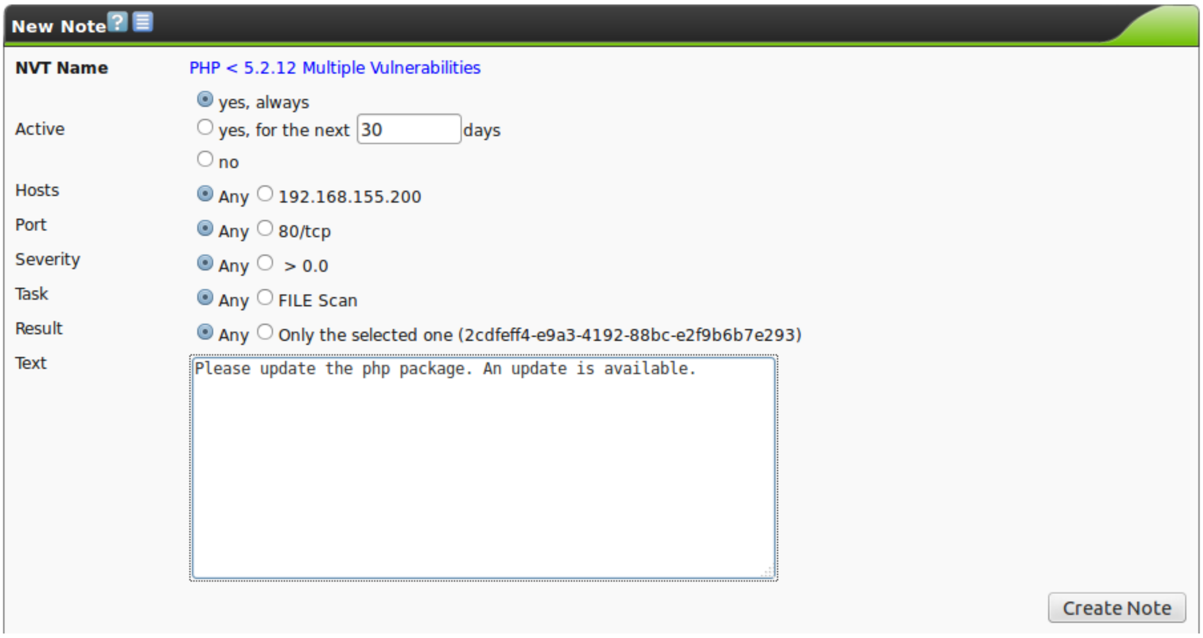
```
Summary:
Rexecd Service is running at this Host.
  Rexecd (Remote Process Execution) has the same kind of functionality
  that rsh has : you can execute shell commands on a remote computer.

  The main difference is that rexecd authenticate by reading the
  username and password *unencrypted* from the socket.
Solution:
Disable rexec Service.
```

Note

Umstellung auf SSH erfolgt innerhalb der nächsten 7 Tage.

Active until: Sun Feb 23 11:49:22 2014.
Last modified: Sun Feb 16 11:49:22 2014.

Fig. 7.45: A note in a report



New Note

NVT Name	PHP < 5.2.12 Multiple Vulnerabilities
Active	● yes, always ○ yes, for the next 30 days ○ no
Hosts	● Any ○ 192.168.155.200
Port	● Any ○ 80/tcp
Severity	● Any ○ > 0.0
Task	● Any ○ FILE Scan
Result	● Any ○ Only the selected one (2cdfeff4-e9a3-4192-88bc-e2f9b6b7e293)
Text	Please update the php package. An update is available.

Fig. 7.46: A generalized note

7.7 Overrides and False Positives

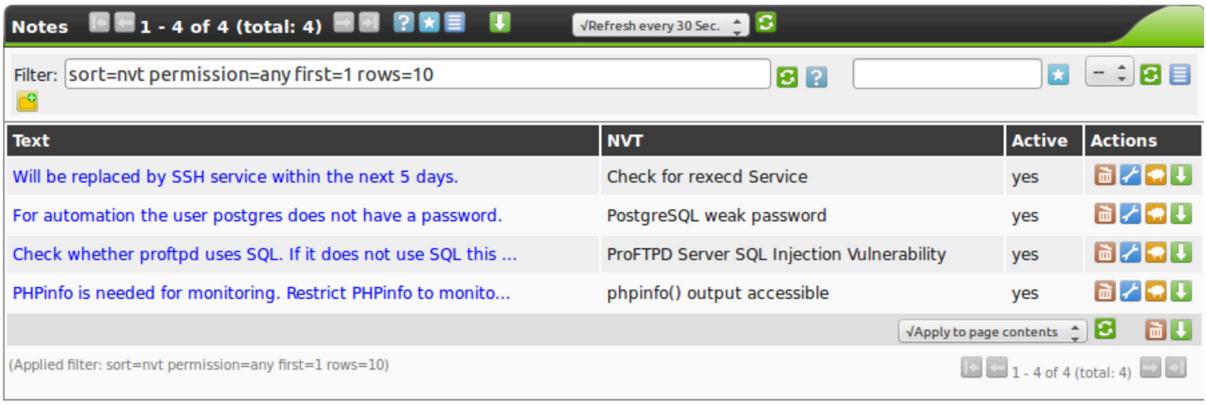
The results of a report can not only be supplemented through meaningful or helpful data but the severity of the results can be modified. This is called Override by the GSM.

These overrides are especially useful to manage results that are discovered as a false positive and that have been given a critical severity but should be given a different severity (i.e. False Positive) in the future. The same is true for results that only have been given the severity Log but should be assigned a higher severity locally. These can be managed with an override as well.

The use of overrides makes also sense to manage acceptable risks. The risk of a vulnerability can be ranked new and as such the risks that, in your opinion, are not critical can be re-evaluated in the results.

7.7.1 What is a false positive?

A false positive is a result that describes a problem that does not exist in reality. Often vulnerability scanners find proof that point to a security issue. A final prediction is not possible, however. Two

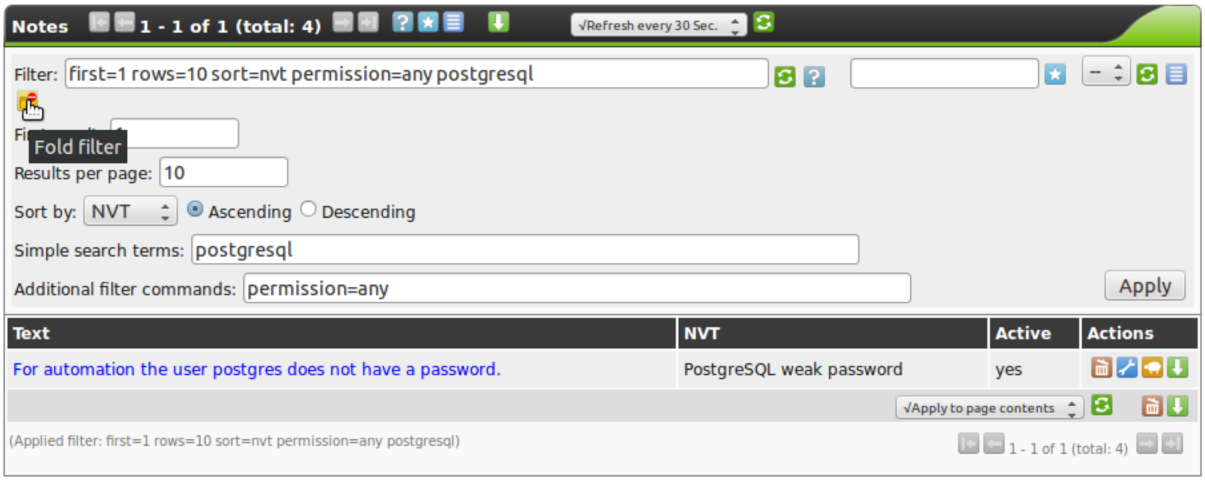


Filter: sort=nvt permission=any first=1 rows=10

Text	NVT	Active	Actions
Will be replaced by SSH service within the next 5 days.	Check for rexecd Service	yes	
For automation the user postgres does not have a password.	PostgreSQL weak password	yes	
Check whether proftpd uses SQL. If it does not use SQL this ...	ProFTPD Server SQL Injection Vulnerability	yes	
PHPinfo is needed for monitoring. Restrict PHPinfo to monito...	phpinfo() output accessible	yes	

(Applied filter: sort=nvt permission=any first=1 rows=10)

Fig. 7.47: Notes can be managed individually.



Filter: first=1 rows=10 sort=nvt permission=any postgresql

Results per page: 10

Sort by: NVT ● Ascending ○ Descending

Simple search terms: postgresql

Additional filter commands: permission=any

Text	NVT	Active	Actions
For automation the user postgres does not have a password.	PostgreSQL weak password	yes	

(Applied filter: first=1 rows=10 sort=nvt permission=any postgresql)

Fig. 7.48: Notes can be limited by a search filter.

options are now available:

- Reporting of a potentially non-existent vulnerability (False Positive).
- Omission of the reporting of the potentially existing vulnerability (False Negative).

Since a user is able to recognize, manage and handle these as it is not the case with false negatives, the GSM vulnerability scanner reports all potentially existing vulnerabilities. The GSM assists with several automatic and semi-automatic to categorize them.

Note: Consider the new concept of Quality of Detection (see sections *Reading of the Reports* (page 66) and *Network Vulnerability Tests* (page 188)).

This problem is especially typical with Enterprise Linux distributions. If, for example, a SSH service in version 4.4 is installed and the software reports this version during a connection attempt, a vulnerability scanner, that knows of a vulnerability in this version, will report this as such. The vendor potentially already addressed the vulnerability and released version 4.4-p1 that is already installed. This version still reports to the outside version 4.4 so that the vulnerability scanner cannot differentiate. If the scan administrator knows of this circumstance an override can ensure that these results are no longer being displayed.

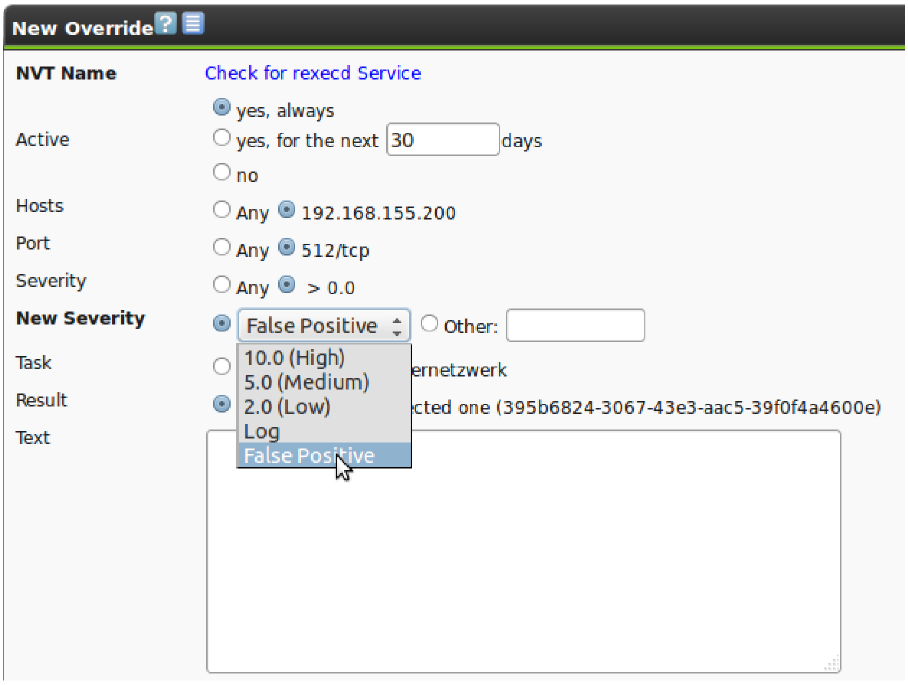
7.7.2 Creating an Override

Overrides like notes can be created in different ways. The simplest way to get to this option is through the respective scan result in a report. At the top right of each finding the *Add Override* icon can be found.

Overrides have the same function as notes, however, they add the possibility to adjust the severity:

- High
- Medium
- Low
- Log
- False Positive

Vulnerabilities with the level False Positive are not being displayed in the reports. But special reports for findings of this level can be created. As with overrides they can have a time limitation.



New Override

NVT Name	Check for rexecd Service
Active	● yes, always ○ yes, for the next 30 days ○ no
Hosts	○ Any ● 192.168.155.200
Port	○ Any ● 512/tcp
Severity	○ Any ● > 0.0
New Severity	● False Positive ○ Other:
Task	○ ernetzwerk
Result	● cted one (395b6824-3067-43e3-aac5-39f0f4a4600e)
Text	

Fig. 7.49: Overrides allow for the customization of the severity level.

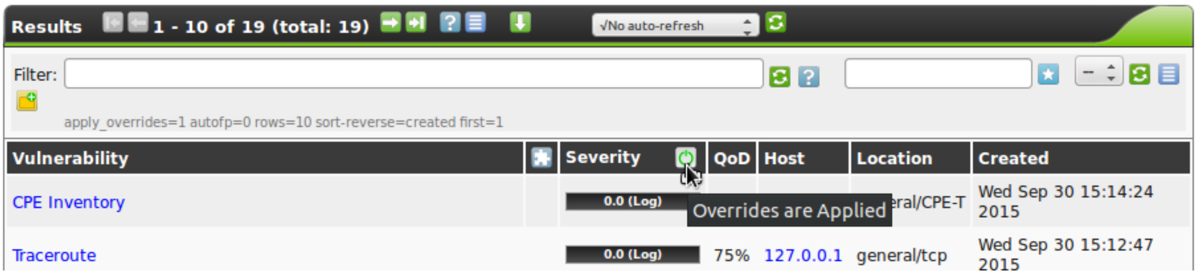
7.7.3 Disabling and Enabling Overrides

Whereever overrides may change the display of the results, the overrides may be enabled or disabled. This may be done using the icon in the title bar.

7.7.4 Automatic False Positives

The GSM is able to detect false positives automatically and can assign an override automatically. However the target system must be analyzed internally and externally with an authenticated scan.

An authenticated scan can identify vulnerabilities in locally installed software. As such vulnerabilities can be identified that can be exploited by local users or are available to an attacker if he already gained local access as an unprivileged user for example. In many cases an attack occurs in different phases and an attacker exploits multiple vulnerabilities to increase his privileges.



Results 1 - 10 of 19 (total: 19) √No auto-refresh

Filter:

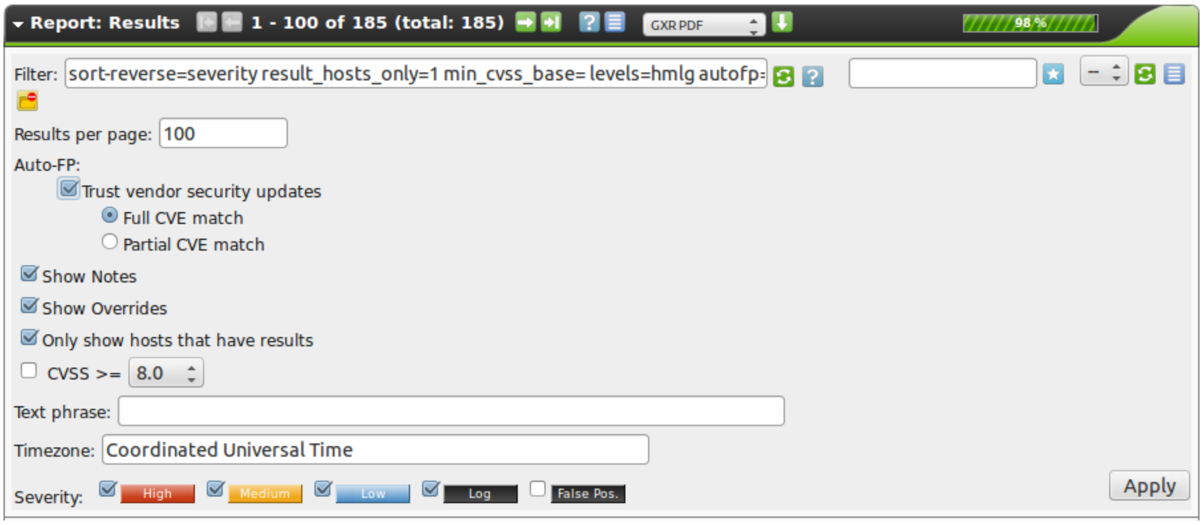
apply_overrides=1 autofp=0 rows=10 sort-reverse=created first=1

Vulnerability		Severity	QoD	Host	Location	Created
CPE Inventory		0.0 (Log)			ral/CPE-T	Wed Sep 30 15:14:24 2015
Traceroute		0.0 (Log)	75%	127.0.0.1	general/tcp	Wed Sep 30 15:12:47 2015

Overrides are Applied

Fig. 7.50: Overrides may be enabled and disabled.

An authenticated scan offers a second more powerful function justifying its execution. In many cases by scanning the system externally, it can not be properly identified if a vulnerability really exists. In doubt, the Greenbone Security Manager reports all potential vulnerabilities. With the authenticated scan many of these potential vulnerabilities can be recognized and filtered as false positives.



Report: Results 1 - 100 of 185 (total: 185) GXR PDF 98 %

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= levels=hmlg autofp=

Results per page: 100

Auto-FP:

☑ Trust vendor security updates

● Full CVE match

○ Partial CVE match

☑ Show Notes

☑ Show Overrides

☑ Only show hosts that have results

□ CVSS >= 8.0

Text phrase:

Timezone: Coordinated Universal Time

Severity: ☑ High ☑ Medium ☑ Low ☑ Log □ False Pos.

Apply

Fig. 7.51: Automatic False Positives

This problem is especially typical with Enterprise Linux distributions. If, for example, a SSH service in version 4.4 is installed and the software reports this version during a connection attempt, a vulnerability scanner, that knows of a vulnerability in this version, will report this as such. The vendor potentially already addressed the vulnerability and released version 4.4-p1 that is already installed. This version still reports to the outside version 4.4 so that the vulnerability scanner cannot differentiate. If an authenticated scan was performed the GSM can recognize that the version 4.4-p1 is installed and no longer contains this vulnerability.

Automatic false positives are enabled with the Report-Filter function (see section *Powerfilter* (page 139)). This functionality gives the best results when using the `Partial CVE match`.

7.8 Scanning Web Applications

The Greenbone Security Manager supports scanning of web applications in two ways:

- With our own Network Vulnerability Tests (NVTs, over 1500 are of some relevance for web applications).
- With connected web applications scanners like the built-in scanner w3af

Using the NVTs, basically all that are relevant for web applications are already selected with the default scan configurations.

Alternatively you can narrow down the scope of the scan configuration to focus on web applications only. An example is available for download which just needs to be imported as a new scan configuration: http://greenbone.net/download/web-app-scan.xml

Note: If you are only interested in the actual web service, you can change the target's port list to cover only port 80 and/or 443.

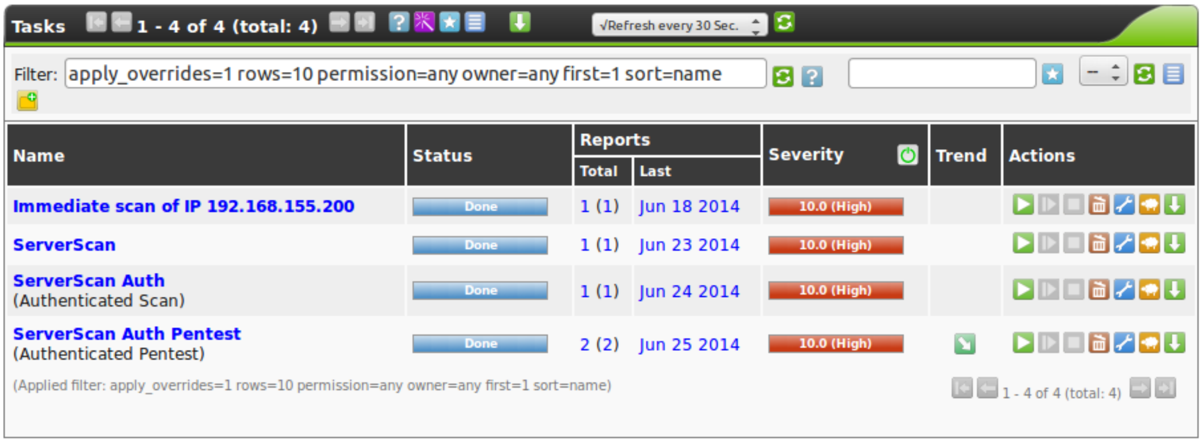
There are various fine-tuning preferences available for the scan configuration.

CHAPTER 8

Reports

The GSM saves all reports of all scans in a local database. Not only is the last report of a scan saved but all reports of all scans ever run. This allows also access to information from the past. The reports contain the discovered vulnerabilities and information of a scan (see section *Reports* (page 63)).

If a scan has been performed multiple times the trend of discovered vulnerabilities will be displayed. However, the trend information can not be found on the report page but under *Scan Management/Tasks*.



Filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=name

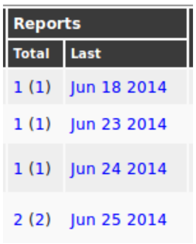
Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 192.168.155.200	Done	1 (1)	Jun 18 2014	10.0 (High)		
ServerScan	Done	1 (1)	Jun 23 2014	10.0 (High)		
ServerScan Auth (Authenticated Scan)	Done	1 (1)	Jun 24 2014	10.0 (High)		
ServerScan Auth Pentest (Authenticated Pentest)	Done	2 (2)	Jun 25 2014	10.0 (High)	↘	

(Applied filter: apply_overrides=1 rows=10 permission=any owner=any first=1 sort=name)

1 - 4 of 4 (total: 4)

Fig. 8.1: The trend of discovered vulnerabilities can be found in the respective column in the task overview.

In this view only reports of a specific scan can be accessed. To do so use the column Reports/Total (see figure *The Reports column contains the amount of reports saved in total and the date of the last report.* (page 87)).



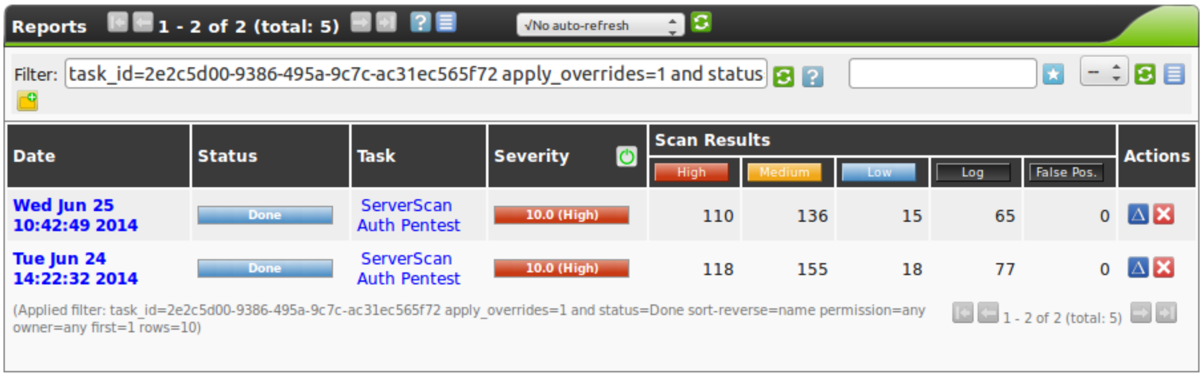
Reports	
Total	Last
1 (1)	Jun 18 2014
1 (1)	Jun 23 2014
1 (1)	Jun 24 2014
2 (2)	Jun 25 2014

Fig. 8.2: The Reports column contains the amount of reports saved in total and the date of the last report.

Here you can find the date of the last saved report as well as the amount of reports available in total. The first value represents the number of all completed scans and the second the amount of reports including the not yet completed ones. By clicking on one of the values you will get a list of the respective reports. By clicking on the date the latest report will be displayed.

8.1 Delta Reports

If more than one report of a task can be displayed (see *Now, for comparison the second report needs to be selected.* (page 88)) a Delta-Report can be created. Use the compare △ option in the Action column. The first report is being selected for comparison.



Reports 1 - 2 of 2 (total: 5) √No auto-refresh

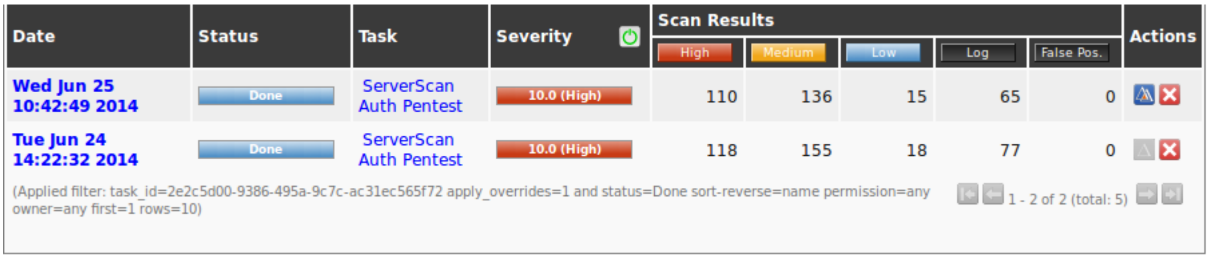
Filter: task_id=2e2c5d00-9386-495a-9c7c-ac31ec565f72 apply_overrides=1 and status

Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Wed Jun 25 10:42:49 2014	Done	ServerScan Auth Pentest	10.0 (High)	110	136	15	65	0	△ ✕
Tue Jun 24 14:22:32 2014	Done	ServerScan Auth Pentest	10.0 (High)	118	155	18	77	0	△ ✕

(Applied filter: task_id=2e2c5d00-9386-495a-9c7c-ac31ec565f72 apply_overrides=1 and status=Done sort-reverse=name permission=any owner=any first=1 rows=10) 1 - 2 of 2 (total: 5)

Fig. 8.3: Two reports of the same task can be compared in a delta report.

Afterwards the respective icon is greyed out for the selected report. The compare icons of the other reports have now changed in their appearance. Use the △ icon to select the second report for comparison.



Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Wed Jun 25 10:42:49 2014	Done	ServerScan Auth Pentest	10.0 (High)	110	136	15	65	0	△ ✕
Tue Jun 24 14:22:32 2014	Done	ServerScan Auth Pentest	10.0 (High)	118	155	18	77	0	✕

(Applied filter: task_id=2e2c5d00-9386-495a-9c7c-ac31ec565f72 apply_overrides=1 and status=Done sort-reverse=name permission=any owner=any first=1 rows=10) 1 - 2 of 2 (total: 5)

Fig. 8.4: Now, for comparison the second report needs to be selected.

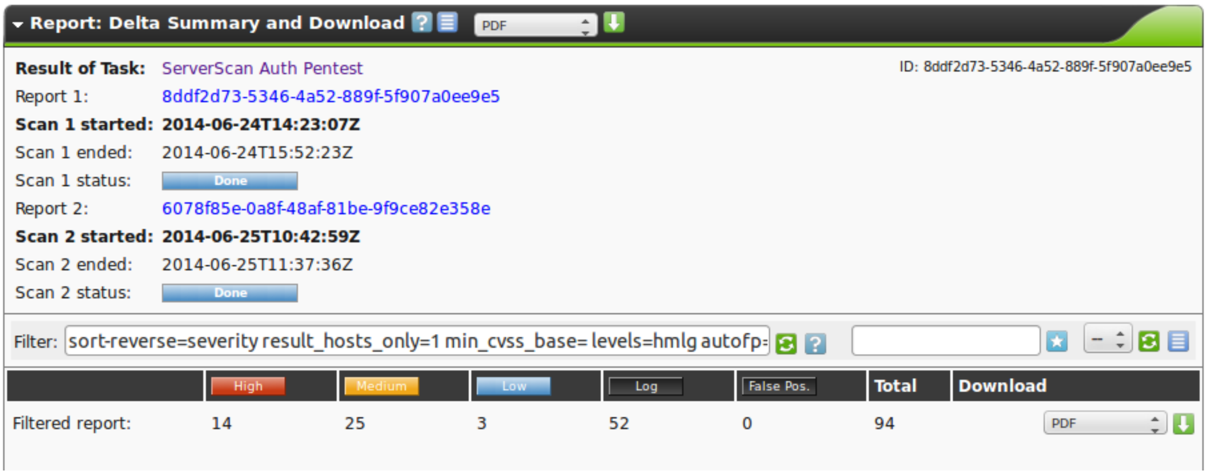
Subsequently you will receive the delta report. As usual, it can be displayed in different formats and exported as PDF.

The report contains information as to which run times are being compared with each other and how many results have been added or were removed.

8.2 Report Plugins

Report plugins are defined as the formats a report is created from, based on the scan results. This ranges from PDF documents as per corporate identity to interactive reports like the Greenbone Security Explorer. These plugins can be used to export report information into other document formats so they can be processed by other third party applications (Connectors).

The name of the exported report is configurable in the user settings (see section *My Settings* (page 185)). Greenbone supports the creation of additional plugins. Requests, suggestions and concrete templates are welcome.



Report: Delta Summary and Download PDF

Result of Task: ServerScan Auth Pentest

ID: 8ddf2d73-5346-4a52-889f-5f907a0ee9e5

Report 1: 8ddf2d73-5346-4a52-889f-5f907a0ee9e5

Scan 1 started: 2014-06-24T14:23:07Z

Scan 1 ended: 2014-06-24T15:52:23Z

Scan 1 status: Done

Report 2: 6078f85e-0a8f-48af-81be-9f9ce82e358e

Scan 2 started: 2014-06-25T10:42:59Z

Scan 2 ended: 2014-06-25T11:37:36Z

Scan 2 status: Done

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= levels=hmlg autofp=

	High	Medium	Low	Log	False Pos.	Total	Download
Filtered report:	14	25	3	52	0	94	PDF

Fig. 8.5: The delta report can be exported as PDF as well.

The report plugin framework has the following properties:

Simple Import/Export: A report plugin is always a single XML file. The import is easily performed (see section *Import of additional plugins* (page 91)).

Parameterized: Plugins can contain parameters that can be customized to specific requirements in the graphical interface.

Content Type: For every plugin it is determined of which type the result is. The well-known HTTP descriptors are being used, for example, `application/pdf`, `graphics/png` or `text/plain`. Depending on the content type the plugins are displayed in contextual relation. For example, the types `text/*` for the sending as email inline.

Signature Support: Through the Greenbone Security Feed signatures for trusted plugins are being provided. That way it can be verified that an imported plugin was verified by Greenbone.

The Reports can be exported in different formats:

ARF: Asset Reporting Format v1.0.0 This format creates a report that represents the NIST Asset Reporting Format.

CPE - Common Enumeration CSV Table This report selects all CPE tables and creates a single comma separated file.

CSV hosts This report creates a comma separated file containing the systems discovered.

CSV Results This report creates a comma separated file with the results of a scan.

GSR PDF - Greenbone Security Report (recommended) This is the complete Greenbone Security report with all vulnerabilities in graphical format as a PDF file. The topology graph is not included when more than 100 hosts are covered in the report. The language is English.

GXR PDF - Greenbone Executive Report (recommended) This is a shortened report with all vulnerabilities in graphical format as a PDF file for management. The topology graph is not included when more than 100 hosts are covered in the report. The language of the report is in English.

HTML This report is in HTML format and as such can be opened in a web browser. It is a detailed listing containing the complete description of vulnerabilities including note and overrides with all references and cross references. It is a neutral document without any further references to Greenbone or the Greenbone Security Manager. The document can also be used offline and the language being used is English.

ITG - IT-Grundschutz catalogue This report is guided by the BSI IT-Grundschutz catalogue. It provides an overview of the discovered results in table view in CSV format and in German.

LaTeX This report is offered as LaTeX source text. The language is English.

NBE This is the old OpenVAS/Nessus report format. It does not have support for notes, overrides and some additional information.

PDF This is a complete report in PDF. Like the HTML format it is neutral. The language is English.

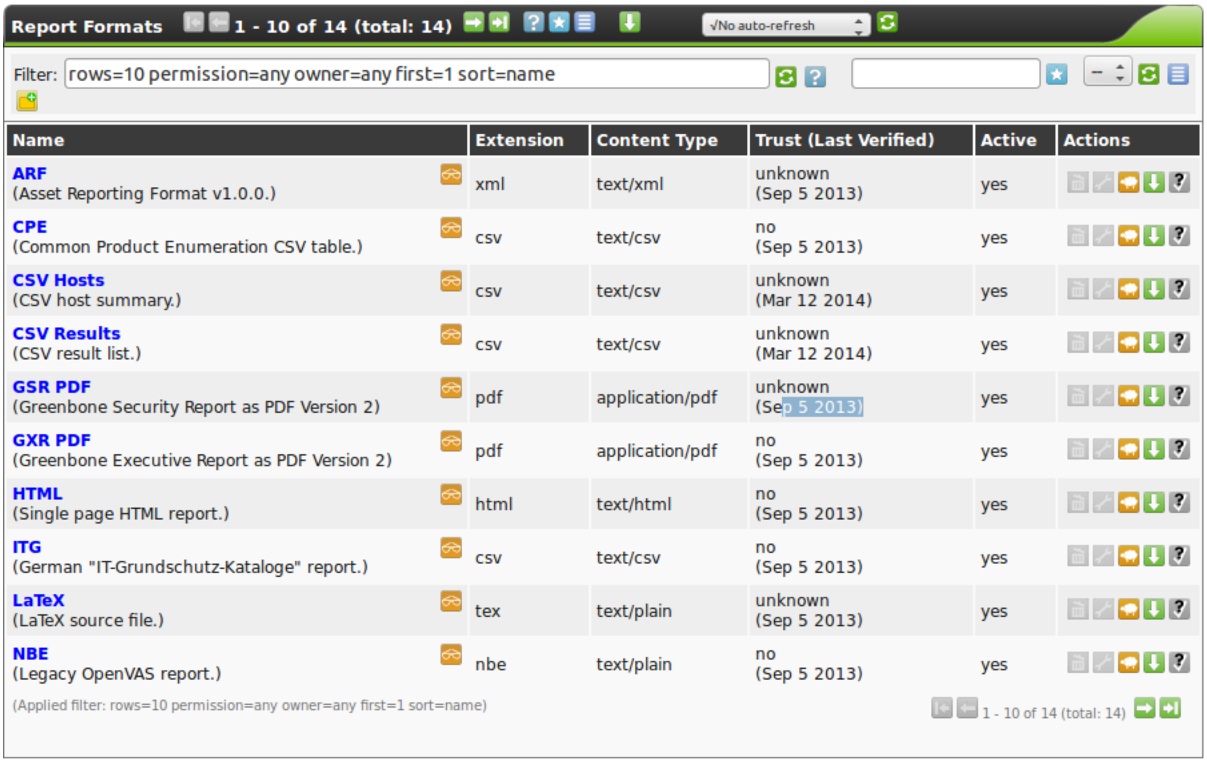
Topology SVG This presents the results in a SVG picture.

TXT This creates a text file. This format is especially useful when being sent by Email. The language is English.

Verinice ISM Creates an import file for the ISMS tool *Verinice*.

Verinice ITG Creates an import file for the ISMS tool *Verinice*.

XML The report is being exported in the native xml format. Contrary to the other formats this format contains all results and does not format them at all.



Report Formats 1 - 10 of 14 (total: 14) √No auto-refresh

Filter: rows=10 permission=any owner=any first=1 sort=name

Name	Extension	Content Type	Trust (Last Verified)	Active	Actions
ARF (Asset Reporting Format v1.0.0.)	xml	text/xml	unknown (Sep 5 2013)	yes	
CPE (Common Product Enumeration CSV table.)	csv	text/csv	no (Sep 5 2013)	yes	
CSV Hosts (CSV host summary.)	csv	text/csv	unknown (Mar 12 2014)	yes	
CSV Results (CSV result list.)	csv	text/csv	unknown (Mar 12 2014)	yes	
GSR PDF (Greenbone Security Report as PDF Version 2)	pdf	application/pdf	unknown (Sep 5 2013)	yes	
GXR PDF (Greenbone Executive Report as PDF Version 2)	pdf	application/pdf	no (Sep 5 2013)	yes	
HTML (Single page HTML report.)	html	text/html	no (Sep 5 2013)	yes	
ITG (German "IT-Grundschutz-Kataloge" report.)	csv	text/csv	no (Sep 5 2013)	yes	
LaTeX (LaTeX source file.)	tex	text/plain	unknown (Sep 5 2013)	yes	
NBE (Legacy OpenVAS report.)	nbe	text/plain	no (Sep 5 2013)	yes	

(Applied filter: rows=10 permission=any owner=any first=1 sort=name)

1 - 10 of 14 (total: 14)

Fig. 8.6: Greenbone includes many report plugins by default.

The report plugins define the format of the reports to be exported. Many report plugins reduce the available data in order to display it in a meaningful way. However, the native GSM xml format contains all data and can be used to import exported reports on another GSM. To do so use the Container Task (see also section *Container Task* (page 63)).

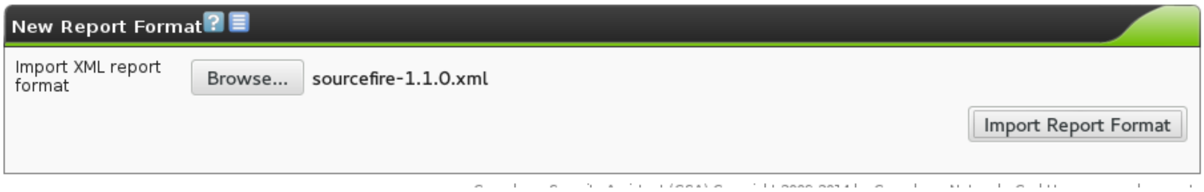
The overview (see figure *Greenbone includes many report plugins by default.* (page 90)) shows additional details of the report plugins. For every plugin in the individual columns the following information is being displayed:

Extension: The file name of the downloaded report through the respective plugin is comprised of the UUID (unique internal ID of the report) and this extension. Among others, the extension supports the browser to start a compatible application in case the specified content type is not recognized.

Content Type: The content type specifies the format in use and is being transmitted when being downloaded. That way a compatible application can be launched by the browser directly. Additionally the content type is important internally: It is being used to offer suitable plugins within its context. For example, when sending a report via Email all plugins of the type `text/\*` are being offered as they can be embedded in an email in a humanly readable way.

Trust: Some plugins only consist of a data transformation while others execute more complex operations and also use support programs. To avoid misuse the plugins are digitally signed. If the signature is authentic and the publisher trusted, it is ensured that the plugin exists in the exact format as certified by the publisher. The verification does not occur automatically rather than manually with the verify icon ☑. The date of the verification is saved automatically. This function should definitely be used for all newly imported plugins before they are being activated. This is not required for the supplied default plugins ?.

Active: The plugins are only available in the respective selection menus if they were activated. Newly imported plugins are always deactivated at first.



New Report Format

Import XML report format	Browse...	sourcefire-1.1.0.xml

Import Report Format

Fig. 8.7: New report formats plugins can be imported easily.

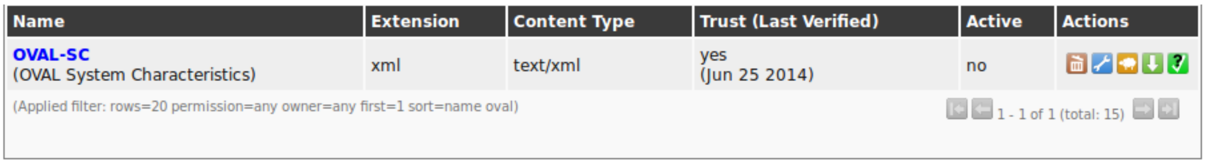
8.2.1 Import of additional plugins

Other report formats can be imported easily. Greenbone offers the following additional report format plugins on the following web page: http://greenbone.net/technology/report_formats.html:

- Sourcefire Host Input Import (see also section *Sourcefire Defence Center* (page 218))
- OVAL System Characteristics
- OVAL System Characteristics Archive

Note: The report format plugins for the verinice connector are now already shipped with the Greenbone operating system. They do not need to be manually imported anymore.

To import a report plugin the respective xml file must be downloaded from Greenbone. Afterwards change to *Configuration/Report Formats*. Select the icon ★ to add the new format.

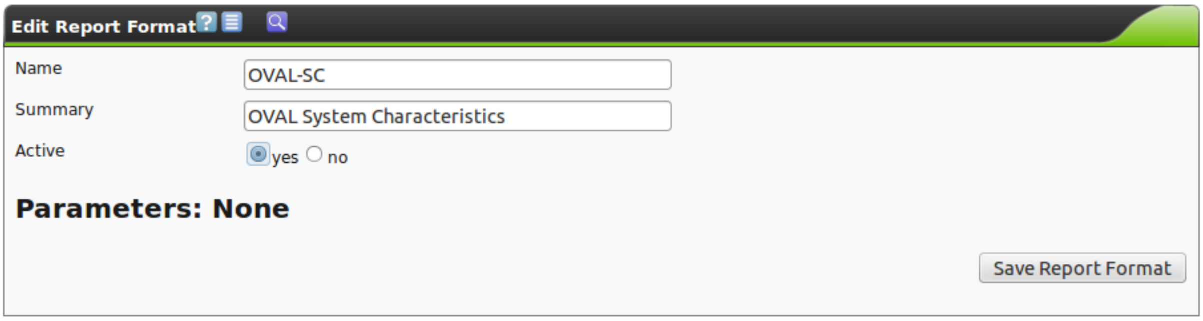


Name	Extension	Content Type	Trust (Last Verified)	Active	Actions
OVAL-SC (OVAL System Characteristics)	xml	text/xml	yes (Jun 25 2014)	no	

(Applied filter: rows=20 permission=any owner=any first=1 sort=name oval)

1 - 1 of 1 (total: 15)

Fig. 8.8: Imported formats should be verified before activation.



Edit Report Format

Name	OVAL-SC
Summary	OVAL System Characteristics
Active	● yes ○ no

Parameters: None

Save Report Format

Fig. 8.9: New report formats plugins can be activated easily.

Select the respective file and then import the format. After importing the new format is not active yet. Report plugins can be signed by the publisher. This signature should get verified before activation. This verification is being done automatically when importing. The result with the date of the verification is being displayed in the Trust column. If the report plugin is trusted it can be activated afterwards. To do so, edit the report plugin by clicking the edit icon in the Actions column.

CHAPTER 9

Compliance and special scans

Compliance in the IT security world is the primary approach for organizations to keep their information and assets protected and secure.

With cybercrime on the rise, governments see the need to protect their citizens and pass rules and regulations on privacy and IT security in the hopes to protect our identities and assets. Information Security bodies such as the Information Systems Audit and Control Association (ISACA) or the International Organization for Standardization (ISO) publish IT security standards, frameworks and guidelines such as the Control Objectives for Information and Related Technology (COBIT) or the ISO 27000 series which cover information security standards. The German Federal Office for Security in Information Technology (BSI), for example, publishes the IT Baseline Protection Catalogs, or IT-Grundschutz-Kataloge. This is a collection of documents that provide useful information for detecting weaknesses and combating attacks on IT environments. To better protect against credit card data theft the Payment Card Industry Security Standards Council publishes the payment Card Industry Data Security Standard (PCI DSS).

All these privacy laws, standards, frameworks, rules and regulations are to force and assist organizations to implement the appropriate safeguards to protect themselves and their information assets from attacks. In order to implement these laws, standards, frameworks, rules and regulations within an organization the organization will have to create an IT security framework consisting of policies, standards, baselines, guidelines and detailed procedures.

Security scanners such as the Greenbone Security Manager (GSM) can assist IT security professionals to check their IT security safeguards against the aforementioned regulations, standards and frameworks for compliance.

In the following sections we will describe how the GSM can be utilized to perform certain compliance checks.

9.1 Generic Policy Scans

When performing policy scans there are several groups each with four NVTs that can be configured accordingly. In the policy section of the NVTs database at least two of these four policy NVTs are required to run a policy scan. The four NVT types are:

- ***Base*** This NVT performs the actual scan/function of the actual policy scan.
- ***Matches*** This NVT summarizes any items which match the checks performed by the base NVT.
- ***Violations*** This NVT summarizes any items which did not match the checks performed by the base NVT.
- ***Errors*** This NVT sumarizes any items where some error occurred when running the policy scan.

The base NVT must be selected for a policy check since it performs the actual tests. The other three plugins may be selected according to your needs. For example, if matching patterns are of no concern then only the violations plugin should be selected additionally.

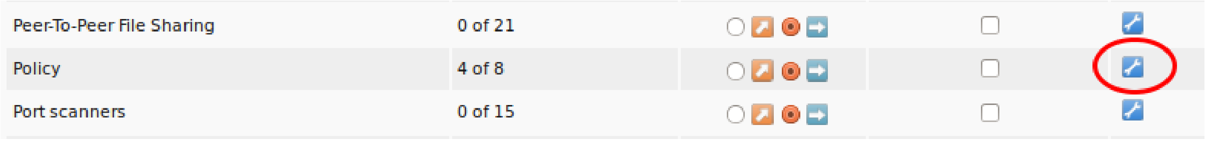
9.1.1 File Content

File content checks belong to policy audits which don't explicitly test for vulnerabilities but rather test the compliance of file contents (e.g. configuration files) regarding a given policy.

GSM provides a policy module to check if a file content is compliant with a given policy.

In general this is an authenticated check, i.e. the scan engine will have to log into the target system to perform the check.

The file content check can only be performed on systems supporting the command `grep`. Normally this means Linux or Linux-like systems.



Peer-To-Peer File Sharing	0 of 21	○	□	
Policy	4 of 8	○	□	
Port scanners	0 of 15	○	□	

Fig. 9.1: The NVT's are in the „Policy“ family

Four different NVT's provide the file content check:

- *File Content*: This NVT performs the actual file content check.
- *File Content: Matches*: This NVT shows the patterns and files which passed the file content check (the predefined pattern matches in the file)
- *File Content: Violations*: This NVT shows the patterns and files which didn't pass the file content check (the predefined pattern doesn't match in the file)
- *File Content: Errors*: This NVT shows the files where some error occurred (e.g. the file is not found on the target system)

The NVT *File Content* must be selected for a file content check since it performs the actual tests. The other three plugins may be selected according to your needs. E.g. if just not matching patterns are of concern then only the plugin *File Content: Violations* should be additionally selected.

Patterns

A reference file with the patterns to check and some other entries must be created. Following is an example:

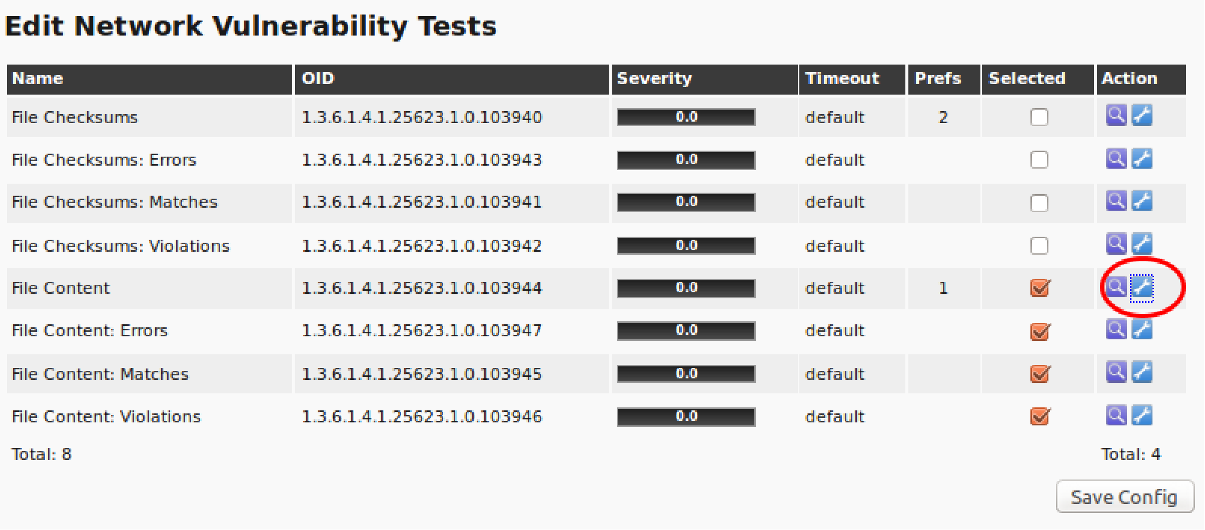
```
filename|pattern|presence/absence
/tmp/filecontent_test|^paramter1=true.*$|presence
/tmp/filecontent_test|^paramter2=true.*$|presence
/tmp/filecontent_test|^paramter3=true.*$|absence
/tmp/filecontent_test_notthere|^paramter3=true.*$|absence
```

This file must contain the row *filename|pattern|presence/absence*. The subsequent rows contain each a test entry. Each row contains three elements which are separated by `|`. The first field contains the path and file name, the second field the pattern to check and the third field indicates if a pattern has to be present or absent.

The pattern to check, the second element in the row, is defined as a regular expression and will be checked in the file accordingly.

Select the file with *Browse* and select *Upload file*. The file upload will be started by clicking *Save Config*.

By clicking on the ⬇ icon it is possible to download the already uploaded reference file. Select *Replace existing file with:* to upload a new reference file. The possibilities to change is only available if the scan configuration is not in use. This is done to ensure immutable audit-compliant scan results.

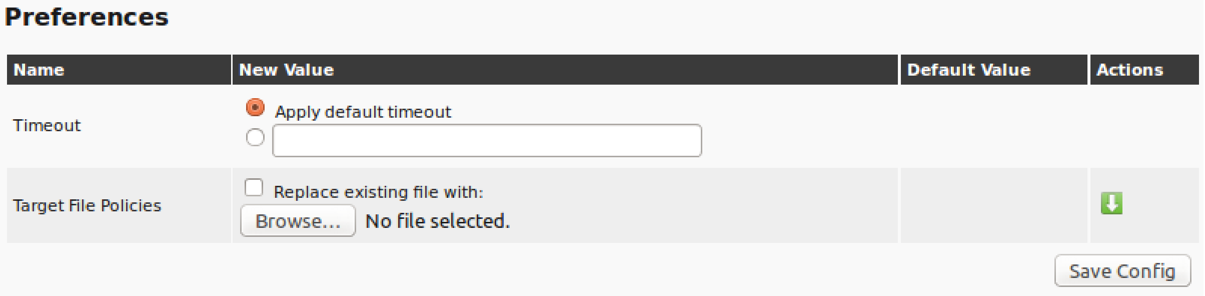


Edit Network Vulnerability Tests

Name	OID	Severity	Timeout	Prefs	Selected	Action
File Checksums	1.3.6.1.4.1.25623.1.0.103940	0.0	default	2	☐	
File Checksums: Errors	1.3.6.1.4.1.25623.1.0.103943	0.0	default		☐	
File Checksums: Matches	1.3.6.1.4.1.25623.1.0.103941	0.0	default		☐	
File Checksums: Violations	1.3.6.1.4.1.25623.1.0.103942	0.0	default		☐	
File Content	1.3.6.1.4.1.25623.1.0.103944	0.0	default	1	☑	
File Content: Errors	1.3.6.1.4.1.25623.1.0.103947	0.0	default		☑	
File Content: Matches	1.3.6.1.4.1.25623.1.0.103945	0.0	default		☑	
File Content: Violations	1.3.6.1.4.1.25623.1.0.103946	0.0	default		☑	
Total: 8						Total: 4

Save Config

Fig. 9.2: Afterwards import this file in the properties of the NVT



Preferences

Name	New Value	Default Value	Actions
Timeout	● Apply default timeout ○		
Target File Policies	☐ Replace existing file with: Browse... No file selected.		

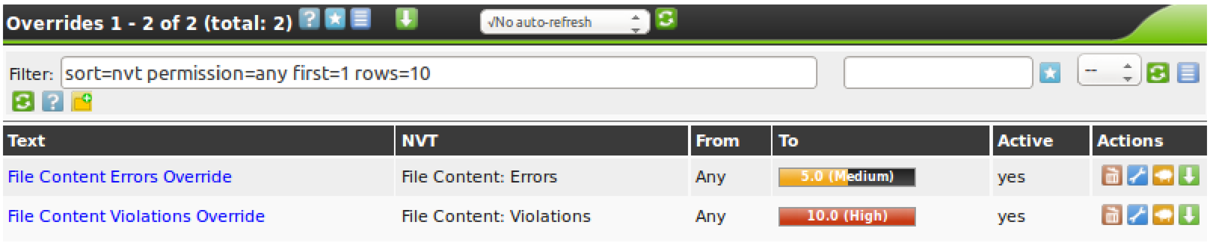
Save Config

Fig. 9.3: The mask will change if there is already a file uploaded

Severity

The file content tests report any result per default as log messages. By sectioning the reporting plugins in three different NVT's it is now possible to create distinct overrides on the severity according your needs.

In the following picture the severities of *File Content: Violations* and *File Content: Errors* have been changed which will be shown in the reports accordingly.



Overrides 1 - 2 of 2 (total: 2)

√No auto-refresh

Filter: sort=nvt permission=any first=1 rows=10

Text	NVT	From	To	Active	Actions
File Content Errors Override	File Content: Errors	Any	5.0 (Medium)	yes	
File Content Violations Override	File Content: Violations	Any	10.0 (High)	yes	

Example

Here (policy_file_content_example.xml[11]) is an example scan configuration with all the relevant NVT's for the file content test to download. The corresponding test file (filecontent_test[12]) should be downloaded and extracted to the /tmp/ directory on the target system.

[11] http://www.greenbone.net/download/scanconfigs/policy_file_content_example.xml

[12] http://www.greenbone.net/download/misc/filecontent_test

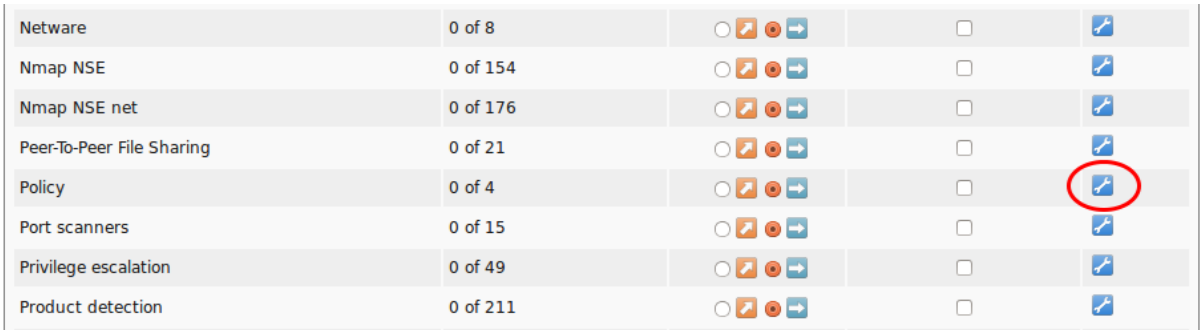
Now create an new task and start it for the target system where you saved test files. Please note that this has to be an authenticated scan with the appropriate SSH Credentials.

The overrides can be created either before or after a scan. The latter is easier since you can create the appropriate reference through a simple click in the result page.

9.1.2 Registry Content

The registry is a database in Windows that contains important information about system hardware, installed programs and settings, and profiles of each of the user accounts on your computer. Windows continually refers to the information in the registry [106].

Due to the nature of the Windows registry every program/application installed under windows will register itself in the Windows registry and as such has a registry entry. Even malware and other malicious code usually leaves traces within the windows registry. The registry now can be utilized to search for specific application or malware related information such as version levels and numbers. Also missing or changed registry settings could point to a potential security policy violation on an endpoint. GSM provides a policy auditing module to verify registry entries on target systems. This module checks for the presence or absence of registry settings as well as registry violations. Since the registry is unique to Windows systems this check can only be run on Windows systems. To access the registry on the target system the check needs to authenticate on the target system.



Netware	0 of 8	○	□
Nmap NSE	0 of 154	○	□
Nmap NSE net	0 of 176	○	□
Peer-To-Peer File Sharing	0 of 21	○	□
Policy	0 of 4	○	□
Port scanners	0 of 15	○	□
Privilege escalation	0 of 49	○	□
Product detection	0 of 211	○	□

Fig. 9.4: The NVT's are in the „Policy" family.

Four different NVT's provide the registry content check:

- *Windows Registry Check*: This NVT performs the actual registry content check on the files.
- *Windows Registry Check: OK*: This NVT shows the registry setting which passed the registry check (registry content OK).
- *Windows Registry Check: Violations*: This NVT shows the registry content which didn't pass the registry check (wrong registry content).
- *Windows Registry Check: Errors*: This NVT shows the registry entries where some error occurred (e.g. registry content not found on the target system).

The plugin *Windows Registry Check* must be selected for a registry check since it performs the actual tests. The other three plugins may be selected according to the needs. E.g. just entries with wrong regsitry content are of concern then only the plugin *Windows Registry Check: Violations* should be additionally selected.

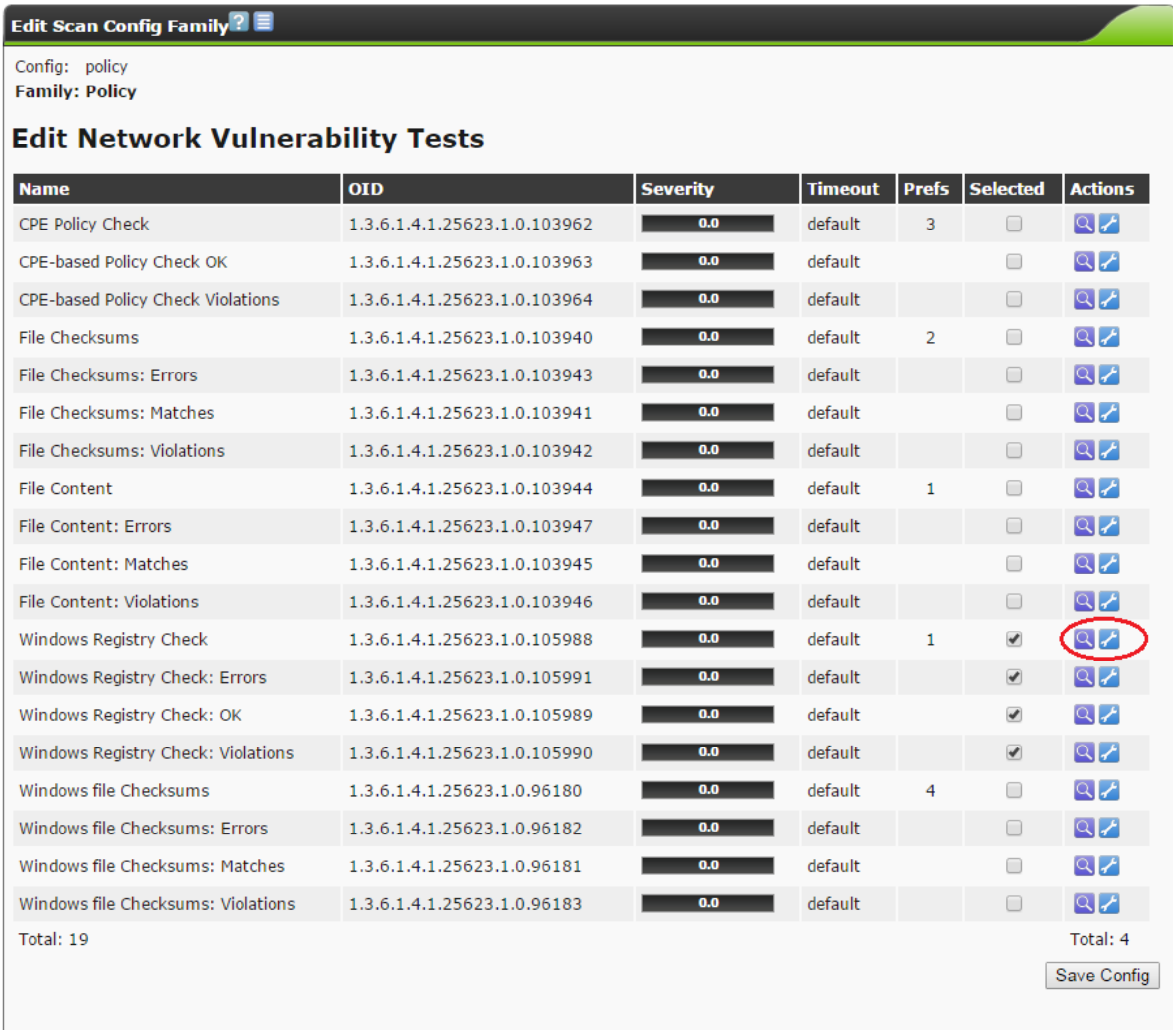
Registry Content Pattern

A file with the reference registry content must be created: Following is an example:

[106] http://windows.microsoft.com/en-ca/windows-vista/what-is-the-registry

```
Present|Hive|Key|Value|ValueType|ValueContent
TRUE|HKLM|SOFTWARE\Macromedia\FlashPlayer\SafeVersions|8.0|REG_DWORD|33
TRUE|HKLM|SOFTWARE\Microsoft\Internet Explorer
TRUE|HKLM|SOFTWARE\Microsoft\Internet Explorer|Version|REG_SZ|9.11.10240.16384
TRUE|HKLM|SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system|DWORD:
    LocalAccountTokenFilterPolicyREG_DWORD|1
FALSE|HKLM|SOFTWARE\Virus
TRUE|HKLM|SOFTWARE\ShouldNotBeHere
```

This file must contain the row *Present|Hive|Key|Value|ValueType|ValueContent*. The subsequent rows contain each a test entry. Each row contains a regsitry entry to be checked. Each row contains six elements which are separated by `|`. The first field sets if a registry entry should be present or not, the second the hive the registry entry is located in, the third the key, the fourth the value, the fifth the value type and the sixth the value content.



Edit Scan Config Family

Config: policy
Family: Policy

Edit Network Vulnerability Tests

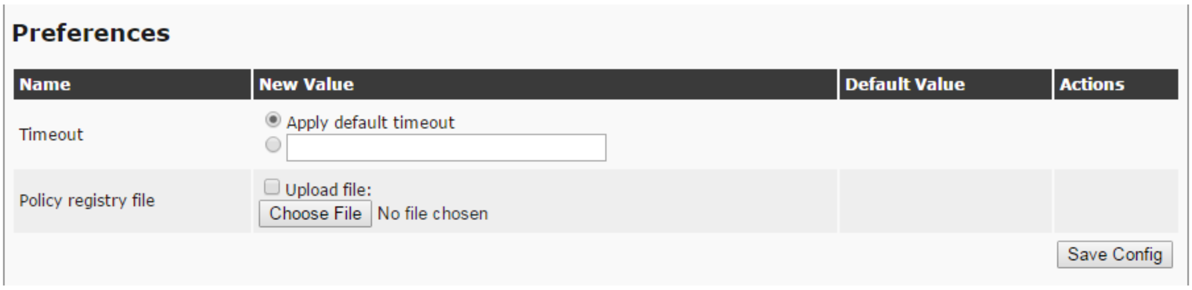
Name	OID	Severity	Timeout	Prefs	Selected	Actions
CPE Policy Check	1.3.6.1.4.1.25623.1.0.103962	0.0	default	3	☐	🔍 🔧
CPE-based Policy Check OK	1.3.6.1.4.1.25623.1.0.103963	0.0	default		☐	🔍 🔧
CPE-based Policy Check Violations	1.3.6.1.4.1.25623.1.0.103964	0.0	default		☐	🔍 🔧
File Checksums	1.3.6.1.4.1.25623.1.0.103940	0.0	default	2	☐	🔍 🔧
File Checksums: Errors	1.3.6.1.4.1.25623.1.0.103943	0.0	default		☐	🔍 🔧
File Checksums: Matches	1.3.6.1.4.1.25623.1.0.103941	0.0	default		☐	🔍 🔧
File Checksums: Violations	1.3.6.1.4.1.25623.1.0.103942	0.0	default		☐	🔍 🔧
File Content	1.3.6.1.4.1.25623.1.0.103944	0.0	default	1	☐	🔍 🔧
File Content: Errors	1.3.6.1.4.1.25623.1.0.103947	0.0	default		☐	🔍 🔧
File Content: Matches	1.3.6.1.4.1.25623.1.0.103945	0.0	default		☐	🔍 🔧
File Content: Violations	1.3.6.1.4.1.25623.1.0.103946	0.0	default		☐	🔍 🔧
Windows Registry Check	1.3.6.1.4.1.25623.1.0.105988	0.0	default	1	☑	🔍 🔧
Windows Registry Check: Errors	1.3.6.1.4.1.25623.1.0.105991	0.0	default		☑	🔍 🔧
Windows Registry Check: OK	1.3.6.1.4.1.25623.1.0.105989	0.0	default		☑	🔍 🔧
Windows Registry Check: Violations	1.3.6.1.4.1.25623.1.0.105990	0.0	default		☑	🔍 🔧
Windows file Checksums	1.3.6.1.4.1.25623.1.0.96180	0.0	default	4	☐	🔍 🔧
Windows file Checksums: Errors	1.3.6.1.4.1.25623.1.0.96182	0.0	default		☐	🔍 🔧
Windows file Checksums: Matches	1.3.6.1.4.1.25623.1.0.96181	0.0	default		☐	🔍 🔧
Windows file Checksums: Violations	1.3.6.1.4.1.25623.1.0.96183	0.0	default		☐	🔍 🔧

Total: 19 Total: 4

Fig. 9.5: Afterwards import this file in the properties of the NVT.

Select the file with *Browse* and select *Upload file*. The file upload will be started by clicking *Save Config*.

By clicking on the ⬇ icon it is possible to download the already uploaded reference file. Select *Replace existing file with:* to upload a new reference file. The option to change is only available if the scan configuration is not in use. This is done to ensure immutable audit-compliant scan results.



Preferences

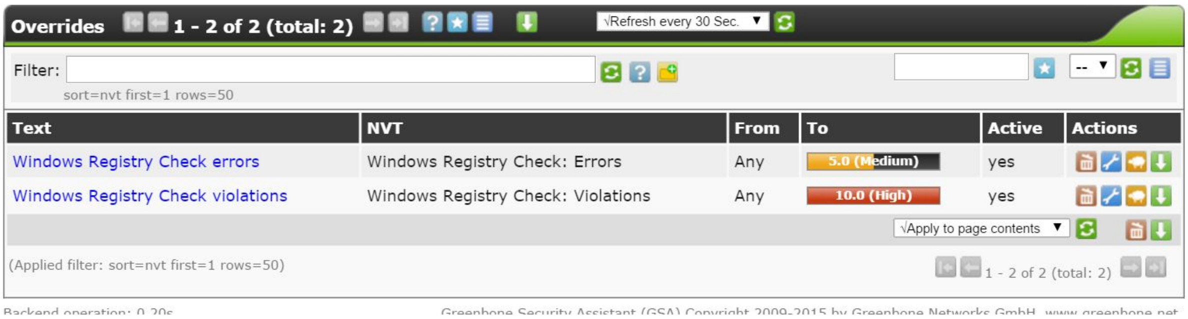
Name	New Value	Default Value	Actions
Timeout	● Apply default timeout ○		
Policy registry file	□ Upload file: Choose File No file chosen		

Fig. 9.6: The mask will change if there is already a file uploaded.

Severity

The registry content tests report any result per default as log messages. By sectioning the reporting plugins in three different NVT's it is now possible to create distinct overrides on the severity according your needs.

In the figure *Severity overrides applied for Windows registry checks.* (page 98) the severities of *Registry Content: Violations* and *Registry Content: Errors* have been changed which will be shown in the reports accordingly.



Overrides 1 - 2 of 2 (total: 2)

√Refresh every 30 Sec.
Filter:
sort=nvt first=1 rows=50

Text	NVT	From	To	Active	Actions
Windows Registry Check errors	Windows Registry Check: Errors	Any	5.0 (Medium)	yes	
Windows Registry Check violations	Windows Registry Check: Violations	Any	10.0 (High)	yes	

√Apply to page contents
(Applied filter: sort=nvt first=1 rows=50)
1 - 2 of 2 (total: 2)
Backend operation: 0.20s
Greenbone Security Assistant (GSA) Copyright 2009-2015 by Greenbone Networks GmbH, www.greenbone.net

Fig. 9.7: Severity overrides applied for Windows registry checks.

Example

Here (policy_registry_ScanConfig.xml[13]) is an example scan configuration with all relevant NVT's for the registry test to download. The corresponding testfiles (Registry_test.txt[14]) should be downloaded to the */tmp/* directory on the target system.

Now create a new task and start it for the target system where you saved test files.

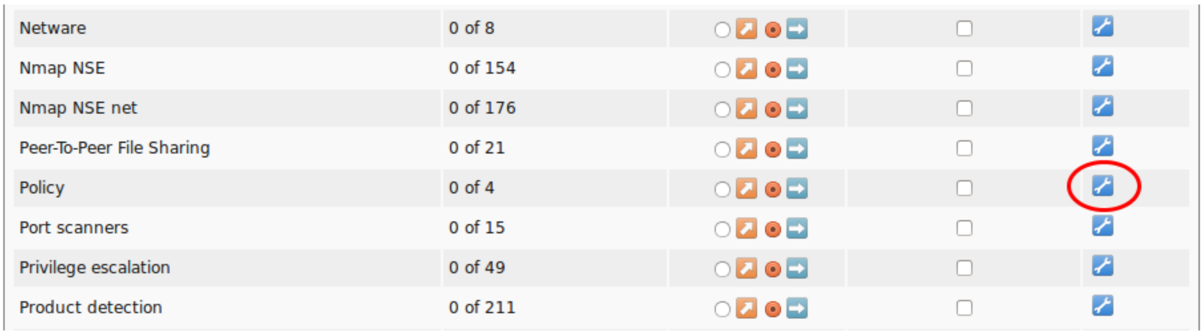
The overrides can be created either before or after a scan. The latter is easier since you can create the appropriate reference through a simple click in the result page.

9.1.3 File Checksums

File checksum checks belong to policy audits which don't explicitly test for vulnerabilities but rather test the integrity of files. GSM provides a policy auditing module to verify file integrity on target systems. This module checks the file content by MD5 or SHA1 checksums. In general this is an authenticated check, i.e. the scan engine will have to log into the target system to perform the check. The file checksum check can only be performed on systems supporting checksums. Normally this means Linux or Linux-like systems. GSM provides however as well a module for checksum checks for Windows systems (see *Windows* (page 101)).

[13] http://www.greenbone.net/download/misc/policy_registry_ScanConfig.xml

[14] http://www.greenbone.net/download/misc/Registry_test.txt



Netware	0 of 8	○ ↗ ● ➡	□	
Nmap NSE	0 of 154	○ ↗ ● ➡	□	
Nmap NSE net	0 of 176	○ ↗ ● ➡	□	
Peer-To-Peer File Sharing	0 of 21	○ ↗ ● ➡	□	
Policy	0 of 4	○ ↗ ● ➡	□	
Port scanners	0 of 15	○ ↗ ● ➡	□	
Privilege escalation	0 of 49	○ ↗ ● ➡	□	
Product detection	0 of 211	○ ↗ ● ➡	□	

Fig. 9.8: The NVT's are in the „Policy“ family.

Four different NVT's provide the file checksum check:

- *File Checksums*: This NVT performs the actual checksum check on the files.
- *File Checksums: Matches*: This NVT shows the files which passed the checksum check (checksum matches).
- *File Checksums: Violations*: This NVT shows the files which didn't pass the checksum check (wrong checksum).
- *File Checksums: Errors*: This NVT shows the files where some error occurred (e.g. file not found on the target system).

The plugin *File Checksums* must be selected for a file checksum check since it performs the actual tests. The other three plugins may be selected according to the needs. E.g. just files with wrong checksums are of concern then only the plugin *File Checksums: Violations* should be additionally selected.

Checksum Patterns

A file with the reference checksums must be created. Following is an example:

```
Checksum|File|Checksumtype
6597ecf8208cf64b2b0eaa52d8169c07|/bin/login|md5
ed3ed98cb2efa9256817948cd27e5a4d9be2bdb8|/bin/bash|sha1
7c59061203b2b67f2b5c51e0d0d01c0d|/bin/pwd|md5
```

This file must first contain the row *Checksum|File|Checksumtype*. The subsequent rows contain each a test entry. Each row contain three elements which are separated by `|`. The first field contains the checksum in hex, the second field the path and file name and the third field the checksum type. Currently MD5 and SHA1 checksums are supported.

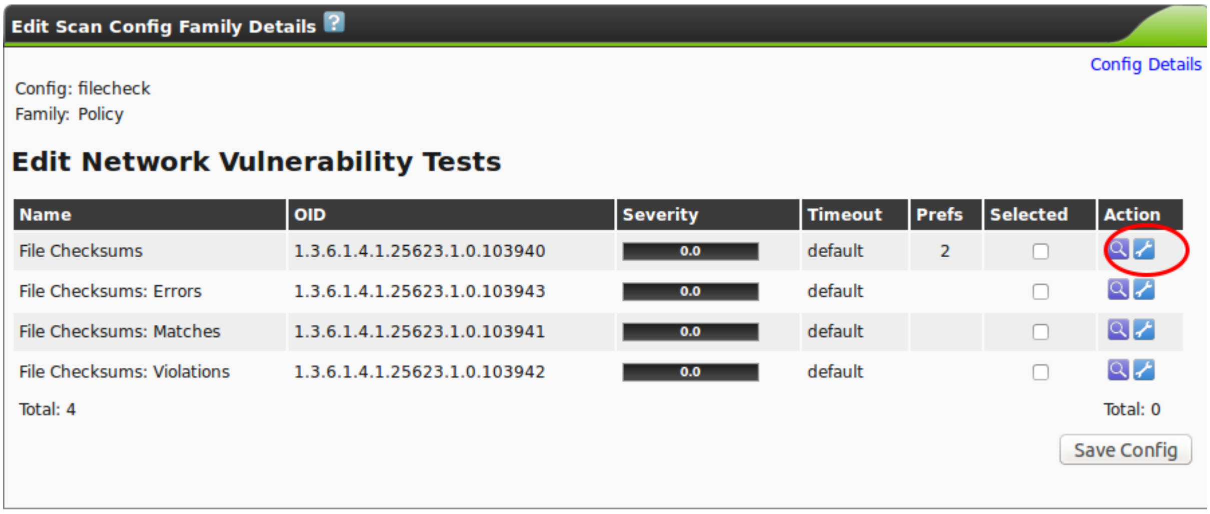
Note: Checksums and checksum type must be lowercase.

Select the file with *Browse* and select *Upload file*. The file upload will be started by clicking *Save Config*.

By clicking on the ⬇ icon it is possible to download the already uploaded reference file. Select *Replace existing file with:* to upload a new reference file. The possibilities to change is only available if the scan configuration is not in use. This is done to ensure immutable audit-compliant scan results.

Severity

The checksum tests report any result per default as log messages. By sectioning the reporting plugins in three different NVT's it is now possible to create distinct overrides on the severity according your needs.



Edit Scan Config Family Details

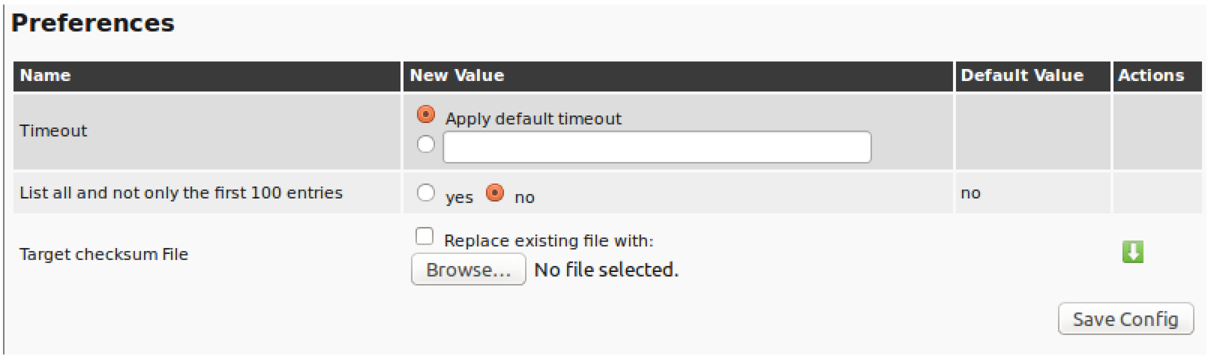
Config Details

Config: filecheck
Family: Policy

Edit Network Vulnerability Tests

Name	OID	Severity	Timeout	Prefs	Selected	Action
File Checksums	1.3.6.1.4.1.25623.1.0.103940	0.0	default	2	□	
File Checksums: Errors	1.3.6.1.4.1.25623.1.0.103943	0.0	default		□	
File Checksums: Matches	1.3.6.1.4.1.25623.1.0.103941	0.0	default		□	
File Checksums: Violations	1.3.6.1.4.1.25623.1.0.103942	0.0	default		□	
Total: 4						Total: 0

Fig. 9.9: Afterwards import this file in the properties of the NVT.

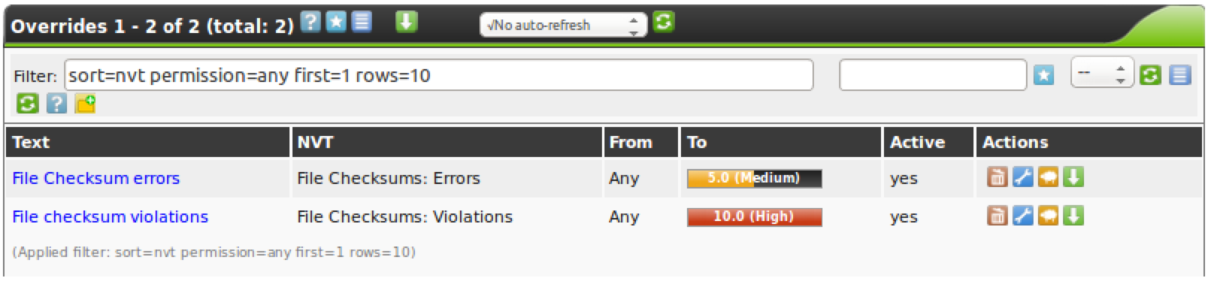


Preferences

Name	New Value	Default Value	Actions
Timeout	● Apply default timeout ○		
List all and not only the first 100 entries	○ yes ● no	no	
Target checksum File	□ Replace existing file with: Browse... No file selected.		

Fig. 9.10: The mask will change if there is already a file uploaded.

In the figure *Severity overrides applied for file checksum checks.* (page 100) the severities of *File Checksum: Violations* and *File Checksum: Errors* have been changed which will be shown in the reports accordingly.



Overrides 1 - 2 of 2 (total: 2)

Filter: sort=nvt permission=any first=1 rows=10

Text	NVT	From	To	Active	Actions
File Checksum errors	File Checksums: Errors	Any	5.0 (Medium)	yes	
File checksum violations	File Checksums: Violations	Any	10.0 (High)	yes	

(Applied filter: sort=nvt permission=any first=1 rows=10)

Fig. 9.11: Severity overrides applied for file checksum checks.

Example

Here (policy_file_checksums_example.xml[15]) is an example scan configuration with all relevant NVT's for the checksum test to download. The corresponding testfiles (policy_file_checksums_testfiles[16]) should be downloaded and extracted to the */tmp/* directory on the

[15] http://www.greenbone.net/download/scanconfigs/policy_file_checksums_example.xml

[16] http://www.greenbone.net/download/misc/policy_file_checksums_testfiles.tar.gz

target system. This can be done e.g. by `tar xvC /tmp/ testfiles_checksum_check.tar.gz`.

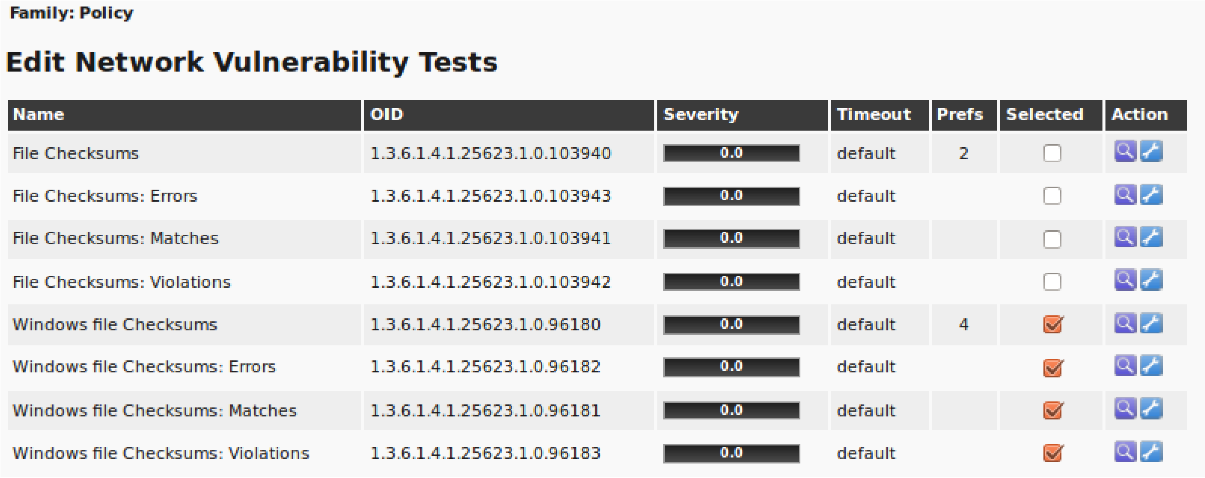
Now create a new task and start it for the target system where you saved test files. Please note that this has to be an authenticated scan with the appropriate SSH Credentials.

The overrides can be created either before or after a scan. The latter is easier since you can create the appropriate reference through a simple click in the result page.

Windows

GSM provides a similar module for Windows systems for checksum checks. Since Windows doesn't provide an internal program for creating checksums it has to be installed one either manually or automatically by the NVT. GSM uses ReHash (http://rehash.sourceforge.net/) for creating checksums on Windows systems.

As for Linux systems the NVT's for checksum checks are located under the *Policy* family.

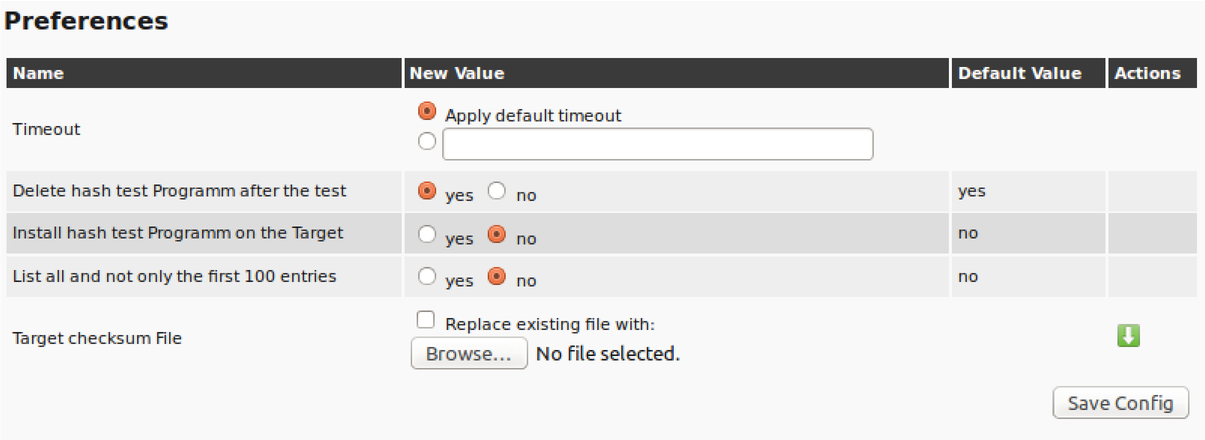


Family: Policy

Edit Network Vulnerability Tests

Name	OID	Severity	Timeout	Prefs	Selected	Action
File Checksums	1.3.6.1.4.1.25623.1.0.103940	0.0	default	2	☐	🔍 ✎
File Checksums: Errors	1.3.6.1.4.1.25623.1.0.103943	0.0	default		☐	🔍 ✎
File Checksums: Matches	1.3.6.1.4.1.25623.1.0.103941	0.0	default		☐	🔍 ✎
File Checksums: Violations	1.3.6.1.4.1.25623.1.0.103942	0.0	default		☐	🔍 ✎
Windows file Checksums	1.3.6.1.4.1.25623.1.0.96180	0.0	default	4	☑	🔍 ✎
Windows file Checksums: Errors	1.3.6.1.4.1.25623.1.0.96182	0.0	default		☑	🔍 ✎
Windows file Checksums: Matches	1.3.6.1.4.1.25623.1.0.96181	0.0	default		☑	🔍 ✎
Windows file Checksums: Violations	1.3.6.1.4.1.25623.1.0.96183	0.0	default		☑	🔍 ✎

Fig. 9.12: Four NVT's are responsible for the checksum checks under Windows



Preferences

Name	New Value	Default Value	Actions
Timeout	● Apply default timeout ○		
Delete hash test Programm after the test	● yes ○ no	yes	
Install hash test Programm on the Target	○ yes ● no	no	
List all and not only the first 100 entries	○ yes ● no	no	
Target checksum File	☐ Replace existing file with: Browse... No file selected.		⬇

Fig. 9.13: The preferences must be set then in the „Windows file Checksums“ NVT.

Please note the two operating modes for these checks: Either a before manually on the target system installed tool will be used or the tool ReHash will automatically be installed and if requested as well deinstalled on the target system during the checking routine.

Through the preferences it can be set if the checksum program ReHash should be deleted after the check or not. The program can be left on the target system to e.g. speed up recurring tests and therefore don't have to be transfered each time. It can further be set if the checksum program should be installed automatically on the target system. If not it has to be manually installed (under *C:\Windows\system32* on 32-bit system) or *C:\Windows\SysWOW64* (on 64-bit systems)) and has to be executable for the authenticated user. The file with the reference checksums must be uploaded in the preferences as it is done for the Linux checksum check. The file has the same structure as the one for Linux.

Example Windows

A sample configuration (sample_config-Windows_file_Policy.xml[17]) with all needed NVT's for the Windows checksum check can be downloaded here. The corresponding example files (windows_checksums_testfiles.zip[18]) can be downloaded and must be saved on the target system.

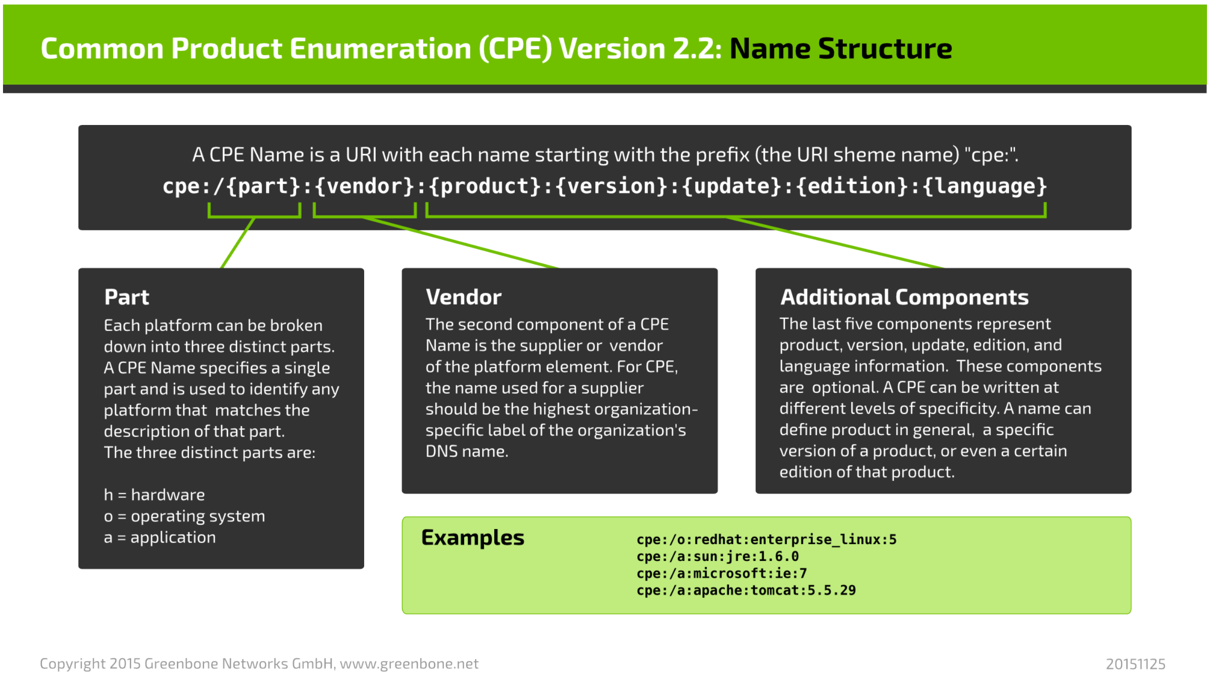
For Tasks and Overrides please proceed as described above.

9.1.4 CPE-based

CPE stands for Common Product Enumeration[19]. It is a structured naming scheme for information technology systems, platforms, and packages.

In other words: CPE provides a unique identifier for virtually any software product that is known for a vulnerability.

The CPE dictionary is maintained by U.S. National Institute for Standards and Technology (NIST)[20] and was developed by the MITRE Corporation (MITRE)[21] and NIST. Close to the end of 2014 MITRE announced that all intellectual property associated with CPE has been transferred to NIST. MITRE still maintains CVE (Common Vulnerability Enumeration) and other relevant security standards.



Common Product Enumeration (CPE) Version 2.2: Name Structure

A CPE Name is a URI with each name starting with the prefix (the URI sheme name) "cpe:".

`cpe:/{part}:{vendor}:{product}:{version}:{update}:{edition}:{language}`

Part
Each platform can be broken down into three distinct parts. A CPE Name specifies a single part and is used to identify any platform that matches the description of that part.
The three distinct parts are:

h = hardware
o = operating system
a = application

Vendor
The second component of a CPE Name is the supplier or vendor of the platform element. For CPE, the name used for a supplier should be the highest organization-specific label of the organization's DNS name.

Additional Components
The last five components represent product, version, update, edition, and language information. These components are optional. A CPE can be written at different levels of specificity. A name can define product in general, a specific version of a product, or even a certain edition of that product.

Examples

```
cpe:/o:redhat:enterprise_linux:5
cpe:/a:sun:jre:1.6.0
cpe:/a:microsoft:ie:7
cpe:/a:apache:tomcat:5.5.29
```

Copyright 2015 Greenbone Networks GmbH, www.greenbone.net 20151125

[17] http://www.greenbone.net/download/scanconfigs/sample_config-Windows_file_Policy.xml
[18] http://www.greenbone.net/download/misc/windows_checksums_testfiles.zip
[19] http://scap.nist.gov/specifications/cpe/
[20] http://www.nist.org
[21] http://www.mitre.org/

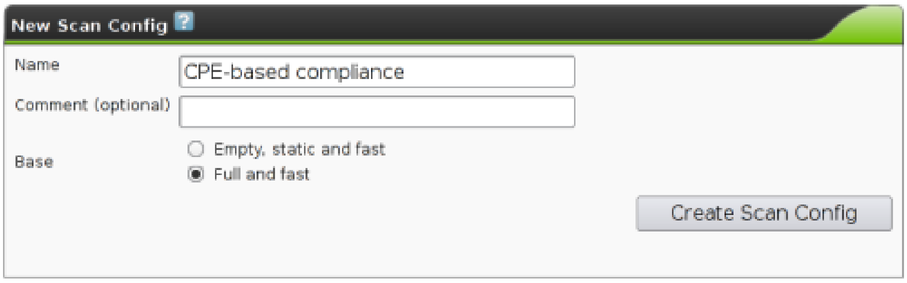
CPE-based, simple checks for security policies

With any executed scan, CPEs for the identified products are stored. This happens independently of whether the product actually reveals a security problem or not. On this basis it is possible to describe simple security policies and the checks for compliance with these. With the Greenbone Security Manager it is possible to describe policies to check for the presence as well as for the absence of a product. These cases can be associated with a severity to appear in the scan report.

Checking policy compliance

This example demonstrates how to check the compliance of a policy regarding specific products in a IT infrastructure and how the reporting with the corresponding severity can be done.

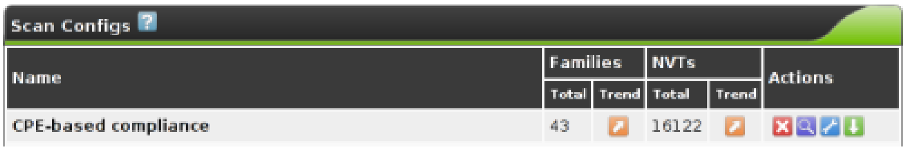
1. The information about whether a certain product is present on the target system is gathered by a single Network Vulnerability Test (NVT) or even independently by a number of special NVTs. This means that for a certain product you can specify an optimized scan configuration that only concentrates on this product and does not do any other scan activity. The advantage of such a special scan configuration is a considerably faster execution of the scan compared to a comprehensive scan configuration such as *Full and Fast*. The disadvantage of a special scan configuration is that some experience is required to select the right set of NVTs to maximize the probability of success. Initially it is easier to apply a comprehensive scan configuration. In this case it is not necessary to care about the product character, you just enter its CPE identifier. This example follows the simple approach. First, a copy of *Full and Fast* is created. This is necessary because *Full and Fast* is a pre-configured scan configuration and thus can not be modified.



New Scan Config

Name	CPE-based compliance
Comment (optional)	
Base	○ Empty, static and fast ● Full and fast

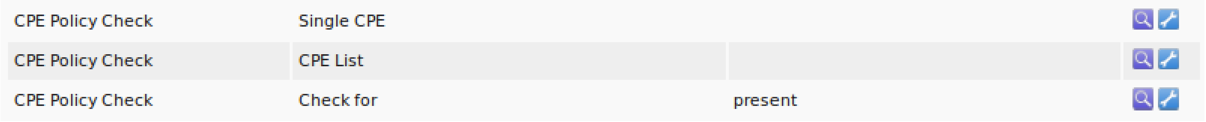
2. Edit the newly created scan configuration by clicking on 🔧.



Scan Configs

Name	Families		NVTs		Actions
	Total	Trend	Total	Trend	
CPE-based compliance	43	↗	16122	↗	✗ 🔍 🔧 ⬇

3. On the overview page for this scan configuration you will find a section *Network Vulnerability Test Preferences*. Here, all NVTs that allow special configuration are listed. With 🔧 you can jump directly to the edit dialog for a specific NVT. This short-cut avoids having to click through the family structures to get to the desired NVT (the here used NVTs are in the family *Policy*).



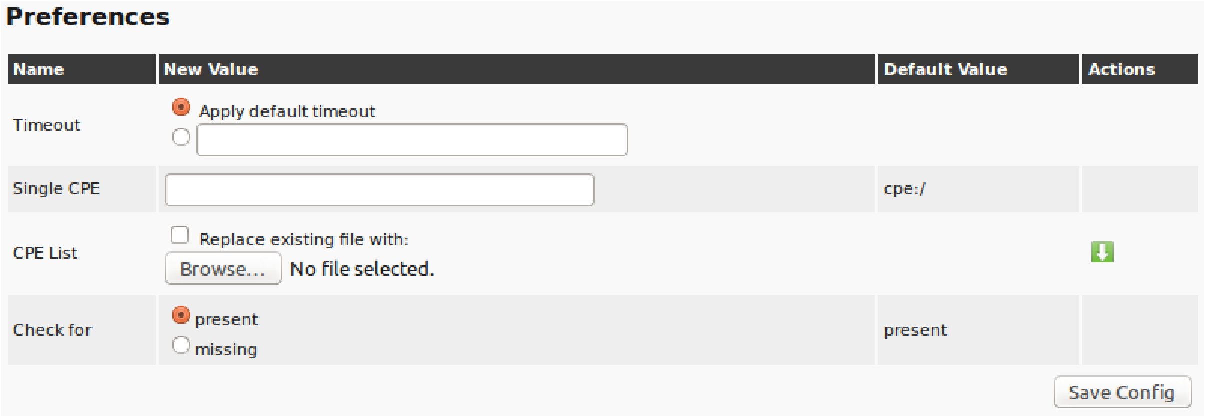
CPE Policy Check	Single CPE		🔍 🔧
CPE Policy Check	CPE List		🔍 🔧
CPE Policy Check	Check for	present	🔍 🔧

4. You can either specify a single CPE directly or a list of CPEs in a file which must be imported afterwards (through clicking on *Browse* to select the file and selecting *Upload file*). Below is an example for checking for Internet Explorer 9 and ClamAV 0.98:

```
cpe:/a:microsoft:ie:9
cpe:/a:clamav:clamav:0.98
```

For this example we have a policy where the stated CPEs must be present to comply. This means we want to know especially if there are some installations which violate this policy (e.g. missing or not wrong products/versions).

Confirm your changes with *Save Config*.



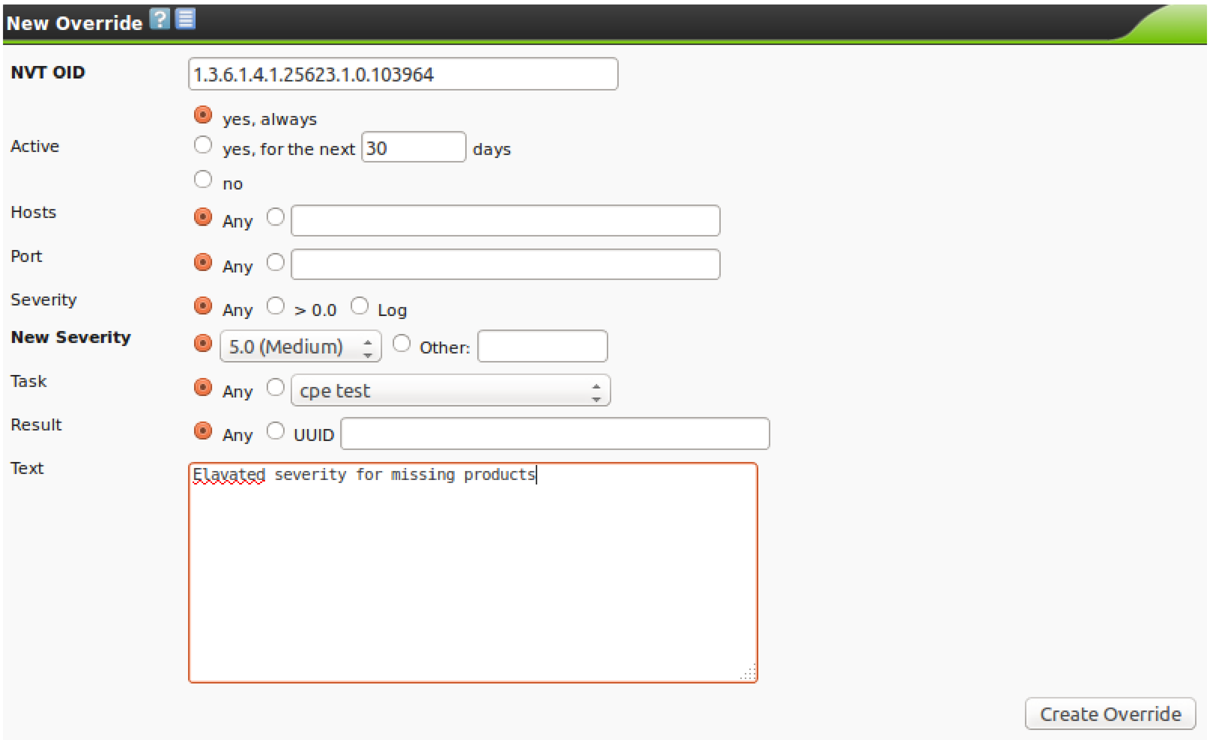
Preferences

Name	New Value	Default Value	Actions
Timeout	● Apply default timeout ○		
Single CPE		cpe:/	
CPE List	□ Replace existing file with: Browse... No file selected.		⬇
Check for	● present ○ missing	present	

Save Config

5. Policy checks report the results in general as "Log" messages. If you want to change this you have to create an override. In this example violations of the policy should be reported with an elevated severity.

   For this a new override has to be created through the *Scan Management*. The OID in this case will be "1.3.6.1.4.1.25623.1.0.103964" (for the NVT *CPE-based Policy Check Violations*) and a new severity of 5.0 (Medium) will be set.

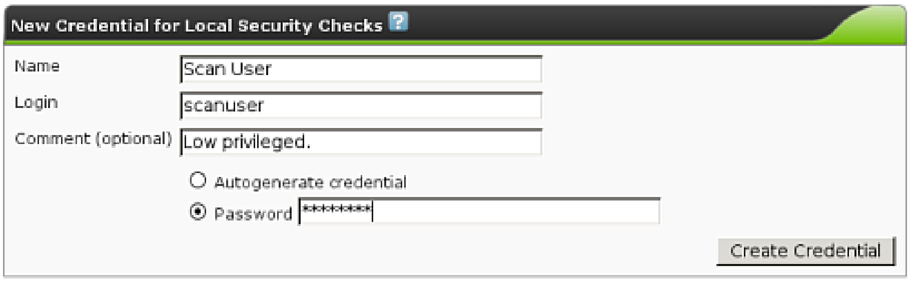


New Override

NVT OID	1.3.6.1.4.1.25623.1.0.103964
Active	● yes, always ○ yes, for the next 30 days ○ no
Hosts	● Any ○
Port	● Any ○
Severity	● Any ○ > 0.0 ○ Log
New Severity	● 5.0 (Medium) ○ Other:
Task	● Any ○ cpe test
Result	● Any ○ UUID
Text	Elavated severity for missing products

Create Override

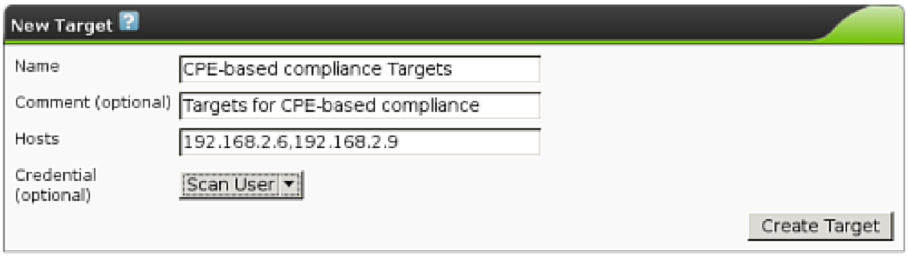
6. In case the detection efficiency should be increased by applying local security checks it is required to configure remote access via the *Credentials* feature. If not done yet, create a corresponding user account on the Windows systems (a low privileged user account is sufficient).



New Credential for Local Security Checks

Name	Scan User
Login	scanuser
Comment (optional)	Low privileged.
	○ Autogenerate credential
	● Password ********

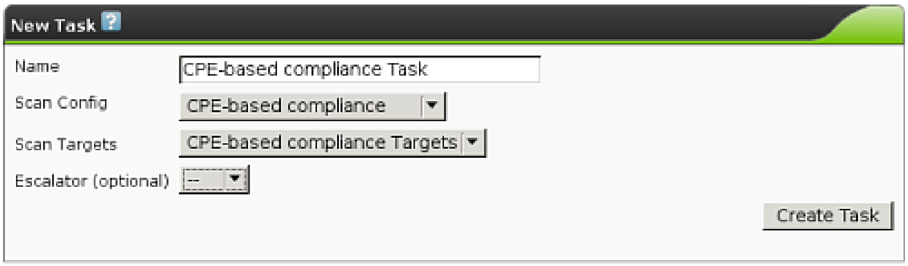
7. Define the target systems (targets) and, if applicable, choose the respective credentials.



New Target

Name	CPE-based compliance Targets
Comment (optional)	Targets for CPE-based compliance
Hosts	192.168.2.6,192.168.2.9
Credential (optional)	Scan User

8. Now you can create the actual task. This means to combine the newly created scan configuration with the newly created targets.



New Task

Name	CPE-based compliance Task
Scan Config	CPE-based compliance
Scan Targets	CPE-based compliance Targets
Escalator (optional)	--

9. The scan is started by clicking on ▶ of the respective task. It can take a while for the scan to complete. To update the view with the current progress, click on ⟳.

10. As soon as the status changes to *Done* the complete report is available. At any time you can review the intermediate results. To only show the results of the CPE-based policy checks, you can apply a suitable filter (search text "cpe").

11. In this example ClamAV 0.98 was found on one of the target systems and reported as a log message.

Internet Explorer 9 on the other hand haven't been found on the target system which will be reported as a medium risk as defined in the override.

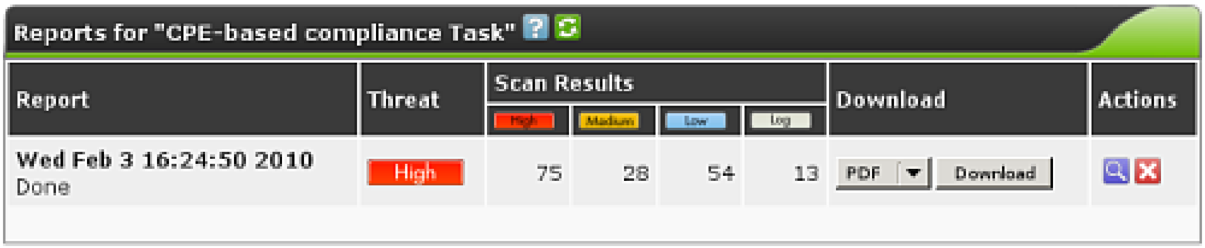
Finding problematic products

This example demonstrates how the presence of a certain product in an IT infrastructure is classified as a severe problem and reported as such.

1. Execute steps 1 to 3 of the above described method for finding checking policy compliance.

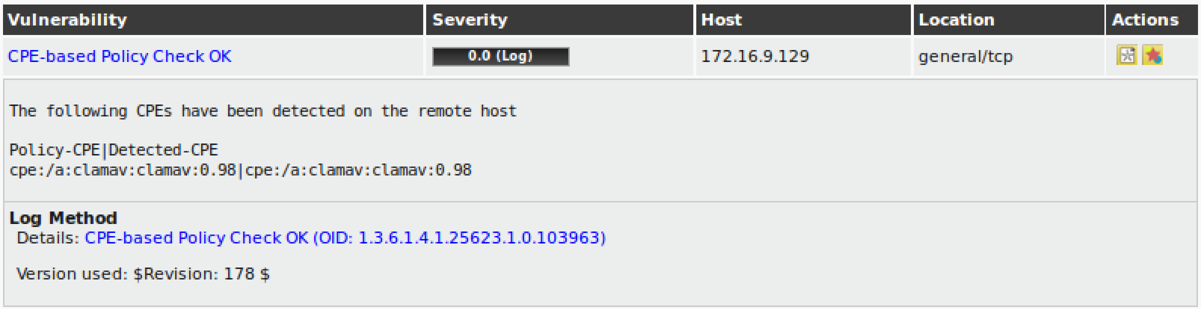
   Note that when choosing a general scan like *Full and Fast* both cases are treated the same, presence of the product as a running service and presence of the product on a hard drive.

   This essentially means that if you want to ensure the desired product indeed runs as a service you should avoid running NVTs that check for the simple presence on the file system or in a registry. If you don't want to go into such details right now, you still have the option to look into the report details in order to check for false positives and false negatives.



Reports for "CPE-based compliance Task"

Report	Threat	Scan Results				Download	Actions
		High	Medium	Low	Log		
Wed Feb 3 16:24:50 2010 Done	High	75	28	54	13	PDF ▾ Download	



Vulnerability	Severity	Host	Location	Actions
CPE-based Policy Check OK	0.0 (Log)	172.16.9.129	general/tcp	

```
The following CPEs have been detected on the remote host

Policy-CPE|Detected-CPE
cpe:/a:clamav:clamav:0.98|cpe:/a:clamav:clamav:0.98
```

Log Method
Details: CPE-based Policy Check OK (OID: 1.3.6.1.4.1.25623.1.0.103963)

Version used: $Revision: 178 $

2. This time a single CPE (Internet Explorer 6) will be searched.

   In this case we have to set that the entered CPE must be “present”.

   Confirm your changes with *Save Config*.

3. Policy checks report the results in general as “Log” messages. If you want to change this you have to create an override. In this example violations of the policy should be reported with an elevated severity.

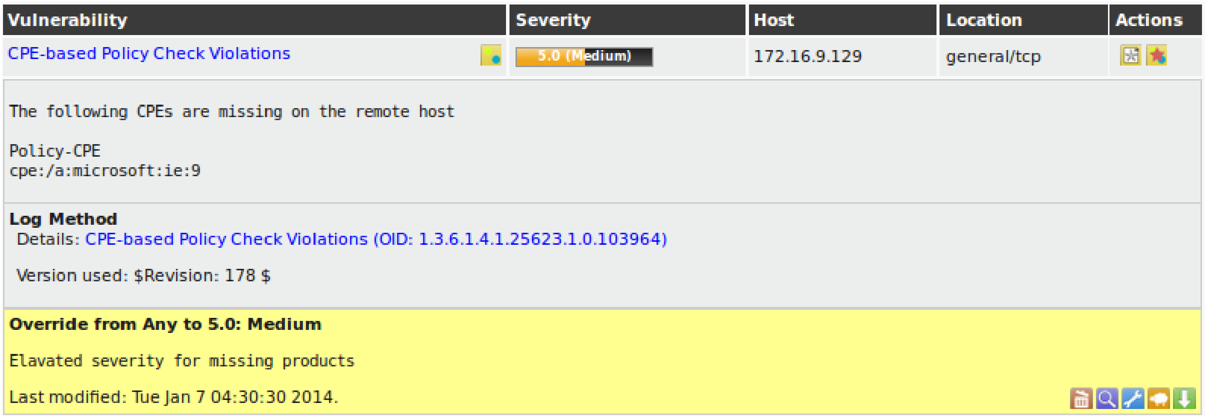
   For this, a new override has to be created through the *Scan Management*. The OID in this case will be “1.3.6.1.4.1.25623.1.0.103963” (for the NVT *CPE-based Policy Check OK*) and a new severity of 10.0 (High) will be set.

4. In case the pure presence of a product should be considered, you should apply local security checks by configuring remote access via the *Credentials* feature. Execute step 6 to 9 in the example above to enable local security checks, to create a new task with the target systems and to start it.

5. As soon as the status changes to *Done* the complete report is available. At any time you can review the intermediate results.

   To only show the results of the CPE-based policy checks, you can apply a suitable filter (search text “cpe”).

6. In this example Internet Explorer 6 was found on one of the target systems and reported as a severe problem as defined in the override.



Vulnerability	Severity	Host	Location	Actions
CPE-based Policy Check Violations	5.0 (Medium)	172.16.9.129	general/tcp	

```
The following CPEs are missing on the remote host

Policy-CPE
cpe:/a:microsoft:ie:9
```

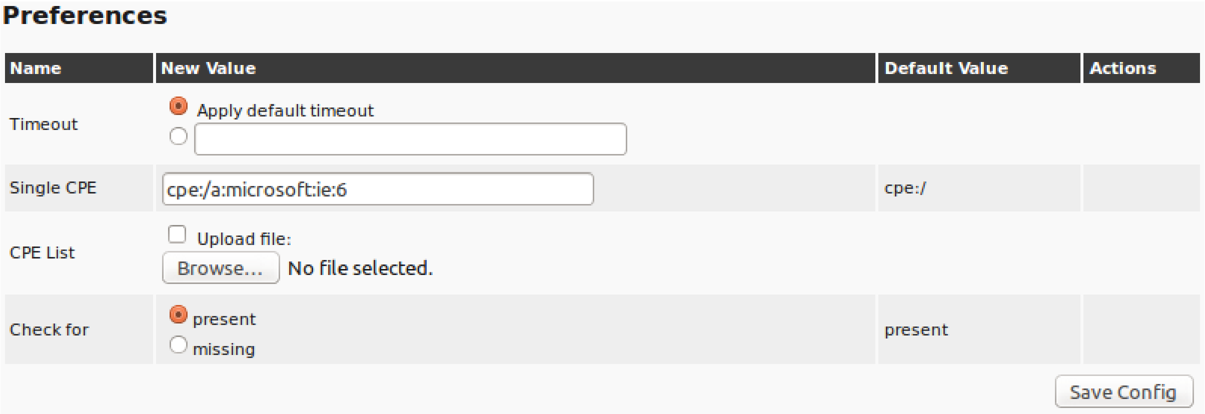
Log Method
Details: CPE-based Policy Check Violations (OID: 1.3.6.1.4.1.25623.1.0.103964)

Version used: $Revision: 178 $

Override from Any to 5.0: Medium

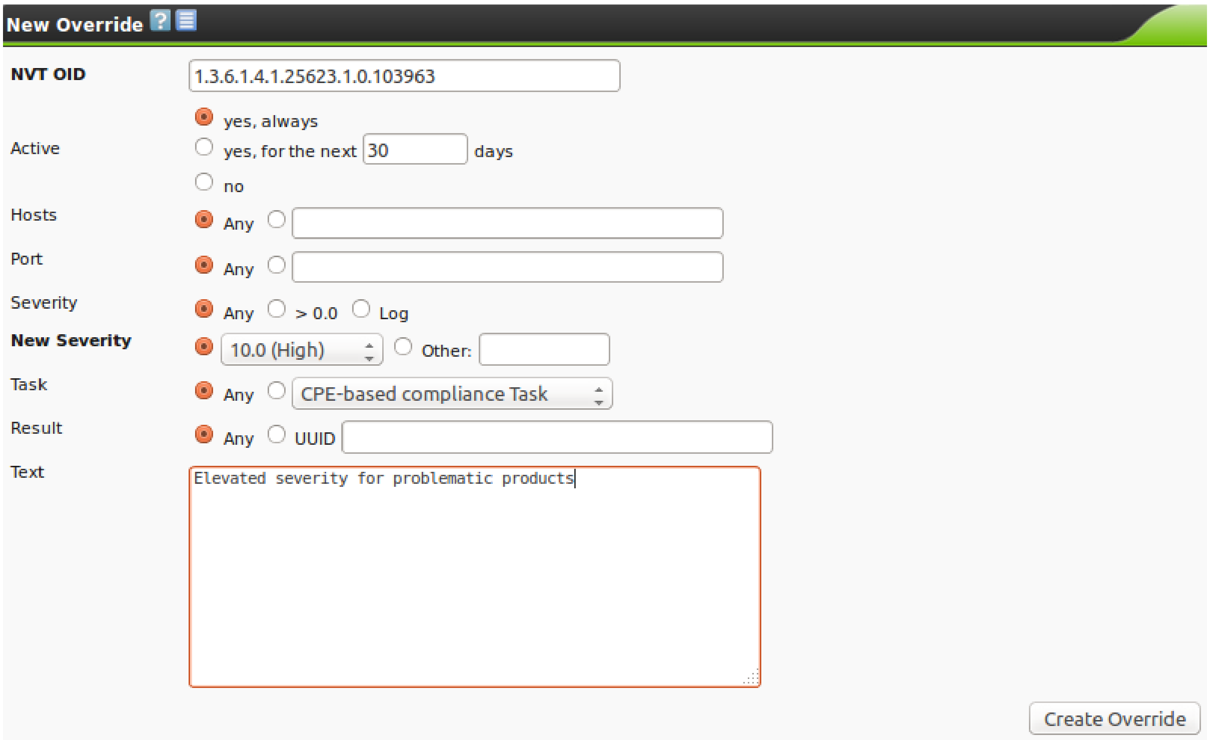
```
Elavated severity for missing products
```

Last modified: Tue Jan 7 04:30:30 2014.



Preferences

Name	New Value	Default Value	Actions
Timeout	● Apply default timeout ○		
Single CPE	cpe:/a:microsoft:ie:6	cpe:/	
CPE List	□ Upload file: Browse... No file selected.		
Check for	● present ○ missing	present	



New Override

NVT OID	1.3.6.1.4.1.25623.1.0.103963
Active	● yes, always ○ yes, for the next 30 days ○ no
Hosts	● Any ○
Port	● Any ○
Severity	● Any ○ > 0.0 ○ Log
New Severity	● 10.0 (High) ○ Other:
Task	● Any ○ CPE-based compliance Task
Result	● Any ○ UUID
Text	Elevated severity for problematic products

Detecting absence of important products

This example shows how the absence of a certain product in your IT infrastructure is defined as a severe problem and reported as such.

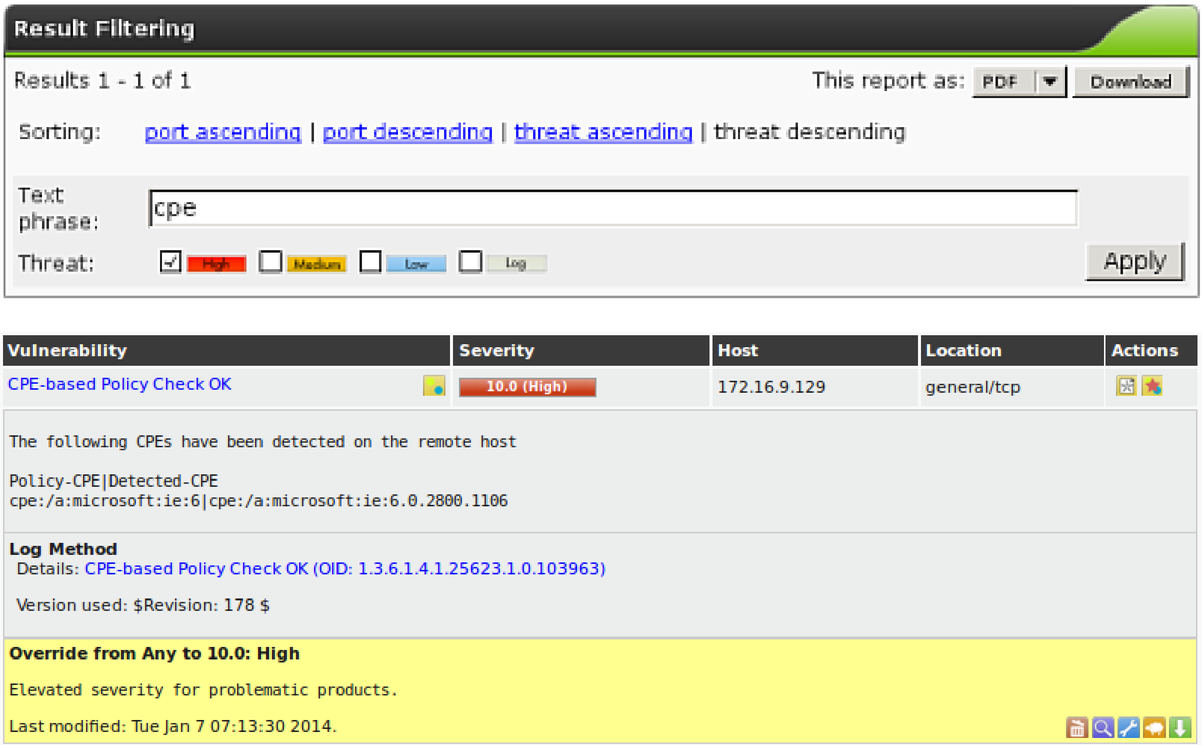
1. Execute steps 1 to 3 of the above described method for finding problematic products.

   Note that when choosing a general scan like *Full and Fast* both cases are treated the same, presence of the product as a running service and presence of the product on a hard drive.

   This essentially means that if you want to ensure the desired product indeed runs as a service you should avoid running NVTs that check for the simple presence on the file system or in a registry. If you don't want to go into such details right now, you still have the option to look into the report details in order to check for false positives and false negatives.

2. This time the configuration of *CPE-based Policy Check* will be set up to check if Norton Antivirus is present on the target system. In this case it will be reported if it is "missing".

3. Policy checks report the results in general as "Log" messages. If you want to change this you have to create an override. In this example violations of the policy should be reported with an elevated severity.



Result Filtering

Results 1 - 1 of 1 This report as: PDF Download

Sorting: port ascending | port descending | threat ascending | threat descending

Text phrase: cpe

Threat: ☑ High □ Medium □ Low □ Log Apply

Vulnerability	Severity	Host	Location	Actions
CPE-based Policy Check OK	10.0 (High)	172.16.9.129	general/tcp	

```
The following CPEs have been detected on the remote host

Policy-CPE|Detected-CPE
cpe:/a:microsoft:ie:6|cpe:/a:microsoft:ie:6.0.2800.1106
```

Log Method
Details: CPE-based Policy Check OK (OID: 1.3.6.1.4.1.25623.1.0.103963)

Version used: $Revision: 178 $

Override from Any to 10.0: High

Elevated severity for problematic products.

Last modified: Tue Jan 7 07:13:30 2014.

For this, a new override has to be created through the *Scan Management*. The OID in this case will be “1.3.6.1.4.1.25623.1.0.103963” (for the NVT *CPE-based Policy Check OK*) and a new severity of 10.0 (High) will be set.

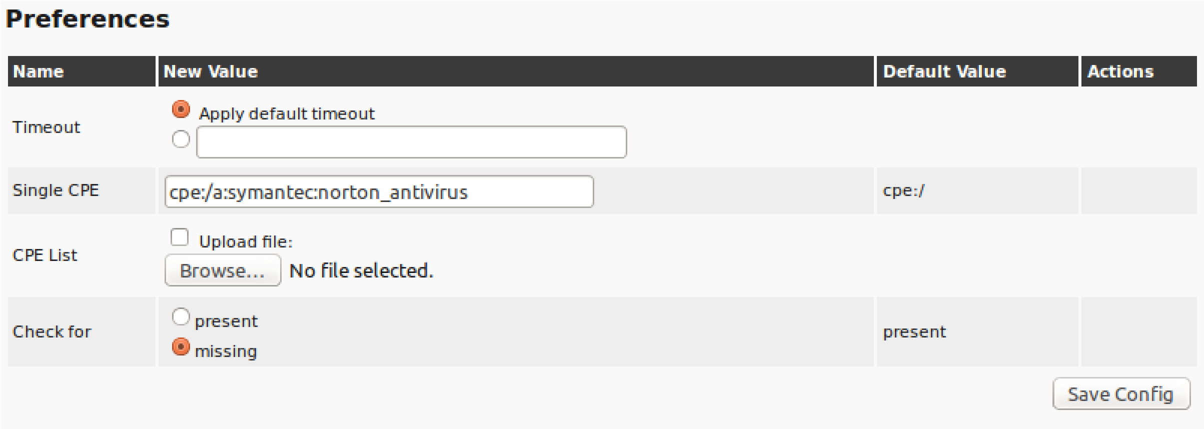
4. For checking simply the availability of a product installation, local security checks can improve the detection rate. If just running network services should be searched it normally doesn't help but rather increase the number of false positives.

   Execute step 6 to 9 in the example *Checking policy compliance* (page 103) to enable local security checks, to create a new task with the target systems and to start it.

5. As soon as the status changes to *Done* the complete report is available. At any time you can review the intermediate results.

   To only show the results of the CPE-based policy checks, you can apply a suitable filter (search text “cpe”).

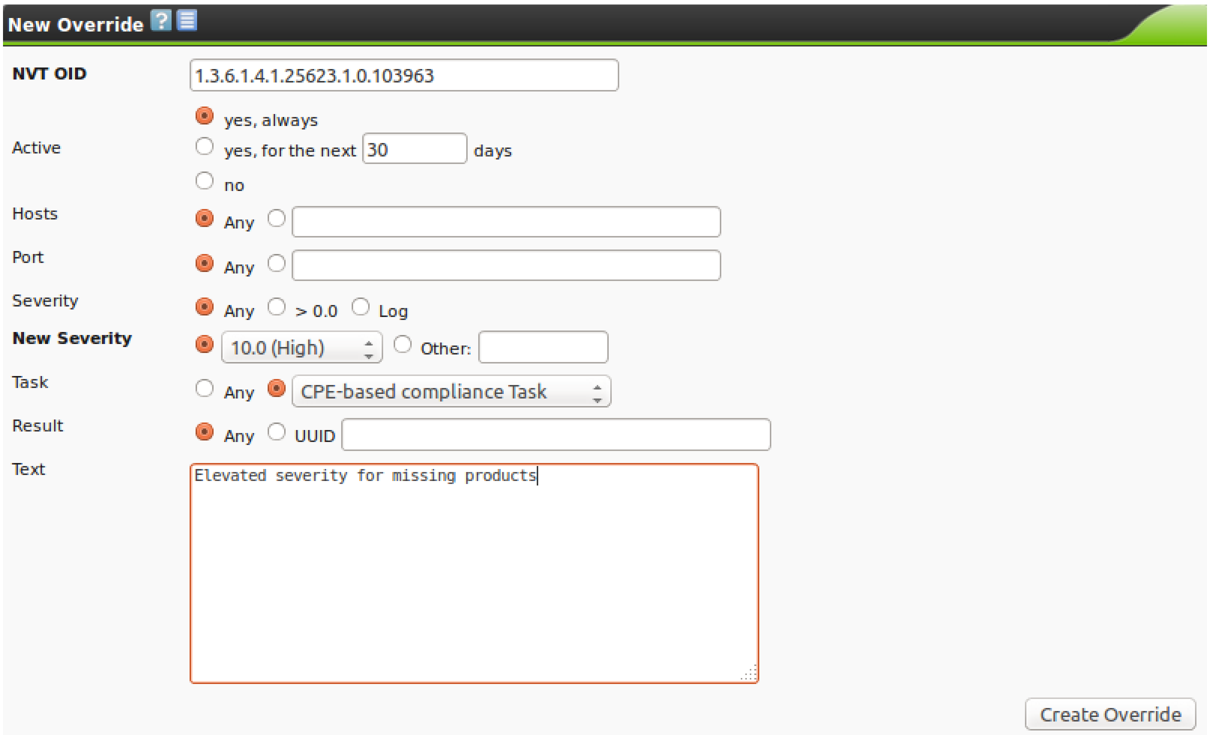
6. In this example Norton Antivirus was not found on one of the target systems.



Preferences

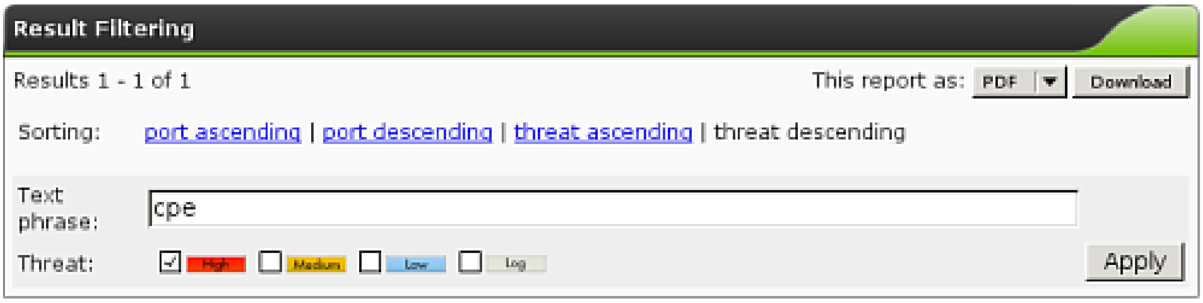
Name	New Value	Default Value	Actions
Timeout	● Apply default timeout ○		
Single CPE	cpe:/a:symantec:norton_antivirus	cpe:/	
CPE List	□ Upload file: Browse... No file selected.		
Check for	○ present ● missing	present	

Save Config



New Override

NVT OID	1.3.6.1.4.1.25623.1.0.103963
Active	● yes, always ○ yes, for the next 30 days ○ no
Hosts	● Any ○
Port	● Any ○
Severity	● Any ○ > 0.0 ○ Log
New Severity	● 10.0 (High) ○ Other:
Task	○ Any ● CPE-based compliance Task
Result	● Any ○ UUID
Text	Elevated severity for missing products



Result Filtering

Results 1 - 1 of 1

This report as: PDF Download

Sorting: port ascending | port descending | threat ascending | threat descending

Text phrase: cpe

Threat: ☑ High ☐ Medium ☐ Low ☐ Log

9.2 Standard Policies

9.2.1 IT-Grundschutz

With the Greenbone Security Manager it is possible to automatically check the German "IT-Grundschutz-Kataloge" as published and maintained by the Bundesamt für Sicherheit in der Informationstechnik[22] (German Federal Office for IT Security, BSI).

Supported is always the current "Ergänzungslieferung" with tests for over 80 measures. That is the maximum number of measures which is possible to support with automatic tests.

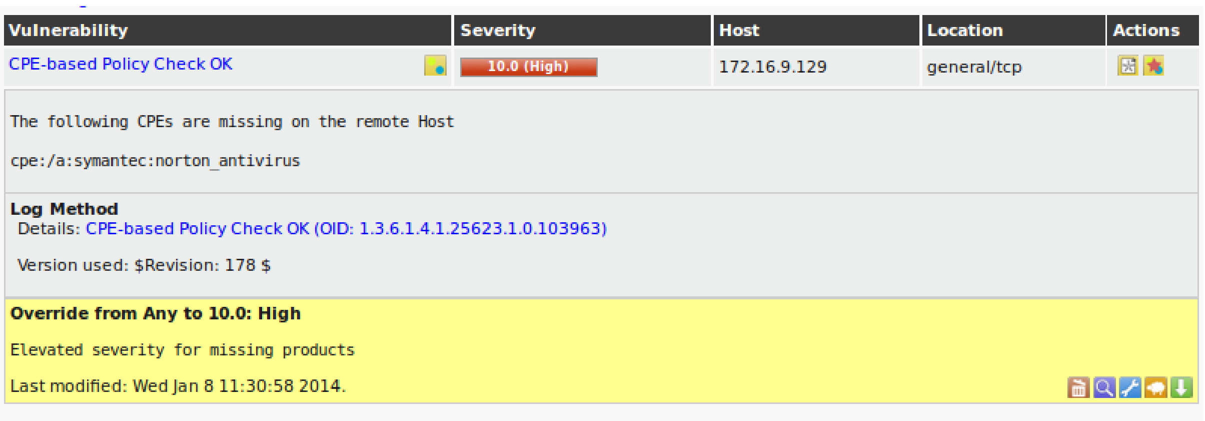
Some measures are quite comprehensive so that and actually consist of several single tests. A couple of measures address a specific operating system ans hence will only be applied to those. The number and type of tested systems remains irrelevant for the Greenbone Security Manager.

This makes the Greenbone Security Manager the fastest co-worker for executing a IT-Grundschutz audit. And it opens the opportunity to install a check for breaches as a permanent background process.

Checking IT-Grundschutz

This example executes a simple check according to the German "IT-Grundschutz-Kataloge".

[22] http://www.bsi.de



Vulnerability	Severity	Host	Location	Actions
CPE-based Policy Check OK	10.0 (High)	172.16.9.129	general/tcp	

```
The following CPEs are missing on the remote Host

cpe:/a:symantec:norton_antivirus
```

Log Method
Details: CPE-based Policy Check OK (OID: 1.3.6.1.4.1.25623.1.0.103963)

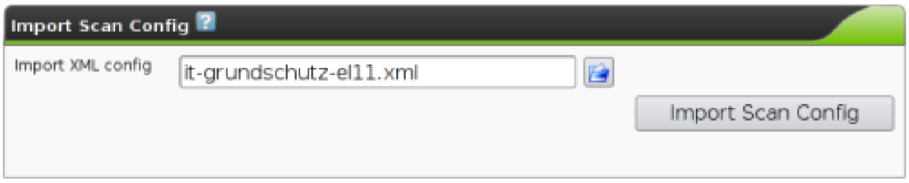
Version used: $Revision: 178 $

Override from Any to 10.0: High

```
Elevated severity for missing products
```

Last modified: Wed Jan 8 11:30:58 2014.

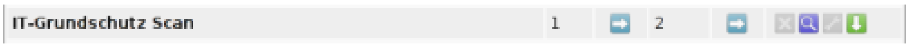
1. Import the scan configuration IT-Grundschutz Scan[23] For verinice integration: IT-Grundschutz Scan incl. Discovery for verinice[24]



Import Scan Config

Import XML config: it-grundschutz-el11.xml

This covers the settings to execute all of the checks. The actual checks are not explicitly selected so that rather a summary result is generated.



IT-Grundschutz Scan	1	2

2. The majority of checks for the measures is based on local security checks. For these a respective access needs to be configured. If not done yet, create a corresponding user account on the Windows systems (the higher the privileges of this user account, the more measures can be checked).
3. Define the target systems (targets) and, if applicable, choose the respective credentials.
4. Now you can create the actual task. This means to combine the imported scan configuration with the newly created targets.
5. The search is started by clicking on ▶ of the respective task. It can take a while for the scan to complete. To update the view with the current progress, click on ⟳.
6. As soon as the status changes to "Done" the complete report is available. At any time you can review the intermediate results. Please note, that for the textual form of the reports you need to enable category "Low" in the filter.

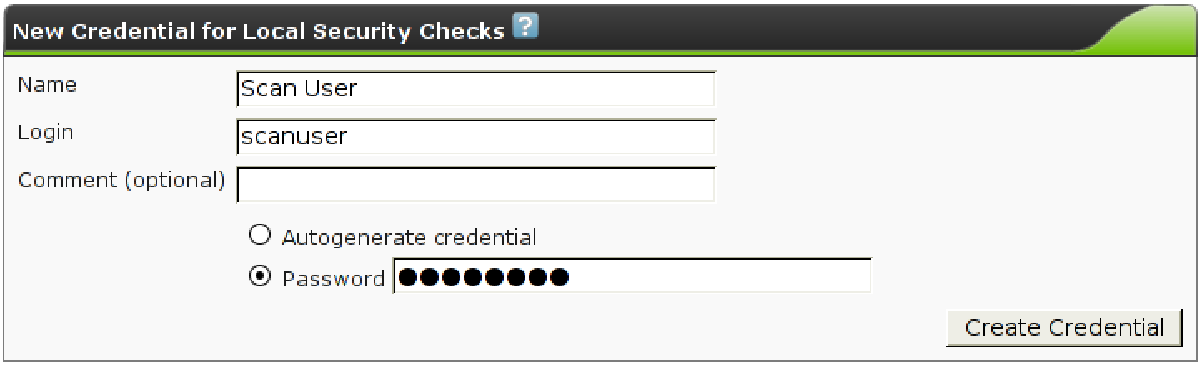
   With the imported scan configuration 2 versions of the results will be created: an overview in textual form (under "general/IT-Grundschutz") and a table for further processing (under "general/IT-Grundschutz-T"). For the latter, you need to enable category "Log" in the report filter

Import of results into a spreadsheet application

1. Choose download format "ITG" either in the report filter or in the task overview. *Note*: Using the report filter it is necessary to enable the category "Log".

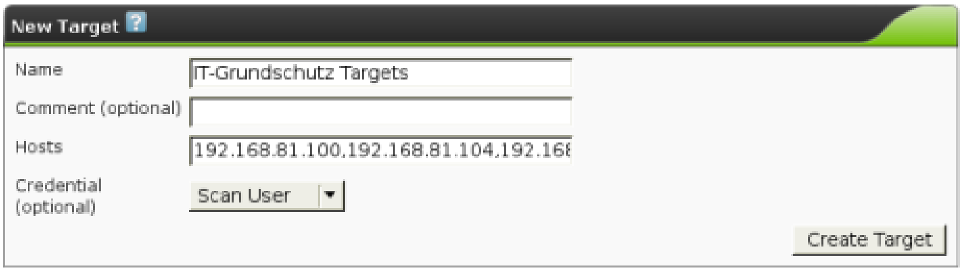
For this download format suitable tabular results for all target systems are automatically collected and joined.

[23] http://www.greenbone.net/download/scanconfigs/it-grundschutz-v2.xml
[24] http://www.greenbone.net/download/scanconfigs/it-grundschutz-discovery-v2.xml



New Credential for Local Security Checks

Name	Scan User
Login	scanuser
Comment (optional)	
	○ Autogenerate credential
	● Password ●●●●●●●●



New Target

Name	IT-Grundschutz Targets
Comment (optional)	
Hosts	192.168.81.100,192.168.81.104,192.168
Credential (optional)	Scan User

2. Import the ITG file as so called CSV table into your spreadsheet application.

The example above shows an import for OpenOffice 3.2. Please take care that the following settings are adjusted for the import (if not already default):

- Charset: UTF-8
- Field separator: The “pipe” symbol (vertical line)
- Text separator: The double quote
- Last column: Type “Text”

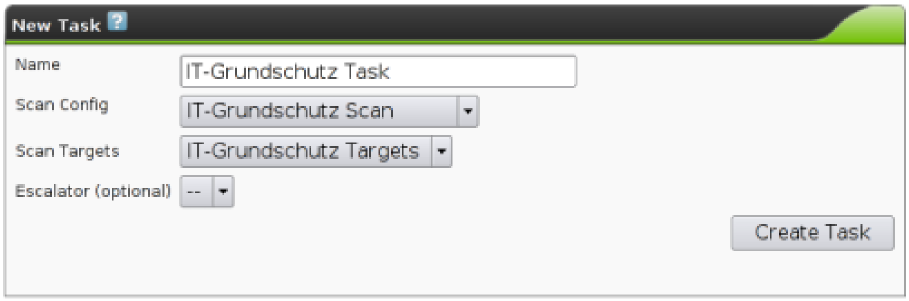
3. Now the scan results are available in the spreadsheet application:
4. From this point you can create simple (like in the screenshot below) or, of course, your individual comprehensive analysis or report.

Import of results into IT-Grundschutz tools

A number of tools is available to help IT-Grundschutz processes with structured approach, data entries and management.

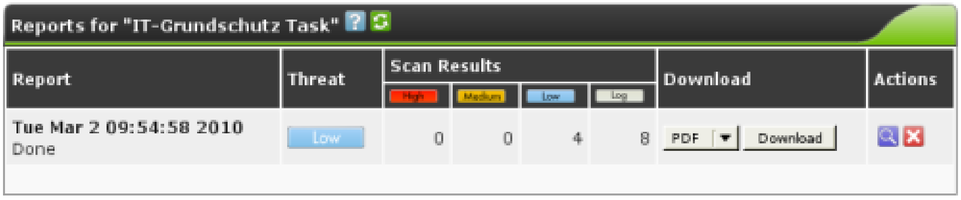
The German federal agency for IT security (Bundesamt für Sicherheit in der Informationstechnik, BSI) offers on its website an overview on IT-Grundschutz tools[25].

[25] https://www.bsi.bund.de/cln_174/DE/Themen/weitereThemen/GSTOOL/AndereTools/anderetools_node.html



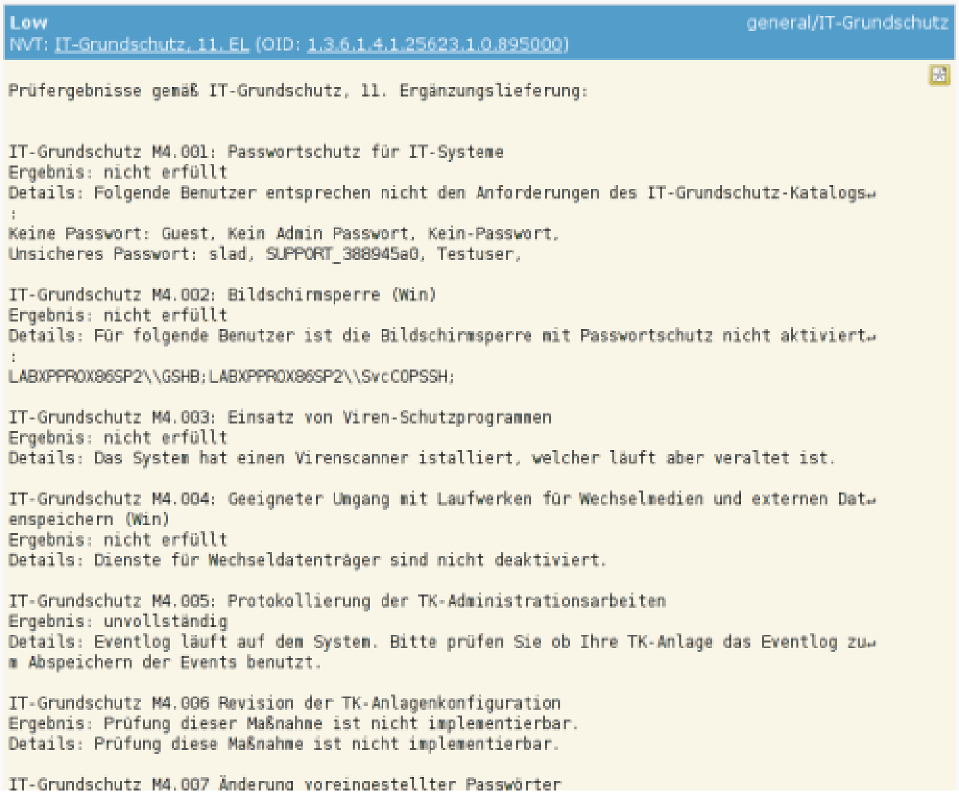
New Task

Name	IT-Grundschutz Task
Scan Config	IT-Grundschutz Scan
Scan Targets	IT-Grundschutz Targets
Escalator (optional)	--



Reports for "IT-Grundschutz Task"

Report	Threat	Scan Results				Download	Actions
		High	Medium	Low	Log		
Tue Mar 2 09:54:58 2010 Done	Low	0	0	4	8	PDF ▾ Download	



Low — general/IT-Grundschutz

NVT: IT-Grundschutz, 11. EL (OID: 1.3.6.1.4.1.25623.1.0.895000)

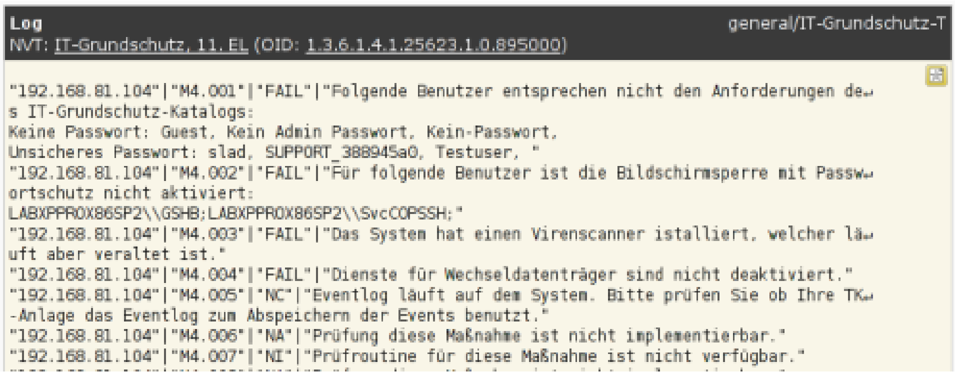
```
Prüfergebnisse gemäß IT-Grundschutz, 11. Ergänzungslieferung:


IT-Grundschutz M4.001: Passwortschutz für IT-Systeme
Ergebnis: nicht erfüllt
Details: Folgende Benutzer entsprechen nicht den Anforderungen des IT-Grundschutz-Katalogs↵
:
Keine Passwort: Guest, Kein Admin Passwort, Kein-Passwort,
Unsicheres Passwort: slad, SUPPORT_388945a0, Testuser,

IT-Grundschutz M4.002: Bildschirmsperre (Win)
Ergebnis: nicht erfüllt
Details: Für folgende Benutzer ist die Bildschirmsperre mit Passwortschutz nicht aktiviert↵
:
LABXPPROX86SP2\\GSHB;LABXPPROX86SP2\\SvcCOPSSH;

IT-Grundschutz M4.003: Einsatz von Viren-Schutzprogrammen
Ergebnis: nicht erfüllt
Details: Das System hat einen Virenscanner istalliert, welcher läuft aber veraltet ist.

IT-Grundschutz M4.004: Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Dat↵
enspeichern (Win)
Ergebnis: nicht erfüllt
Details: Dienste für Wechseldatenträger sind nicht deaktiviert.

IT-Grundschutz M4.005: Protokollierung der TK-Administrationsarbeiten
Ergebnis: unvollständig
Details: Eventlog läuft auf dem System. Bitte prüfen Sie ob Ihre TK-Anlage das Eventlog zu↵
m Abspeichern der Events benutzt.

IT-Grundschutz M4.006 Revision der TK-Anlagenkonfiguration
Ergebnis: Prüfung dieser Maßnahme ist nicht implementierbar.
Details: Prüfung diese Maßnahme ist nicht implementierbar.

IT-Grundschutz M4.007 Änderung voreingestellter Passwörter
```

For an import of the results of a IT-Grundschutz scan into one of these tools please contact the vendor of the corresponding tool. For additional questions please don't hesitate to contact the Greenbone Support.

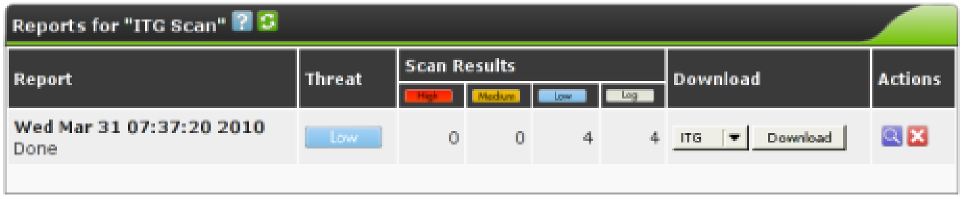
Result classes of IT-Grundschutz checks

The following result classes can occur for a check:

- ***Not fulfilled (FAIL)*:** It was detected that the target system does not fulfill the measure.
- ***Fulfilled (OK)*:** It was detected that the target system does fulfill the measure.
- ***Error (ERR)*:** It was not possible to execute the test routine properly. For example, some checks require credentials. If the credentials are missing, the check can not be executed for technical reasons. In case no credentials are provided many of the checks will have this status.
- ***Check of this measure is not available (NI)*:** In general it is assumed this measure can be automatically checked for, but an implementation is not yet available. For newly released "Ergänzungslieferungen" this is initially true for a number of measures. However, the Greenbone Security Feed is updated continuously, and eventually all measures will be implemented.
- ***Check of the measure is not implemented (NA)*:** A number of measures of the "IT-Grundschutzkataloge" are kept too general to create an explicit automatic check. Other measures describe checks that can only be done physically and thus also belong to this class of test that can't be implemented at all.



```
Log                                                          general/IT-Grundschutz-T
NVT: IT-Grundschutz, 11. EL (OID: 1.3.6.1.4.1.25623.1.0.895000)

"192.168.81.104"|"M4.001"|"FAIL"|"Folgende Benutzer entsprechen nicht den Anforderungen de↵
s IT-Grundschutz-Katalogs:
Keine Passwort: Guest, Kein Admin Passwort, Kein-Passwort,
Unsicheres Passwort: slad, SUPPORT_388945a0, Testuser, "
"192.168.81.104"|"M4.002"|"FAIL"|"Für folgende Benutzer ist die Bildschirmsperre mit Passw↵
ortschutz nicht aktiviert:
LABXPPROX86SP2\\GSHB;LABXPPROX86SP2\\SvcCOPSSH;"
"192.168.81.104"|"M4.003"|"FAIL"|"Das System hat einen Virenscanner istalliert, welcher lä↵
uft aber veraltet ist."
"192.168.81.104"|"M4.004"|"FAIL"|"Dienste für Wechseldatenträger sind nicht deaktiviert."
"192.168.81.104"|"M4.005"|"NC"|"Eventlog läuft auf dem System. Bitte prüfen Sie ob Ihre TK↵
-Anlage das Eventlog zum Abspeichern der Events benutzt."
"192.168.81.104"|"M4.006"|"NA"|"Prüfung diese Maßnahme ist nicht implementierbar."
"192.168.81.104"|"M4.007"|"NI"|"Prüfroutine für diese Maßnahme ist nicht verfügbar."
```



Reports for "ITG Scan"

Report	Threat	Scan Results				Download	Actions
		High	Medium	Low	Log		
Wed Mar 31 07:37:20 2010 Done	Low	0	0	4	4	ITG ▾ Download	

- ***Check not suited for the target system (NS)*:** Some measures refer exclusively to a special type of operating system. If the target system runs another operating system type, the measure does not apply and the result class is set to NS.
- ***This measure is deprecated (DEP)*:** Some updates ("Ergänzungslieferungen") removed some measures without a replacement. Old IDs of such deprecated measures are never re-used. So, the results marked as DEP can be safely ignored but the entries remain for completeness.

Supported measures

This overview refers to the current Ergänzungslieferung. The measure ID's link to the corresponding detailed information available on the website of BSI.

The following test types are distinguished:

- Remote: For the check it is only necessary to have network connection to the target system.
- Credentials: For the check is is required to use a account on the target system.

BSI reference	Title	Test type	Note
M4.2[26]	Screen lock	Credentials	Windows: Can only test for local accounts. Linux: Only default screen savers in Gnome and KDE.
M4.3[27]	Use of anti virus protection software	Credentials	
M4.4[28]	Compliant handling of drives for removable media and external data storage devices	Credentials	
M4.5[29]	Logging of telecommunication equipment	Credentials	
M4.7[30]	Changing of default passwords	Remote	Test only via SSH and Telnet.
M4.9[31]	Use of the seccurity mechanisms of XWindows	Credentials	
M4.14[32]	Mandatory password protection in Unix	Credentials	

Continued on next page

Table 9.1 – continued from previous page

BSI reference	Title	Test type	Note
M4.15[33]	Secure login	Credentials	
M4.16[34]	Access restrictions of user IDs and / or terminals	Credentials	
M4.17[35]	Locking and deleting unneeded accounts and terminals	Credentials	
M4.18[36]	Administrative and technical securing of access to monitoring and single-user mode	Credentials	
M4.19[37]	Restrictive allocation of attributes for UNIX system files and directories	Credentials	
M4.20[38]	Restrictive allocation of attributes for UNIX user files and directories	Credentials	
M4.21[39]	Preventing of unauthorized escalation of administrator rights	Credentials	
M4.22[40]	Preventing of loss of confidentiality of sensitive data in the UNIX system	Credentials	
M4.23[41]	Safe access of executable files	Credentials	
M4.33[42]	Use of a virus scanning program for storage media exchange and data transfer	Credentials	
M4.36[43]	Disabling of certain fax receiving phone numbers	Credentials	Cisco devices can only be tested via telnet because they do not support blowfish-cbc encryption.
M4.37[44]	Disabling of cetrain fax sending phone numbers	Credentials	Cisco devices can only be tested via telnet because they do not support blowfish-cbc encryption.
M4.40[45]	Preventing the unauthorized use of the computer microphone	Credentials	Only implemented for Linux. Under Windows it is not possible to determine the status of the microphone via registry/WMI.
M4.48[46]	Password protection if Windows systems	Credentials	
M4.49[47]	Securing of the the boot process of Windows systems	Credentials	
M4.52[48]	Equipment protection under Windows NT-based systems	Credentials	
M4.57[49]	Deactivation of automatic CD-ROM recognition	Credentials	
M4.80[50]	Sichere Zugriffsmechanismen bei Fernadministration	Remote	
M4.94[51]	Protection of web server files	Remote	
M4.96[52]	Disabling of DNS	Credentials	
M4.97[53]	One service per server	Remote	
M4.98[54]	Limit communication though a packet filter to a minimum	Credentials	Microsoft Windows Firewall is being tested. For Vista and newer any firewall that is installed comforming to the system.

Continued on next page

Table 9.1 – continued from previous page

BSI reference	Title	Test type	Note
M4.106[55]	Activation of system wide logging	Credentials	
M4.135[56]	Restrictive assigning of access rights to system files	Credentials	
M4.147[57]	Secure use of EFS under Windows	Credentials	
M4.200[58]	Use of USB storage media	Credentials	
M4.227[59]	Use of a local NTP server for time synchronization	Credentials	
M4.238[60]	Use of a local packet filter	Credentials	Microsoft Windows Firewall is being tested. For Vista and newer any firewall that is installed comforming to the system.
M4.244[61]	Secure system configuration of Windows client operating systems	Credentials	
M4.277[62]	Securing of the SMB, LDAP and RCP communication of Windows servers	Credentials	
M4.284[63]	Handling of services of Windows Server 2003	Credentials	
M4.285[64]	Uninstallation of unneeded client services of Windows Server 2003	Credentials	
M4.287[65]	Secure administration of VoIP middleware	Remote	
M4.300[66]	Information protection of printers, copies and multi-function equipment	Remote	
M4.305[67]	Use of storage quotas	Credentials	
M4.310[68]	Implementaion of LDAP access to file services	Remote	
M4.313[69]	Providing of secure domain controllers	Credentials	
M4.325[70]	Deletion of swap files	Credentials	
M4.326[71]	Providing the NTFS properties on a Samba file server	Credentials	
M4.328[72]	Secure base configuration of a Samba server	Credentials	
M4.331[73]	Secure configuration of the operating system for a samba server	Credentials	
M4.332[74]	Secure configuration of access controls of a samber server	Credentials	
M4.333[75]	Secure configuration of Winbind under Samba	Credentials	
M4.334[76]	SMB message signing and Samba	Credentials	
M4.338[77]	Use of Windows Vista and new file and registry virtulization	Credentials	Only a general test if file and registry virtulization is enabled.
M4.339[78]	Avoidance of unauthorized use of portable media under Windows Vista and later	Credentials	

Continued on next page

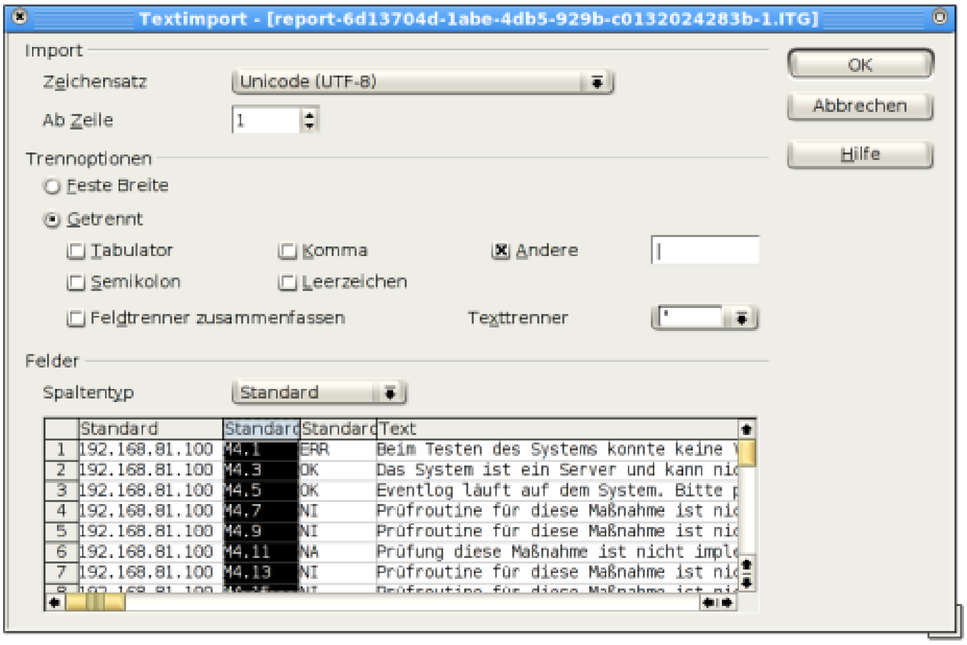
Table 9.1 – continued from previous page

BSI reference	Title	Test type	Note
M4.340[79]	Use of the Windows user account control UAC starting with Windows Vista	Credentials	
M4.341[80]	Integrity protection starting with Windows Vista	Credentials	Where possible technically implemented (active UAC and protected mode in different zones).
M4.342[81]	Activation of last access certificate stamp starting with Windows Vista	Credentials	
M4.344[82]	Monitoring of Windows Vista-, Windows 7 und Windows Server 2008-Systemen	Credentials	
M4.368[83]	Regular audits of the terminal server environemnt	Credentials	
M5.8[84]	Regular security check of the network	Remote	Only a message is being displayed that tests should be performed with up-to date plugins.
M5.17[85]	Use of the security mechanisms of NFS	Credentials	
M5.18[86]	Use of the security mechanisms of NIS	Credentials	
M5.19[87]	Use of the security mechanisms of sendmail	Remote	
M5.19[88]	Use of the security mechanisms of sendmail	Credentials	
M5.20[89]	Use of the security mechanisms of rlogin, rsh and rcp	Credentials	
M5.21[90]	Secure use of telnet, ftp, tftp and rexec	Credentials	
M5.34[91]	Use of one time passwords	Credentials	
M5.59[92]	Protection from DNS-spoofing with authentication mechanisms	Credentials	
M5.63[93]	Use of GnuPG or PGP	Credentials	
M5.64[94]	Secure shell	Remote	
M5.66[95]	Use of TLS/SSL	Remote	
M5.72[96]	Deactivation of not required net services	Credentials	Only displays the services in question.
M5.90[97]	Use of IPSec under Windows	Credentials	
M5.91[98]	Use of fersonal firewalls for clients	Credentials	Microsoft Windows Firewall is being tested. For Vista and newer any firewall that is installed comforming to the system. On Linux systems, displaying if the the iptables rules, if possible.
M5.109[99]	Use of a e-mail scanners on the mailserver	Remote	
M5.123[100]	Securing of the network commuication under Windows	Credentials	
M5.131[101]	Securing of the IP protocols under Windows Server 2003	Credentials	
M5.145[102]	Secure use of CUPS	Credentials	

Continued on next page

Table 9.1 – continued from previous page

BSI reference	Title	Test type	Note
M5.147[103]	Securing of the communication with directory services	Remote	


Textimport - [report-6d13704d-1abe-4db5-929b-c0132024283b-1.ITG]
OK
Abbrechen
Hilfe

Import

Zeichensatz: Unicode (UTF-8)

Ab Zeile: 1

Trennoptionen

○ Feste Breite

● Getrennt

☐ Tabulator ☐ Komma ☒ Andere |

☐ Semikolon ☐ Leerzeichen

☐ Feldtrenner zusammenfassen Texttrenner '

Felder

Spaltentyp: Standard

	Standard	Standard	Standard	Text
1	192.168.81.100	M4.1	ERR	Beim Testen des Systems konnte keine V
2	192.168.81.100	M4.3	OK	Das System ist ein Server und kann nic
3	192.168.81.100	M4.5	OK	Eventlog läuft auf dem System. Bitte p
4	192.168.81.100	M4.7	NI	Prüfroutine für diese Maßnahme ist nic
5	192.168.81.100	M4.9	NI	Prüfroutine für diese Maßnahme ist nic
6	192.168.81.100	M4.11	NA	Prüfung diese Maßnahme ist nicht imple
7	192.168.81.100	M4.13	NI	Prüfroutine für diese Maßnahme ist nic

[26] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04002.html

[27] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04003.html

[28] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04004.html

[29] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04005.html

[30] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04007.html

[31] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04009.html

[32] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04014.html

[33] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04015.html

[34] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04016.html

[35] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04017.html

[36] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04018.html

[37] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04019.html

[38] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04020.html

[39] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04021.html

[40] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04022.html

[41] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04023.html

[42] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04033.html

[43] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04036.html

[44] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04037.html

[45] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04040.html

[46] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04048.html

[47] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04049.html

[48] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04052.html

[49] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04057.html

[50] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04080.html

[51] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04094.html

[52] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04096.html

[53] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04097.html

[54] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04098.html

[55] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04106.html

[56] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04135.html

[57] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04147.html

[58] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04200.html

[59] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04227.html

[60] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04238.html

[61] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04244.html

[62] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04277.html

[63] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04284.html

[64] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04285.html

[65] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04287.html

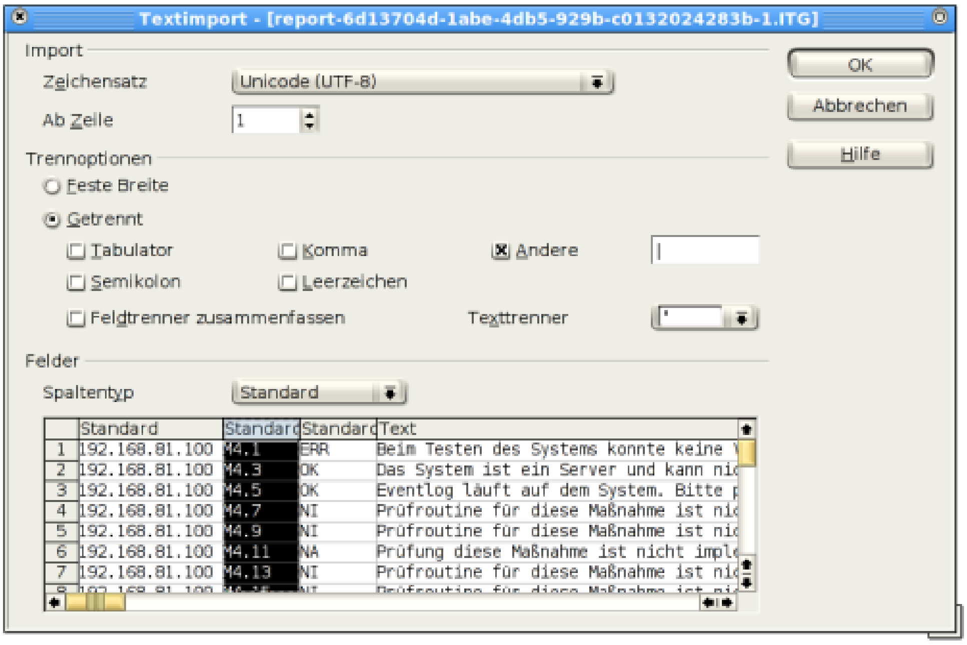
[66] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04300.html

[67] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04305.html

[68] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04310.html

[69] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04313.html

[70] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04325.html


Textimport - [report-6d13704d-1abe-4db5-929b-c0132024283b-1.ITG]
OK
Abbrechen
Hilfe

Import

Zeichensatz: Unicode (UTF-8)

Ab Zeile: 1

Trennoptionen

○ Feste Breite

● Getrennt

□ Tabulator □ Komma ☒ Andere: |

□ Semikolon □ Leerzeichen

□ Feldtrenner zusammenfassen Texttrenner: '

Felder

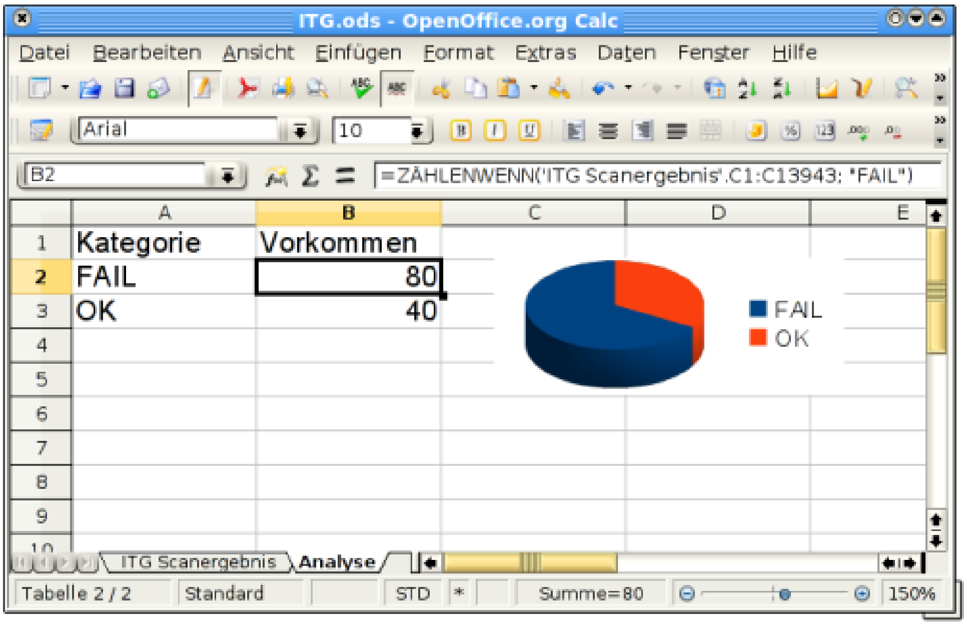
Spaltentyp: Standard

	Standard	Standard	Standard	Text
1	192.168.81.100	M4.1	ERR	Beim Testen des Systems konnte keine V
2	192.168.81.100	M4.3	OK	Das System ist ein Server und kann nic
3	192.168.81.100	M4.5	OK	Eventlog läuft auf dem System. Bitte p
4	192.168.81.100	M4.7	NI	Prüfroutine für diese Maßnahme ist nic
5	192.168.81.100	M4.9	NI	Prüfroutine für diese Maßnahme ist nic
6	192.168.81.100	M4.11	NA	Prüfung diese Maßnahme ist nicht imple
7	192.168.81.100	M4.13	NI	Prüfroutine für diese Maßnahme ist nic

9.2.2 PCI DSS

Introduction into vulnerability analysis and policy monitoring for the Payment Card Industry Data Security Standard (PCI DSS) with the Greenbone Security Manager.

[71] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04326.html
[72] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04328.html
[73] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04331.html
[74] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04332.html
[75] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04333.html
[76] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04334.html
[77] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04338.html
[78] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04339.html
[79] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04340.html
[80] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04341.html
[81] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04342.html
[82] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04344.html
[83] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04368.html
[84] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05008.html
[85] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05017.html
[86] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05018.html
[87] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05019.html
[88] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05019.html
[89] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05020.html
[90] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05021.html
[91] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05034.html
[92] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05059.html
[93] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05063.html
[94] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05064.html
[95] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05066.html
[96] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05072.html
[97] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05090.html
[98] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05091.html
[99] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05109.html
[100] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05123.html
[101] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05131.html
[102] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05145.html
[103] http://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05147.html


ITG.ods - OpenOffice.org Calc
Datei Bearbeiten Ansicht Einfügen Format Extras Daten Fenster Hilfe
Arial
10
B2
ITG Scanergebnis
Analyse
FAIL
OK

=ZÄHLENWENN('ITG Scanergebnis'.C1:C13943; "FAIL")

	A	B
1	Kategorie	Vorkommen
2	FAIL	80
3	OK	40

Tabelle 2 / 2 | Standard | STD | * | Summe=80 | 150%

Payment Card Industry Data Security Standard

The PCI DSS is a security standard for payment card transactions and is supported by the major payment systems MasterCard, Visa, AMEX, Discover and JCB.

All organizations that process card payments, store or transfer card data are required to perform compliance validation according to PCI DSS. Non-compliance or lack of validation means the risk of being fined or, ultimately, losing the ability to process payment cards.

The validation of compliance depends on the volume of card transactions. Here, service providers are usually classified as Level 1 Service Provider and they must, on a quarterly basis, validate their cardholder data environment by an independent scanning vendor approved by the PCI Security Standards Council (PCI SSC). In addition, an annual on-site PCI Security Audit has to be performed by an independent Qualified Security Assessor (QSA), also approved by the PCI SSC.

The “Approved Scanning Vendor” (ASV) is a service provider who performs a vulnerability scan of the cardholder data environment visible to the internet. As such the vulnerability scanners themselves can not be classified or certified as ASVs. However, they are tools for the ASV to perform the vulnerability scan using the approved process.

Greenbone Security Manager and PCI DSS

According to PCI DSS (Version 3.1, Requirement 11.2) two types of vulnerability scans are to be perfomred on a quarterly basis and after significant changes to the cardholder data environment. This includes the vulnerability scan conducted by the ASV explained above and an internal scan of the cardholder data environment. The latter scan may be performed by employees of the organization and requires no approval by the PCI SSC.

The Greenbone Security Manager (GSM) can perform both of these scans. The false positive management features help avoid significant work load of manual elimination of wrong alerts.

A merchant can use the GSM to check the security requirements prior to the ASV vulnerability scan in order to avoid costly re-scans.

This way, a merchant can use the GSM to check for PCI compliance on an ongoing basis even between the scans performed by the ASV.

Since security changes are stored immutable for audit compliance within the GSM, the correct security and compliance status can even be verified at all times in between the quarterly ASV scans.

Escalation methods can inform an external auditor as well as internal experts continuously about the security status. Summaries are sent to the responsible parties.

Policy Monitoring

In the same way the GSM checks the technical aspects of other policies periodically it can also check the system parameters according to the PCI DSS policy.

With a permanent background policy scan it is ensured that antivirus tools are not outdated or firewalls don't get deactivated without notice. Such parameters can be monitored and escalated in the same way as software vulnerabilities.

Advantages for merchant:

- Permanent policy monitoring
- Flexible escalation
- “False Positive” management
- Internal and external vulnerability scanning
- Complete vulnerability analysis according to PCI DSS for internal scans

Advantages for the ASV:

- “False Positive” Management
- Static scan configuration for re-scans
- Complete vulnerability analysis according to PCI DSS for external scans via internet
- Flexible reporting framework for individual scan reports

Greenbone Networks GmbH as the vendor of the GSM does not act as an ASV. But among Greenbone's business partners you will find security consultants that as an ASV at the same time and can introduce the GSM into your security process.

9.3 Special Policies

9.3.1 Mailserver Online Test

In September 2014 the Bavarian State Office for Data Protection performed an online test “Mailserver regarding STARTTLS, Perfect Forward Secrecy and Hartbleed[104]”. The organizations that were found to be affected by this test were asked to remove the security risks.

Using Greenbone Security Manager or OpenVAS respectively an organziation can test themselves if their own mail servers comply with the security criteria. For this follow these steps:

1. Import the following scan config: onlinepruefung-mailserver-scanconfig.xml[105].
2. Configure a new port with the port range *T:25*.
3. Configure a target containing the mailservers to be tested and select the port list created in the previous step. Depending on the the network settings it could make sense to use “Consider Alive” as Alive Test.
4. Create a task with the target created above and the imported scan config.
5. Start the scan. It can take 30-40 Minutes because generally the scanner has to wait for some data from the mailservers a bit longer.

[104] http://www.lda.bayern.de/onlinepruefung/emailserver.html
[105] http://www.greenbone.net/download/scanconfigs/onlinepruefung-mailserver-scanconfig.xml

6. Finally you will get a scan report with different log entries for each mailserver. The missing StartTLS will initially only be displayed as a log message as it is a policy question how it should be assessed. For Example an override for this NVT can be created defining it as a high risk. The override can then be expanded to all hosts and possibly all tasks.
7. Should monitoring be established, a schedule for this task can be created (i.e. every week on Sundays) as well as an alert (i.e. an email). Combined with the respective overrides an automated warning system is being created in the background.

9.4 TLS-Map

The TLS (Transport Layer Security) protocol ensures the confidentiality, authenticity and integrity of communication in insecure networks. It establishes confidential communication between sender and receiver, for example web server and web browser. In the past years various security holes were detected for the often used protocol TLS 1.0 and used by attackers to actually read the communication.

With the GSM it is possible to identify systems that offer services using SSL/TLS protocols. Additionally GSM detects the protocol versions and offered encryption algorithms. Further details about the service can be achieved in case it can be properly identified.

9.4.1 Preparations

For a simplified export of your scan results we prepared a special Report Format Plugin. The resulting data file makes it easy to further process the data.

Please download and import the TLS-Map Report Format Plugin[107].

Remind that you need to activate the plugin after import for making it available. For this, click on the wrench icon and set “Active” to “yes” in the dialog. Finally click “Save Report Format”.

9.4.2 Checking for TLS

For an overview on TLS usage in your network or on single systems we recommend to use one of the following scan configurations:

- TLS-Map Scan Config[108]

  This scan configuration identifies the used protocol versions and the offered encryption algorithms, but does not try to identify in-depth details of the service.

- TLS-Map with service detection[109]

  This scan configuration identifies the used protocol versions and the offered encryption algorithms and additionally tries to identify in-depth details of the service. This identification takes more time and produces more network traffic compared to the above simple scan configuration.

Import one or both of these scan configurations according to your needs.

Now choose a suitable list of ports to be scanned. Pay attention that all ports your are interested in are covered by the list. The more extensive the list the longer the scan will take, but this may also detect services at unusual ports.

Via menu “Port Lists” you can choose from the pre-configured lists or create you own.

Consider for the choice that the TLS protocol is based on the TCP protocol. A port list with UDP port hence will slow down the scan without benefits. If you want to cover any TCP port, then you should choose “All TCP”.

[107] http://www.greenbone.net/download/rfps/tls-map-1.0.0.xml
[108] http://www.greenbone.net/download/scanconfigs/tls-map-scan-config.xml
[109] http://www.greenbone.net/download/scanconfigs/tls-map-app-detection-scan-config.xml

Next, create a target covering the systems and/or networks you want to check. Link this target with the port list you have choosen in the “New Target” dialog.

Create a new task and configure the imported scan configuration and the target. Start the new task.

9.4.3 Exporting the scan results

As soon as the status of the started task changes to “Done”, the scan is complete and the results can be exported.

For the export, open the report of the task, for example by clicking on the date in column “Last” in the task overview.

Change to the “Report: Summary and Download” page via the report menu and then select the “TLS Map” report format plugin for the “Full report” and select download.

The report will be prepared in CSV format. You can open this file with convenient application, for example with a spreadsheet tool.

The file contains one line per port and systems where a SSL/TLS protocol is offered:

```
IP,Host,Port,TLS-Version,Ciphers,Application-CPE
192.168.12.34,www.local,443,TLSv1.0;SSLv3,SSL3_RSA_RC4_128_SHA;TLS1_RSA_RC4_128_SHA,
  cpe:/a:apache:http_server:2.2.22;cpe:/a:php:php:5.4.4
192.168.56.78,www2.local,443,TLSv1.0;SSLv3,SSL3_RSA_RC4_128_SHA;TLS1_RSA_RC4_128_SHA,
  cpe:/a:apache:http_server:2.2.22
```

Separated by commans, each line contains the following information:

- IP: The IP address of the system where the service was detected.
- Host: The DNS name of the system in case it is available
- Port: The port where the service was detected.
- TLS-Version: The protocol version offered by the service. In case more than one is offered, the versions are separated with semicolos.
- Ciphers: The encryption algorithms offered by the service. In case more than one is offered, the algorithms are separated with semicolons.
- Application-CPE: The detected application in CPE format. In case more than one is identified, the applications are separated with semicolons.

9.5 Conficker Search

Conficker[110] is a computer worm that occured in fall 2008. It threatens Windows operating systems and caused numerous network failures with significant financial damage. The worm takes advantage of a security hole in the operating system and is self-updating.

Microsoft Bulletin MS08-067[111] describes the most important security hole that is exploited by Conficker to attack the corresponding systems.

9.5.1 Search methods for vulnerability and infection

Using the Greenbone Security Manager two methods are recommended for the search:

- Non-invasive search for the security holes described by Microsoft in Bulletin MS08-067, including the Conficker worm.

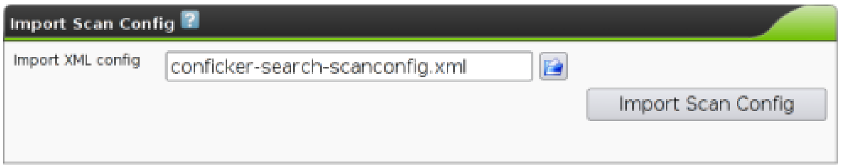
[110] http://en.wikipedia.org/wiki/Conficker
[111] http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx

- Invasive search for the security holes described by Microsoft in Bulletin MS08-067, including the Conficker worm.

The first method is able to detect the presence of the vulnerability. The second method goes as far as exploiting the vulnerability to be certain that it is indeed present. Admittedly, this may cause outages of the corresponding systems and thus should be executed with appropriate prudence.

9.5.2 Execute search for vulnerability and Conficker

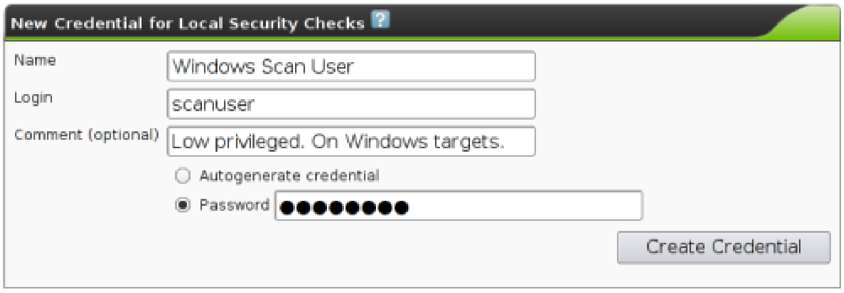
- Import the scan configuration Conficker Search[112] or, for the invasive search, the scan configuration Invasive Conficker Search[113].



Import Scan Config

Import XML config: conficker-search-scanconfig.xml

- If the target systems do not allow anonymous access, create credentials to provide the scan engine with access to the target systems. If not done yet, create a corresponding user account on the Windows systems (a low privileged user account is sufficient).



New Credential for Local Security Checks

Name: Windows Scan User

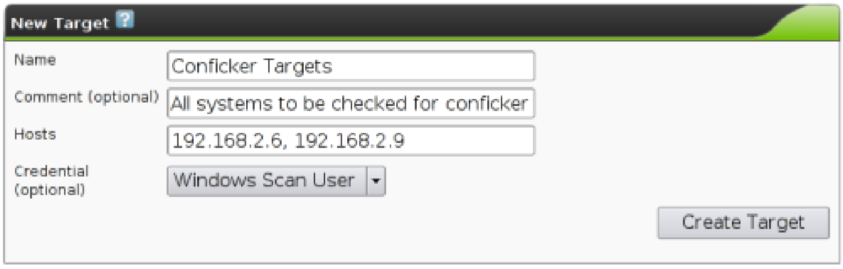
Login: scanuser

Comment (optional): Low privileged. On Windows targets.

○ Autogenerate credential

● Password ●●●●●●●●

- Define the target systems (targets) and, if applicable, choose the respective credentials.



New Target

Name: Conficker Targets

Comment (optional): All systems to be checked for conficker

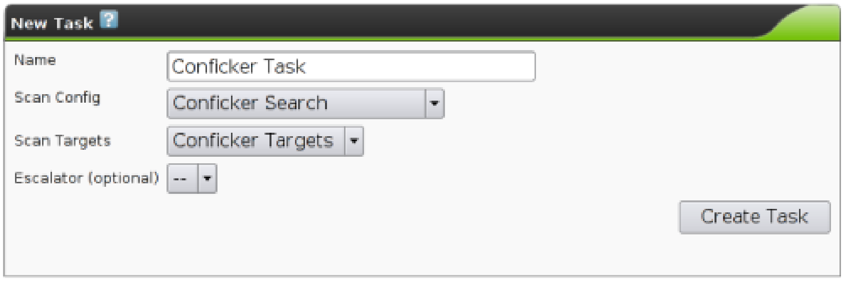
Hosts: 192.168.2.6, 192.168.2.9

Credential (optional): Windows Scan User

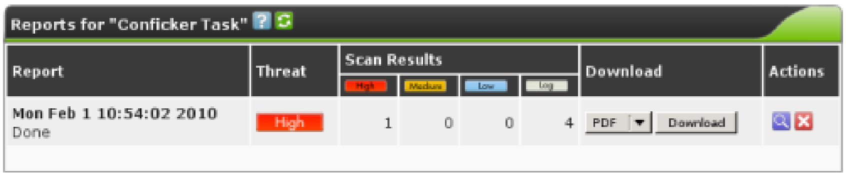
- Now you can create the actual task. This means to combine the imported scan configuration with the newly created targets.
- The search is started by clicking on ▶ of the respective task. It can take a while for the scan to complete. To update the view with the current progress, click on ⟳.
- As soon as the status changes to "Done" the complete report is available. At any time you can review the intermediate results. Here is an example for a system where the vendor security update for MS08-67 has not been installed.

[112] http://www.greenbone.net/download/scanconfigs/conficker-search-scanconfig-v4.xml

[113] http://www.greenbone.net/download/scanconfigs/conficker-search-scanconfig-invasive-v4.xml



Name	Conficker Task
Scan Config	Conficker Search
Scan Targets	Conficker Targets
Escalator (optional)	--



Report	Threat	Scan Results				Download	Actions
		High	Medium	Low	Log		
Mon Feb 1 10:54:02 2010 Done	High	1	0	0	4	PDF Download	

9.6 OVAL System Characteristics

The Open Vulnerability and Assessment Language (OVAL)[114] is an approach for a standardized description of the (security) state of an IT system. OVAL files describe a vulnerability and define tests to identify the state in which a system is vulnerable. They usually refer to specific version of software products for which a known vulnerability exists.

This means that in order to check for vulnerabilities described in an OVAL definition, information about the current state of the system is needed. This information is collected in a standardized format as well — the OVAL System Characteristics (SC).

There are a number of solutions which perform checks based on OVAL definitions and SC files. OVAL definitions are provided by various vendors[115]. MITRE provides the OVAL Repository[116] with more than 13,000 entries.

9.6.1 OVAL Adoption Program

Greenbone is an official OVAL Adopter and Greenbone Security Manager is registered as a "Systems Characteristics Producer".

See also: OVAL Adoption Program[117].

Supported are OVAL versions 5.3 to 5.10. Should any wrong, missing or incomplete OVAL element be found, users are encouraged to provide feedback to the Greenbone support team. The OVAL-SC implementation of the Greenbone solution allows to activate updates within a single day and therefore provides timely improvements for the users.

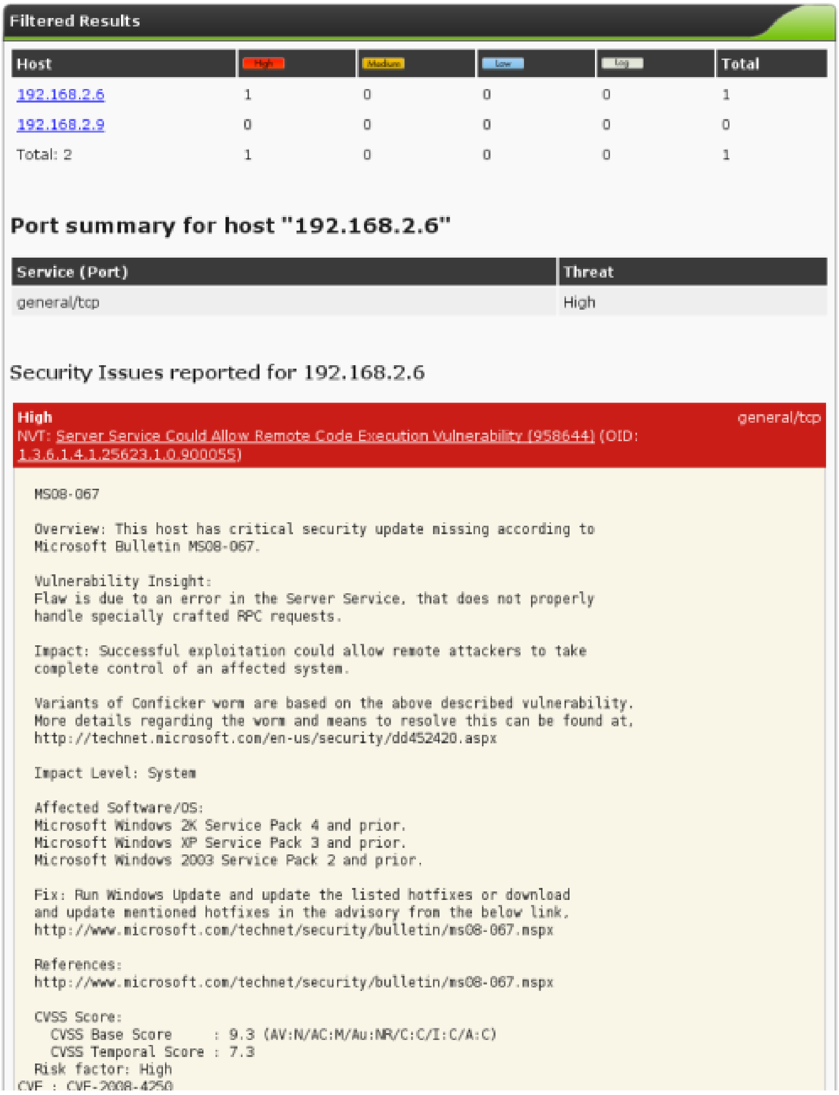
9.6.2 Collecting Scan Results as OVAL SCs

> During a scan the Greenbone Security Manager collects large amounts of data about the target system. This information is managed in an optimized data pool. Parts of this information are usable as a component of an OVAL System Characteristics.

The creation of OVAL SC files is not enabled by default but has to be explicitly enabled. The following scan configuration can be used to achieve this: collect-oval-sc-v2.xml[118].

Import the scan configuration in the GSM:

[114] http://oval.mitre.org/
[115] http://oval.mitre.org/repository/about/other_repositories.html
[116] http://oval.mitre.org/repository/
[117] http://oval.mitre.org/adoption/
[118] http://www.greenbone.net/download/scanconfigs/collect-oval-sc-v2.xml



Filtered Results

Host	High	Medium	Low	Log	Total
192.168.2.6	1	0	0	0	1
192.168.2.9	0	0	0	0	0
Total: 2	1	0	0	0	1

Port summary for host "192.168.2.6"

Service (Port)	Threat
general/tcp	High

Security Issues reported for 192.168.2.6

High general/tcp
NVT: Server Service Could Allow Remote Code Execution Vulnerability (958644) (OID: 1.3.6.1.4.1.25623.1.0.900055)

```
  MS08-067

  Overview: This host has critical security update missing according to
  Microsoft Bulletin MS08-067.

  Vulnerability Insight:
  Flaw is due to an error in the Server Service, that does not properly
  handle specially crafted RPC requests.

  Impact: Successful exploitation could allow remote attackers to take
  complete control of an affected system.

  Variants of Conficker worm are based on the above described vulnerability.
  More details regarding the worm and means to resolve this can be found at,
  http://technet.microsoft.com/en-us/security/dd452420.aspx

  Impact Level: System

  Affected Software/OS:
  Microsoft Windows 2K Service Pack 4 and prior.
  Microsoft Windows XP Service Pack 3 and prior.
  Microsoft Windows 2003 Service Pack 2 and prior.

  Fix: Run Windows Update and update the listed hotfixes or download
  and update mentioned hotfixes in the advisory from the below link.
  http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx

  References:
  http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx

  CVSS Score:
    CVSS Base Score     : 9.3 (AV:N/AC:M/Au:NR/C:C/I:C/A:C)
    CVSS Temporal Score : 7.3
  Risk factor: High
CVE : CVE-2008-4250
```

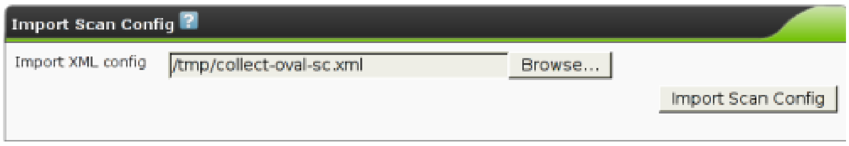
The new scan configuration is now shown in the list:

The most comprehensive results of a target system can be collected using authenticated scans. For this you need to create an account on the target system. Ensure that the account has the necessary privileges. For unixoid systems an account with low privileges is usually sufficient, for Windows system administrative privileges are required.

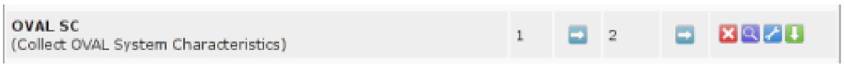
The following example shows the creation of a Linux target. For a Windows target the credential must be set in the SMB field instead of SSH.

Now create the task, which you can start immediately.

The scan itself is quite fast because the scan configuration is optimized to collect only the specific data needed for generating the System Characteristics file.


Import Scan Config

Import XML config: /tmp/collect-oval-sc.xml


OVAL SC
(Collect OVAL System Characteristics)

The results are returned a log information. If you adjust your filter you can see the OVAL System Characteristics in XML formatted for easy readability:

Please note: If you have collected data from a large number of target systems this view may become hard to read.

9.6.3 Exporting OVAL SCs

> OVAL SC files are defined in a way that one file can contain only information about one system. Using the Greenbone Security Manager you can collect a large number of System Characteristics from many different systems in one single step.

Because of this we provide two Report Format Plugins:

- OVAL System Characteristics: Produces a single SC file in the XML format.
- OVAL System Characteristics Archive: Can be used for an arbitrary number of System Characteristics, which will be collected in a ZIP file. The names of the individual SC files will contain the IP address of the target system.

Both plugins are available for download on the Report Formats page[119].

Import the report format plugins, verify the signature and activate them. For detailed information about this process, please refer to: *Report Plugins* (page 88).

You can now download the results in the format you require for further processing. Select the format "OVAL-SC" or "OVAL-SC archive" in the "Full report" line:

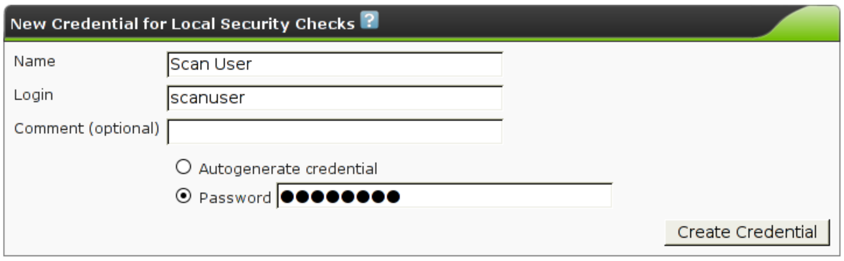
The ZIP archives look as follows:

9.6.4 Example: Using OVAL SCs with ovaldi

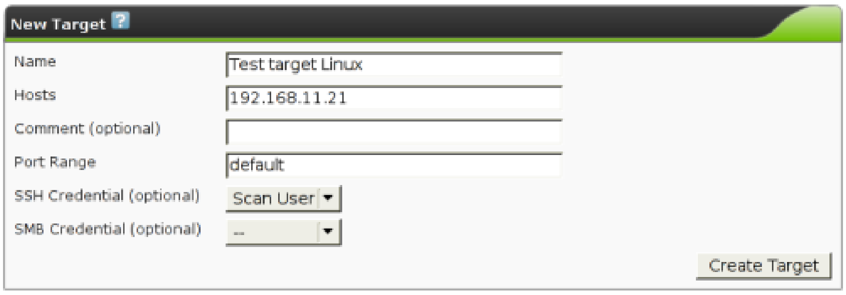
> The MITRE organization not only provides the OVAL standard but also provides a reference implementation for local OVAL checks. The OVAL Interpreter ovaldi[120] is available under an Open Source license.

By using the Greenbone Security Manager to provide OVAL System Characteristics it is easy to use ovaldi on Linux to check a Windows system — or the other way round.

[119] http://www.greenbone.net/technology/report_formats.html
[120] http://oval.mitre.org/language/interpreter.html

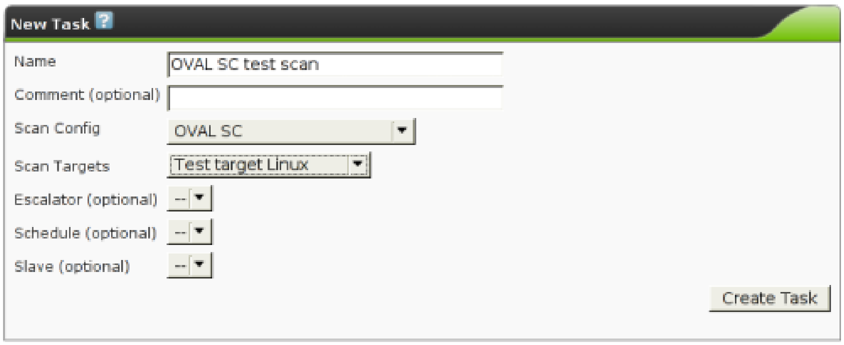

New Credential for Local Security Checks

Name: Scan User
Login: scanuser
Comment (optional):
○ Autogenerate credential
● Password ●●●●●●●●●



New Target

Name	Test target Linux
Hosts	192.168.11.21
Comment (optional)	
Port Range	default
SSH Credential (optional)	Scan User
SMB Credential (optional)	--



New Task

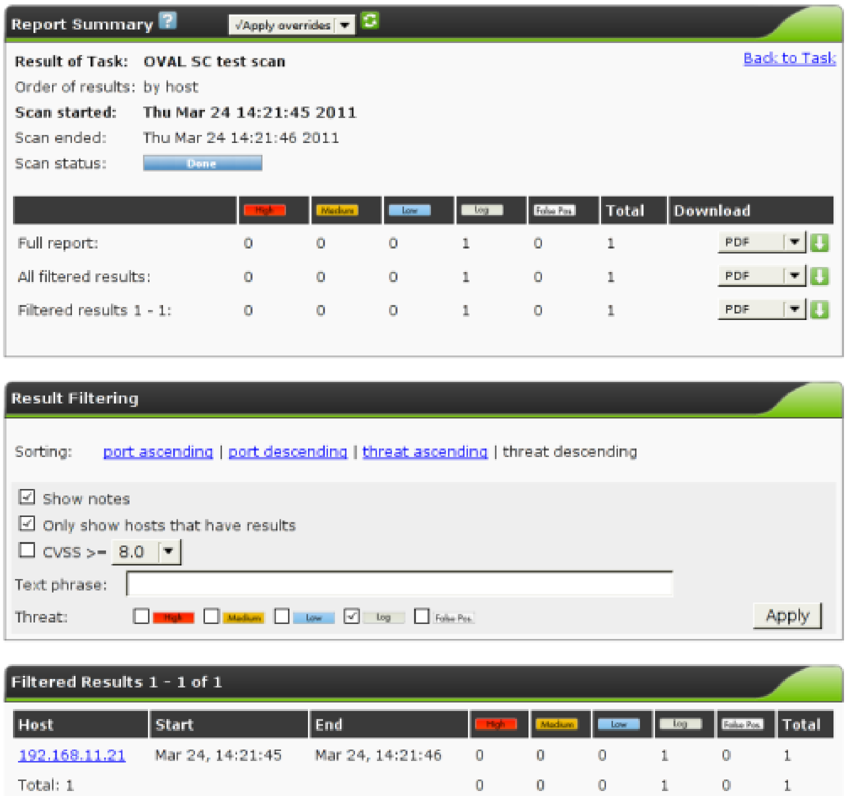
Name	OVAL SC test scan
Comment (optional)	
Scan Config	OVAL SC
Scan Targets	Test target Linux
Escalator (optional)	--
Schedule (optional)	--
Slave (optional)	--

For example, if the target system you tested above was a Debian Linux system, you can now download the official Debian OVAL definitions 2010[121] and execute the test ("false" means that a condition was not met, i.e. a vulnerability does not exist on the target).

Ovaldi automatically creates a HTML and XML version of the plain text output as shown below: oval-sc-debian-squeeze-sample-ovaldi-results.html[122] (102 KByte) and oval-sc-debian-squeeze-sample-ovaldi-results.xml[123] (4.2 MByte). To run the tests additionally download the files oval-definitions-2010.xml[124] and oval-sc-debian-squeeze-sample.xml[125].

```
$ cd /tmp
$ ovaldi -m -o /tmp/oval-definitions-2010.xml \
  -i /tmp/oval-sc-debian-squeeze-sample.xml \
  -a /usr/share/ovaldi/xml/

----------------------------------------------------
OVAL Definition Interpreter
Version: 5.10.1 Build: 2
Build date: Sep 11 2012 07:49:59
Copyright (c) 2002-2012 - The MITRE Corporation
----------------------------------------------------

Start Time: Tue Sep 11 12:12:52 2012

 ** parsing /tmp/oval-definitions-2010.xml file.
    - validating xml schema.
 ** checking schema version
    - Schema version - 5.3
 ** skipping Schematron validation
 ** parsing /tmp/oval-sc-debian-lenny-sample.xml for analysis.
    - validating xml schema.
 ** running the OVAL Definition analysis.
    Analyzing definition:  FINISHED
 ** applying directives to OVAL results.
 ** OVAL definition results.
```

[121] http://www.debian.org/security/oval/oval-definitions-2010.xml
[122] http://www.greenbone.net/download/misc/oval-sc-debian-squeeze-sample-ovaldi-results.html
[123] http://www.greenbone.net/download/misc/oval-sc-debian-squeeze-sample-ovaldi-results.xml
[124] http://www.debian.org/security/oval/oval-definitions-2010.xml
[125] http://www.greenbone.net/download/misc/oval-sc-debian-squeeze-sample.xml



Report Summary

Back to Task

Result of Task: **OVAL SC test scan**

Order of results: by host

Scan started: **Thu Mar 24 14:21:45 2011**

Scan ended: Thu Mar 24 14:21:46 2011

Scan status: Done

	High	Medium	Low	Log	False Pos	Total	Download
Full report:	0	0	0	1	0	1	PDF ▾
All filtered results:	0	0	0	1	0	1	PDF ▾
Filtered results 1 - 1:	0	0	0	1	0	1	PDF ▾

Result Filtering

Sorting: port ascending | port descending | threat ascending | threat descending

☑ Show notes

☑ Only show hosts that have results

☐ CVSS >= 8.0 ▾

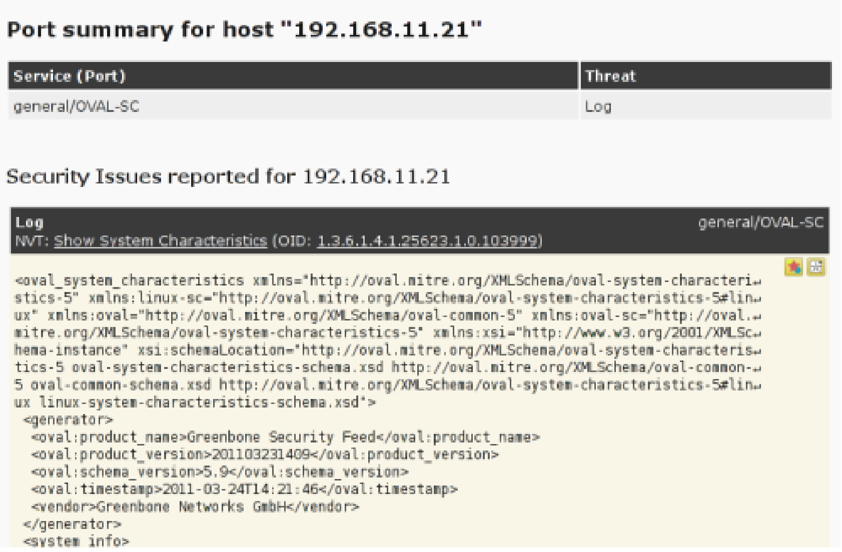
Text phrase:

Threat: ☐ High ☐ Medium ☐ Low ☑ Log ☐ False Pos.

Filtered Results 1 - 1 of 1

Host	Start	End	High	Medium	Low	Log	False Pos	Total
192.168.11.21	Mar 24, 14:21:45	Mar 24, 14:21:46	0	0	0	1	0	1
Total: 1			0	0	0	1	0	1

```
OVAL Id                                         Result
-------------------------------------------------------
oval:org.debian:def:1965                        false
oval:org.debian:def:1966                        false
oval:org.debian:def:1967                        false
oval:org.debian:def:1968                        false
oval:org.debian:def:1969                        false
oval:org.debian:def:1970                        false
oval:org.debian:def:1971                        false
oval:org.debian:def:1972                        false
oval:org.debian:def:1973                        false
oval:org.debian:def:1974                        false
...
```



Port summary for host "192.168.11.21"

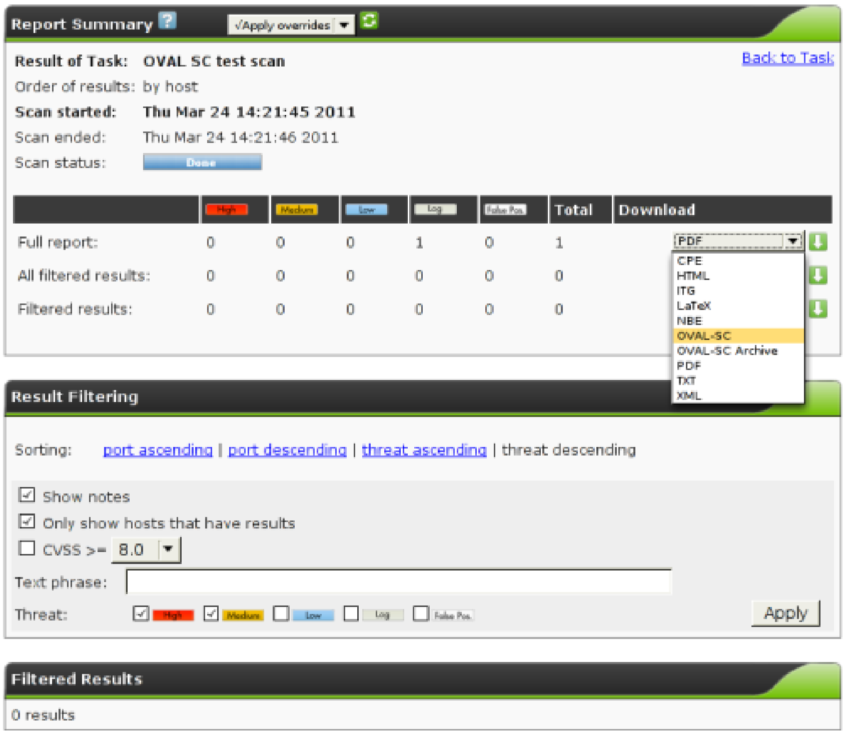
Service (Port)	Threat
general/OVAL-SC	Log

Security Issues reported for 192.168.11.21

Log general/OVAL-SC

NVT: Show System Characteristics (OID: 1.3.6.1.4.1.25623.1.0.103999)

```
<oval_system_characteristics xmlns="http://oval.mitre.org/XMLSchema/oval-system-characteri↵
stics-5" xmlns:linux-sc="http://oval.mitre.org/XMLSchema/oval-system-characteristics-5#lin↵
ux" xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5" xmlns:oval-sc="http://oval.↵
mitre.org/XMLSchema/oval-system-characteristics-5" xmlns:xsi="http://www.w3.org/2001/XMLSc↵
hema-instance" xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-system-characteris↵
tics-5 oval-system-characteristics-schema.xsd http://oval.mitre.org/XMLSchema/oval-common-↵
5 oval-common-schema.xsd http://oval.mitre.org/XMLSchema/oval-system-characteristics-5#lin↵
ux linux-system-characteristics-schema.xsd">
 <generator>
  <oval:product_name>Greenbone Security Feed</oval:product_name>
  <oval:product_version>201103231409</oval:product_version>
  <oval:schema_version>5.9</oval:schema_version>
  <oval:timestamp>2011-03-24T14:21:46</oval:timestamp>
  <vendor>Greenbone Networks GmbH</vendor>
 </generator>
 <system_info>
```



Report Summary

√Apply overrides

Result of Task: OVAL SC test scan

Back to Task

Order of results: by host

Scan started: Thu Mar 24 14:21:45 2011

Scan ended: Thu Mar 24 14:21:46 2011

Scan status: Done

	High	Medium	Low	Log	False Pos.	Total	Download
Full report:	0	0	0	1	0	1	PDF
All filtered results:	0	0	0	0	0	0	
Filtered results:	0	0	0	0	0	0	

Result Filtering

Sorting: port ascending | port descending | threat ascending | threat descending

☑ Show notes

☑ Only show hosts that have results

□ CVSS >= 8.0

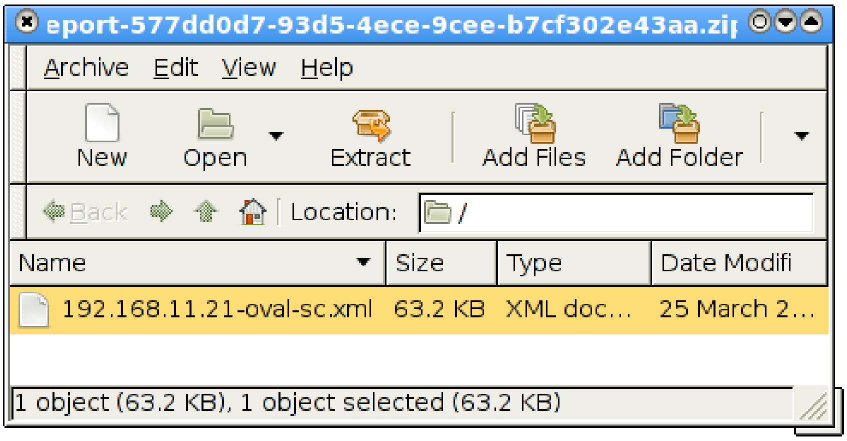
Text phrase:

Threat: ☑ High ☑ Medium □ Low □ Log □ False Pos.

Apply

Filtered Results

0 results



Location: /

Name	Size	Type	Date Modifi
192.168.11.21-oval-sc.xml	63.2 KB	XML doc...	25 March 2...

1 object (63.2 KB), 1 object selected (63.2 KB)

```
   oval:org.debian:def:2124                    false
   oval:org.debian:def:2125                    false
   oval:org.debian:def:2126                    false
   oval:org.debian:def:2127                    false
   oval:org.debian:def:2128                    false
   oval:org.debian:def:2129                    false
   oval:org.debian:def:2130                    false
   oval:org.debian:def:2131                    false
   oval:org.debian:def:2132                    false
   oval:org.debian:def:2133                    false
   -------------------------------------------------------


 ** finished evaluating OVAL definitions.

 ** saving OVAL results to results.xml.
 ** running OVAL Results xsl: /usr/share/ovaldi/xml//results_to_html.xsl.

 ----------------------------------------------------
```

If the target system was a Microsoft Windows system, you can use the definitions provided by MITRE[126] and execute the test ("false" means that a condition was not met, i.e. a vulnerability does not exist on the target).

Ovaldi automatically creates a HTML and XML version of the plain text output as shown below: oval-sc-windows-xp-sample-ovaldi-results.html[127] (23 KByte) and oval-sc-windows-xp-sample-ovaldi-results.xml[128] (159 KByte).

To run the tests additionally download the files windows.xml[129] and oval-sc-windows-xp-sample.xml[130].

```
$ cd /tmp
$ ovaldi -m -o /tmp/windows.xml \
  -i /tmp/oval-sc-windows-xp-sample.xml \
  -a /usr/share/ovaldi/xml/

----------------------------------------------------
OVAL Definition Interpreter
Version: 5.10.1 Build: 2
Build date: Sep 11 2012 07:49:59
Copyright (c) 2002-2012 - The MITRE Corporation
----------------------------------------------------

Start Time: Tue Sep 11 15:57:55 2012

 ** parsing /tmp/windows.xml file.
    - validating xml schema.
 ** checking schema version
    - Schema version - 5.10
 ** skipping Schematron validation
 ** parsing /tmp/oval-sc-windows-xp-sample.xml for analysis.
    - validating xml schema.
 ** running the OVAL Definition analysis.
      Analyzing definition:  FINISHED
 ** applying directives to OVAL results.
 ** OVAL definition results.

  OVAL Id                                   Result
  -------------------------------------------------------
  oval:org.mitre.oval:def:754               true
  oval:org.mitre.oval:def:15339             false
  oval:org.mitre.oval:def:15465             false
  oval:org.mitre.oval:def:15452             false
  oval:org.mitre.oval:def:15377             false
  oval:org.mitre.oval:def:15346             false
  oval:org.mitre.oval:def:15173             false
  oval:org.mitre.oval:def:15057             false
  oval:org.mitre.oval:def:15546             false
  oval:org.mitre.oval:def:14566             false
  oval:org.mitre.oval:def:720               false
  oval:org.mitre.oval:def:627               false
  oval:org.mitre.oval:def:286               false
  oval:org.mitre.oval:def:748               false
  oval:org.mitre.oval:def:684               false
  oval:org.mitre.oval:def:396               false
  oval:org.mitre.oval:def:1205              false
  oval:org.mitre.oval:def:679               false
  oval:org.mitre.oval:def:165               false
```

[126] http://oval.mitre.org/rep-data/5.10/org.mitre.oval/p/family/windows.xml
[127] http://www.greenbone.net/download/misc/oval-sc-windows-xp-sample-ovaldi-results.html
[128] http://www.greenbone.net/download/misc/oval-sc-windows-xp-sample-ovaldi-results.xml
[129] http://oval.mitre.org/rep-data/5.10/org.mitre.oval/p/family/windows.xml
[130] http://www.greenbone.net/download/misc/oval-sc-windows-xp-sample.xml

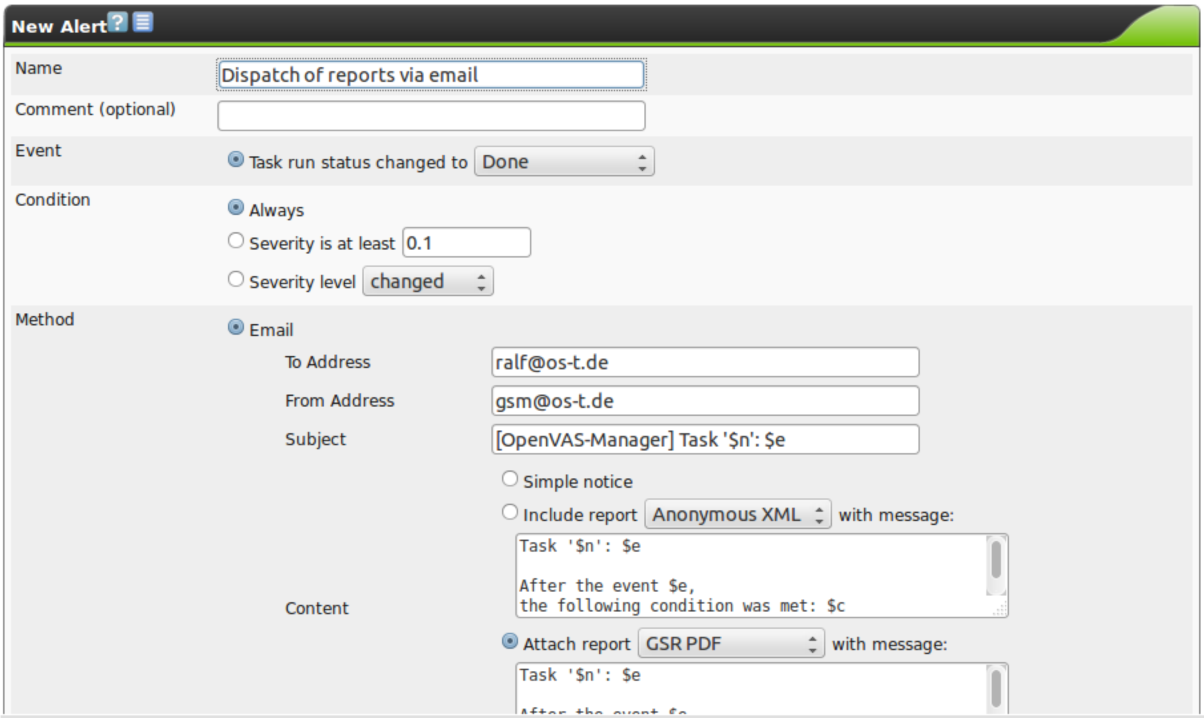
```
 oval:org.mitre.oval:def:565             false
 oval:org.mitre.oval:def:289             false
 oval:org.mitre.oval:def:730             false
 oval:org.mitre.oval:def:1162            false
 oval:org.mitre.oval:def:2041            false
 oval:org.mitre.oval:def:1946            false
 oval:org.mitre.oval:def:1815            false
 oval:org.mitre.oval:def:1282            false
 oval:org.mitre.oval:def:1804            false
 oval:org.mitre.oval:def:1469            false
 oval:org.mitre.oval:def:718             false
 oval:org.mitre.oval:def:347             false
 oval:org.mitre.oval:def:283             false
 oval:org.mitre.oval:def:282             false
 -------------------------------------------------------


** finished evaluating OVAL definitions.

** saving OVAL results to results.xml.
** running OVAL Results xsl: /usr/share/ovaldi/xml/results_to_html.xsl.

----------------------------------------------------
```

CHAPTER 10

Alerts

With the use of alerts the state and results of a scan can be sent to others systems automatically. Alerts are anchored within the system in a way that each configured event will trigger an action, for example, when a task is started or completed. Additionally this can be tied to a condition. This could be the discovery of a vulnerability of a severity greater than 9. If met, an email or a SNMP trap can be triggered.

To create an alert change to *Configuration/Alerts*. Now add a new alert ★.



New Alert

Name: Dispatch of reports via email

Comment (optional):

Event: ● Task run status changed to Done

Condition:
● Always
○ Severity is at least 0.1
○ Severity level changed

Method: ● Email

To Address: ralf@os-t.de

From Address: gsm@os-t.de

Subject: [OpenVAS-Manager] Task '$n': $e

Content:
○ Simple notice
○ Include report Anonymous XML with message:

```
Task '$n': $e

After the event $e,
the following condition was met: $c
```

● Attach report GSR PDF with message:

```
Task '$n': $e
```

Fig. 10.1: Alerts offer various alerting options.

Now, the following can be defined:

Name: The name, describing the alert, can be freely chosen

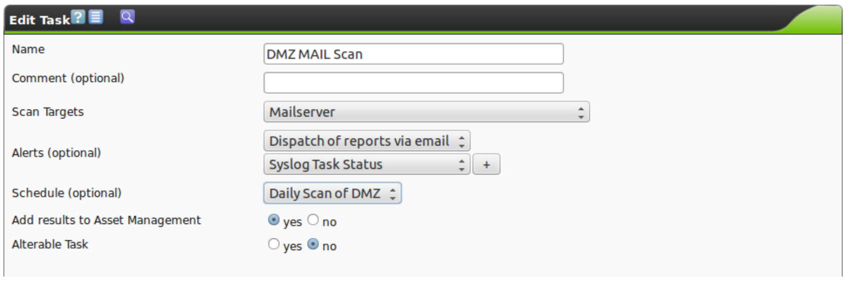
Comment: The optional comment can contain additional information.

Event: Here the event, for which the alert message is being sent, is being defined. For example, this can occur when the status of a task changes.

Condition: Here additional conditions, that have to be met, are being defined. The alert message can occur:

- Always

- Only when at minimum a specific severity level is reached.
- If the severity level changes, increases or decreases.



Edit Task

Name	DMZ MAIL Scan
Comment (optional)	
Scan Targets	Mailserver
Alerts (optional)	Dispatch of reports via email Syslog Task Status +
Schedule (optional)	Daily Scan of DMZ
Add results to Asset Management	● yes ○ no
Alterable Task	○ yes ● no

Fig. 10.2: Alerts must be activated in their respective task.

Method: Here the method for the alert is selected. Only one method per alert can be chosen. If different alerts for the same event should be triggered, multiple alerts must be created and linked to the same task.

Email This is the most powerful and most used method. To use this method the mailserver to be used must be defined in the GSM command line (see section *Mail Server* (page 25)). Then you can chose between the following options:

To Address: This is the email address to which the email should be sent to.

From Address: This is the sender address of the generated email.

Subject: This is the subject of the email. You can use variables like $n (task name) and $e (event description).

Content: Here the content of the email can be defined:

Simple Notice: This is only a simple description of the event.

Include Report: If the event for the completion of the task (Default: Done) is selected the report can be included in the email. Here a report format that uses the content type `text/*` can be chosen as an email does not support binary content directly. Additionally you can modify the contents of the email message. Within the message you may use variables:

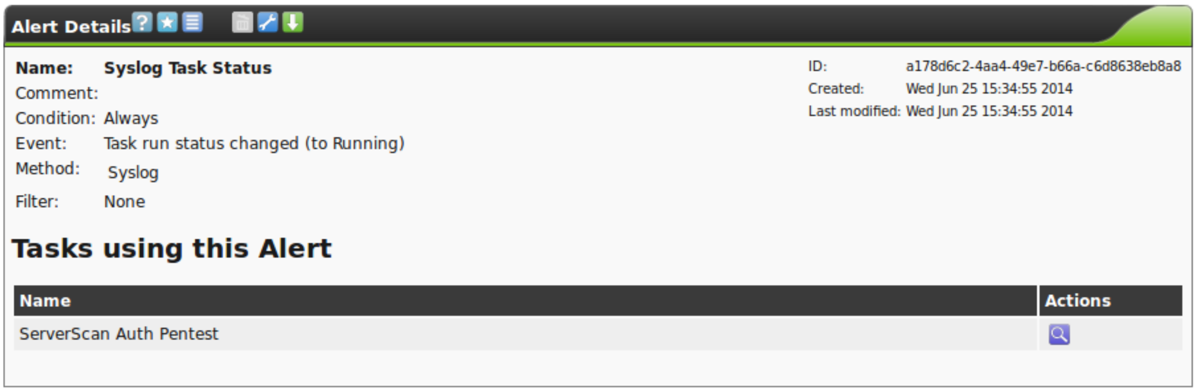
- $c condtion description
- $e event description
- $F name of filter
- $f filter term
- $H host summary
- $i report text
- $n task name
- $r report format name
- $t a note if the report was truncated
- $z timezone

Attach Report: If the event for the completion of the task (Default: Done) is selected the report can be attached to the email. Here any report format can be chosen. The report will be attached in its correct MIME type to the generated email. PDF is possible as well. Additionally you can modify the contents of the email message. The same variables may be used.

System Logger This method allows for the sending of the alert to a Syslog daemon or via a SNMP trap automatically. The Syslog server as well as the SNMP trap service are defined via the command line (see section *Central Logging Server* (page 25) and *SNMP* (page 26)).

HTTP Get With the HTTP Get method, for example, an SMS text message or a message to a trouble ticket system can be sent automatically. The following variables can be used when specifying the URL:

- `$n`: Name of the task
- `$e`: Description of the event (Start, Stop, Done)
- `$c`: Description of the condition that occurred
- `$$`: The $ symbol



Alert Details

Name:	Syslog Task Status
Comment:	
Condition:	Always
Event:	Task run status changed (to Running)
Method:	Syslog
Filter:	None

ID:	a178d6c2-4aa4-49e7-b66a-c6d8638eb8a8
Created:	Wed Jun 25 15:34:55 2014
Last modified:	Wed Jun 25 15:34:55 2014

Tasks using this Alert

Name	Actions
ServerScan Auth Pentest	🔍

Fig. 10.3: In an alert its use within different tasks can be referenced.

Sourcefire Connector Here the data can be sent automatically to a Sourcefire Defense Center. For more information see section *Sourcefire Defence Center* (page 218).

verinice.PRO Connector Here the data can be sent automatically to a verinice.PRO installation. For more information see section *Verinice* (page 208).

Report Result Filter Finally the results can be limited with an additional filter. A filter must be created and saved prior (see section *Powerfilter* (page 139)).

For the alert to be used afterwards, a specific task definition must be created (see figure *Alerts must be activated in their respective task.* (page 134)). To do so edit the respective task. This change of the task is also allowed for already defined and used tasks as it does not have any effect on already created reports.

Afterwards the respective alert displays that it is in use as well (see figure *In an alert its use within different tasks can be referenced.* (page 135)).

CHAPTER 11

GUI Concepts

This chapter covers recurring concepts when using the web user interface of the Greenbone Security Manager. This includes standard icons, Powerfilters, tags and the graphics in the Secinfo dashboard.

11.1 Icons

The web user interface uses recurring icons for the execution of identical actions. The reference of these icons results from the context of the current view.

- Display context aware help.
- Display a list of current objects.
- Create a new object. It could be a user, a target, a task, permission or a filter.
- Move an object to the trash can.
- Edit an object.
- Copy/Clone a resource.
- Export a resource as GSM object. This object can then be imported on another GSM.
- Refresh the page.
- Expand or collapse additional information, for example, the Powerfilter in the view.
- Delete an object irrevocably.
- Jump to the next object (page) in a view.
- Jump to the last object (page) in a view.
- Other users have permission to access the object as well.

Other icons can only be accessed in a certain context. This applies to the following icons:

- Start of a currently not running task.
- Stop a currently running task. All discovered results will be written to the database.
- Resume a stopped task.
- Enable or disable overrides.
- Indicates if a fix for a vulnerability exists.
- Indicates a vendor patch.
- Indicates a workaround.
- Indicates no solution exists.
- Indicates that a scan configuration is being amended with additional NVTs automatically.

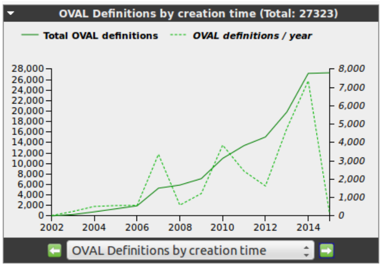
- ➡ Indicates that a scan configuration is not activating new NVTs automatically.

11.2 Charts

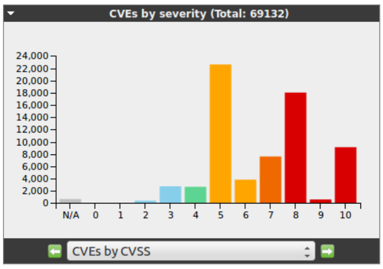
The charts in the SecInfo dashboard can be customized. This allows to display and format the SecInfo data in different ways. The created graphs can be downloaded and included into other documents.

There are four different chart types available:

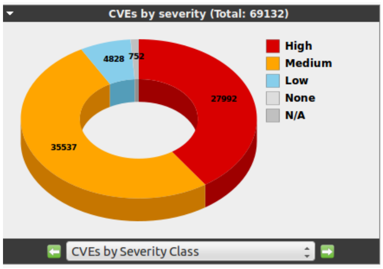
- Line chart



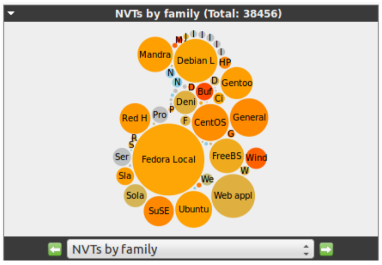
- Bar chart



- Donut chart



- Bubble chart



The contents of the charts can be selected via the drop down menu at the bottom of the chart. This immediately also changes the chart type automatically. Downloading the pictures or a copy can be selected through the context menu at the top left of the chart.

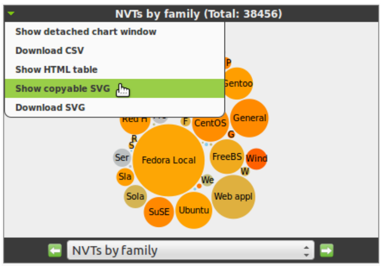
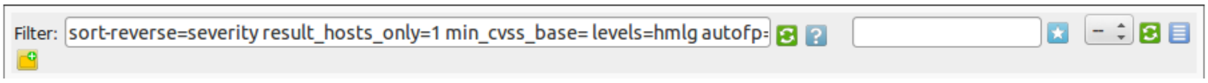


Fig. 11.1: The chart context menu allows for the download of a chart.

11.3 Powerfilter

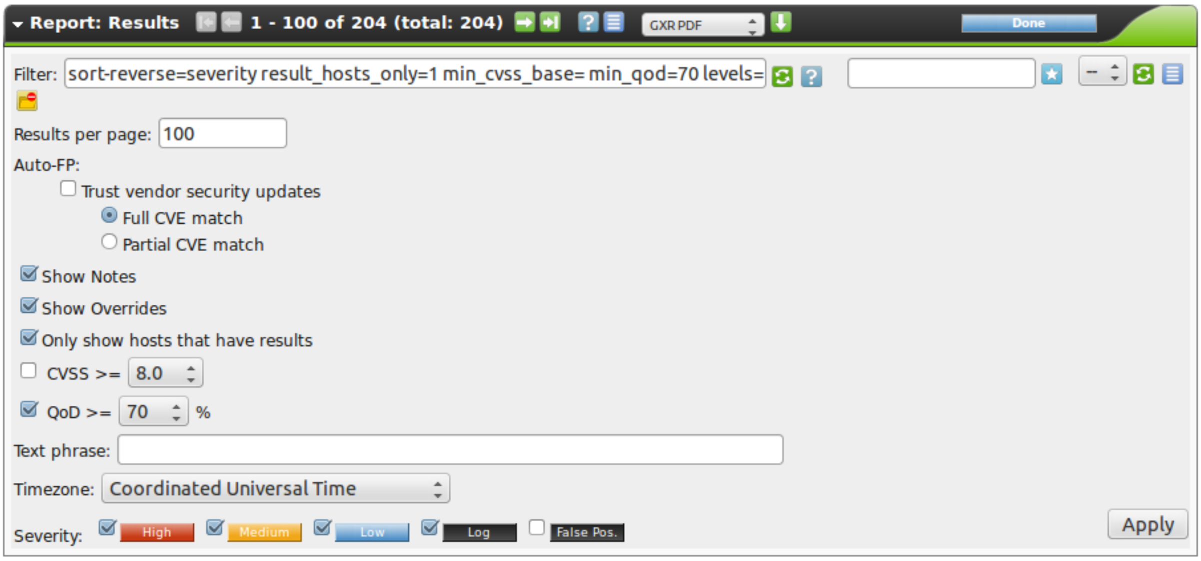
Almost every screen in the web user interface offers the possibility to filter the information displayed. The required entries can be performed in the filter bar at the top of the web user interface.



Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= levels=hmlg autofp=

Fig. 11.2: The Powerfilter offers filtering of the displayed results everywhere.

The filter bar can be expanded by ⊞. Then multiple context aware parameters are being displayed that are being combined to become the Powerfilter. They can be edited in the filter bar directly.



Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= min_qod=70 levels=

Results per page: 100

Auto-FP:

- ☐ Trust vendor security updates
  - ● Full CVE match
  - ○ Partial CVE match

☑ Show Notes

☑ Show Overrides

☑ Only show hosts that have results

☐ CVSS >= 8.0

☑ QoD >= 70 %

Text phrase:

Timezone: Coordinated Universal Time

Severity: ☑ High ☑ Medium ☑ Low ☑ Log ☐ False Pos.

Apply

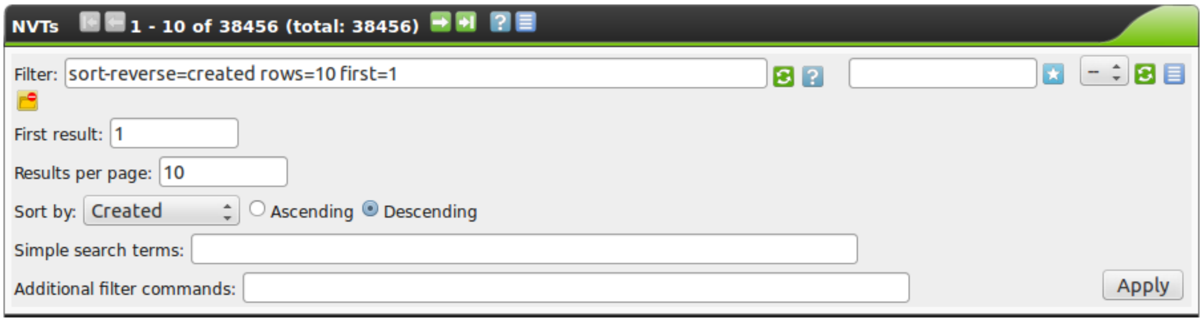
Fig. 11.3: The Powerfilter can be expanded.

Thereby the Powerfilter is context aware again. Should NVTs or targets being filtered more or less options are available respectively after expanding.

Note:

The Powerfilter is not case sensitive.

A typical Powerfilter search could search for all CVE-2009-2906 vulnerabilities within the 192.168.155.0/24 network.



NVTs 1 - 10 of 38456 (total: 38456)

Filter: sort-reverse=created rows=10 first=1

First result: 1

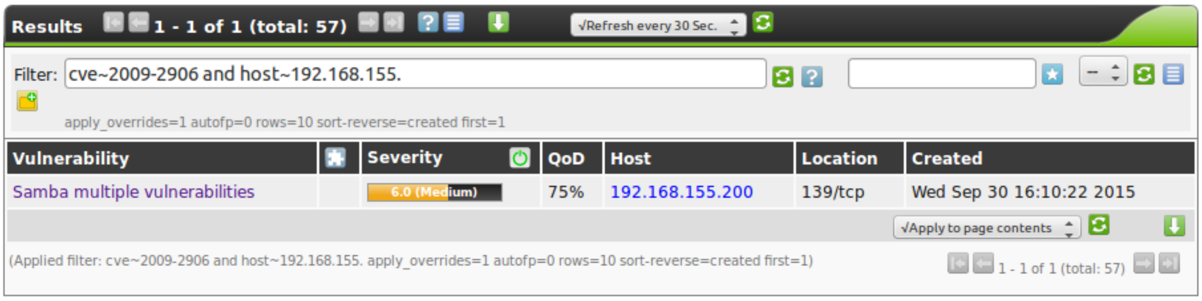
Results per page: 10

Sort by: Created ○ Ascending ● Descending

Simple search terms:

Additional filter commands:

Fig. 11.4: The options of the Powerfilter are context aware.



Results 1 - 1 of 1 (total: 57) √Refresh every 30 Sec.

Filter: cve~2009-2906 and host~192.168.155.

apply_overrides=1 autofp=0 rows=10 sort-reverse=created first=1

Vulnerability		Severity	QoD	Host	Location	Created
Samba multiple vulnerabilities		6.0 (Medium)	75%	192.168.155.200	139/tcp	Wed Sep 30 16:10:22 2015

(Applied filter: cve~2009-2906 and host~192.168.155. apply_overrides=1 autofp=0 rows=10 sort-reverse=created first=1)

1 - 1 of 1 (total: 57)

Fig. 11.5: Powerfilters may search for CVEs

11.3.1 Components

The possible components of the Powerfilter depend on its context. In general the specification of the following parameters is always possible:

***rows*:** Enter the amount of the results to be displayed. Mostly the value is *rows=10*. Entering a value of `-1` will display all results. Entering a value of `-2` will use the value that was pre-set in *My Settings* under *Rows Per Page*.

***first*:** Sets from which position the results should be displayed. If a search returns 50 results but only 10 should be displayed at the same time, *rows=10 first=11* displays the second 10 results.

***sort*:** Defines the column that should be used for sorting the results (*sort=name*). The results are being sorted ascending. The name of the column can mostly be deducted from the name of the column. By clicking the column the name of the column can be verified. Typical column names are:

- *name*
- *severity*
- *host*
- *location*

The column names will be changed to small caps and spaces to underscores. Additionally a couple of other fields are available.

- *uuid*: The uuid of a result
- *comment*: A possible comment
- *modified*: Date and time of the last modification
- *created*: Data and time of the creation

***sort-reverse*:** Defines the column that should be used for sorting the results (*sort-reverse=name*). The results will be sorted descending.

***tag*:** Selects only the results with a specific Tag (see also *Tags* (page 143)). It can be filtered by a specific tag value (*tag="server:mail"*) or search only for the tag (*tag="server"*). Regular expressions are also allowed.

Note: By filtering using tags custom categories can be created and used in the filters. This allows for versatile and granular filter functionality!

When specifying these components many operators can be used:

- = equals i.e. rows=10
- ~ contains i.e. name~admin
- < less than i.e. created<-1 w older than a week
- > greater than i.e. created>-1 w younger than a week
- :RegEx i.e. name:admin$

There are a couple of special features. If the value is omitted after the equal sign all results will be displayed where this value is not set:

```
comment=
```

shows all results without a comment.

If the column that should be searched is omitted all columns will be searched:

```
=192.168.15.5
```

This searches if at least one column contains the search string.

The data is usually *or* combined. This can be specifically specified with the key word `or`. To achieve an and-combination the keyword *and* needs to be specified. Using *not* will negate the filter.

Date specifications

Date specifications in the Powerfilter can be absolute or relative. An absolute data specification has the following format:

```
2014-05-26T13h50
```

The time can be omitted:

```
2014-05-26
```

The time of 12:00am will be assumed automatically. The date specification can be used in the search filter i.e. *created>2014-05-26*.

Relative time specifications are always calculated in relation to the current time. Positive time specification are interpreted as being in the future. Time specification in the past are defined with a prepended minus (-). For time periods the following letters can be used:

- s second
- m minute
- h hour
- d day
- w week
- m month (30 days)
- y year (365 days)

To view the results of the past 5 days enter *-5d*. A combination *5d1h* is not permitted. This is to be replaced with *121h* respectively.

To limit the time period , i.e. month, for which information should be displayed the following expression can be used:

```
modified>2014-06-01 and modified<2014-07-01
```

Text phrases

In general, additionally text phrases that are being searched for can be specified. Then only results are being displayed in which the text phrases where found. If the text phrases or not limited to a column (*name=text*) all columns will be searched. This means that also columns that are hidden from the current view will be searched as well.

The following examples can be useful:

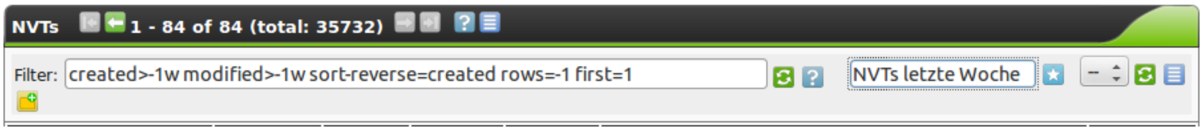
`overflow` Finds all results that contain the word `overflow`. This applies to both `Overflow` as well as `Bufferoverflow`. Also `192.168.0.1` will find `192.168.0.1` as well as `192.168.0.100`.

`remote exploit` Will find all results containing `remote` or `exploit`. Of course results that contain both words will be displayed as well.

`remote and exploit` Both words must be found in a result in any column. The results do not have to be found in the same column.

`"remote exploit"` The exact string is being searched for and not the individual words.

`regexp 192\.168\.[0-9]+.1` The regex is being searched for.


NVTs 1 - 84 of 84 (total: 35732)

Filter: created>-1w modified>-1w sort-reverse=created rows=-1 first=1

NVTs letzte Woche

Fig. 11.6: Often used Powerfilters can be saved and retrieved again.

11.3.2 Saving and Management

Interesting and often used filters can be saved as well. This simplifies their re-use. For example, to display the NVTs that were modified or added to the feed last week, in the GUI select *SecInfo Management* followed by *NVTs*. Then edit the Powerfilter so that it has the following content (see figure *Often used Powerfilters can be saved and retrieved again.* (page 142)):

```
Created>-1w or modified>-1w sort-reverse=created rows=1 first=1
```

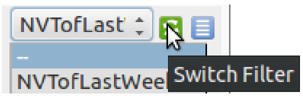
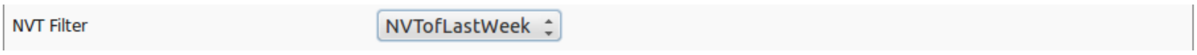


Fig. 11.7: The filters can be selected via the drop down box.

This displays all the NVTs that were created or modified last week. This filter can now be given a name. Use the field to the right of the Powerfilter. Enter the name and confirm with ★. The filter is now being saved and can be selected via the drop down box next to it.

To use a previously saved filter use the drop down box and confirm afterwards by clicking *Switch Filter* ↻ (see figure *The filters can be selected via the drop down box.* (page 142)). If Java script is activated the filter is executed immediately after selection from the drop down box.

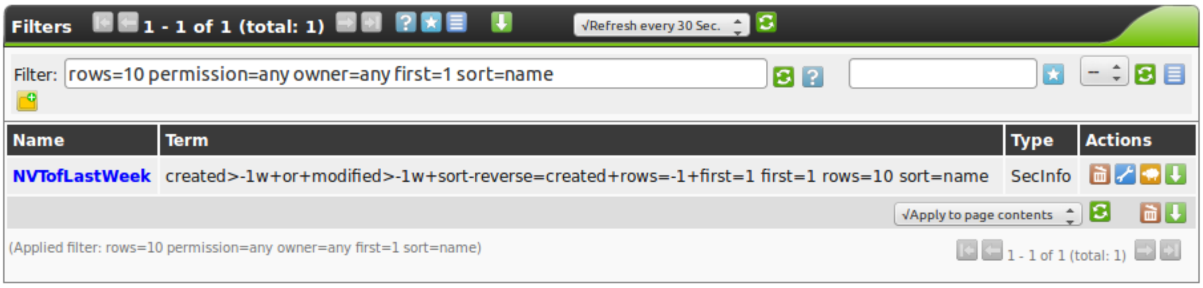
If a specific filter should always be activated in a specific view it can be done in the user settings (see also chapter My Settings (page 185)). In this example (see figure *Often used filters can be set up as default filter in the user settings.* (page 143)) it is the *NVT Filter*.



NVT Filter	NVTofLastWeek

Fig. 11.8: Often used filters can be set up as default filter in the user settings.

All saved filters can be managed in *Configuration/Filters*. Here, filters can be deleted, edited, cloned and exported as GSM object for import into other appliances.



Filters 1 - 1 of 1 (total: 1)

√Refresh every 30 Sec.

Filter: rows=10 permission=any owner=any first=1 sort=name

Name	Term	Type	Actions
NVTofLastWeek	created>-1w+or+modified>-1w+sort-reverse=created+rows=-1+first=1 first=1 rows=10 sort=name	SecInfo	

√Apply to page contents

(Applied filter: rows=10 permission=any owner=any first=1 sort=name)

1 - 1 of 1 (total: 1)

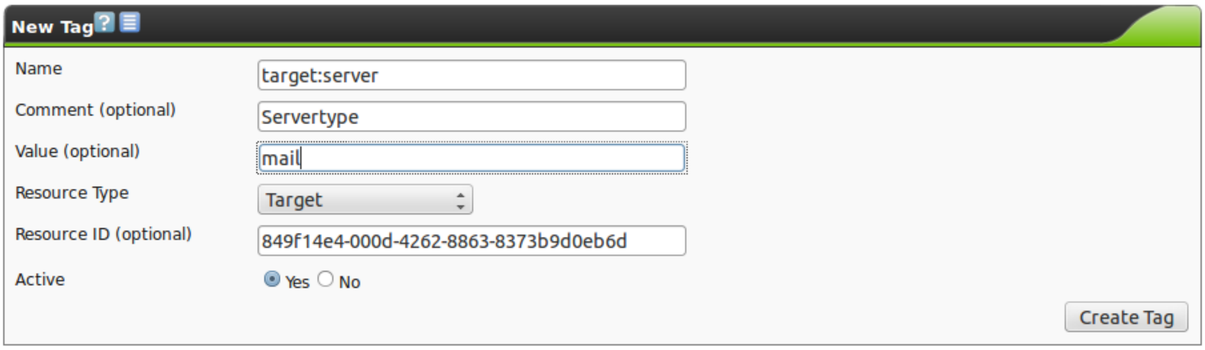
Fig. 11.9: All filters can be easily managed.

These filters can then be used to filter results of events for the alerts as well.

Filters can be shared.

11.4 Tags

Tags are discretionary information that can be linked to any resource. Tags are simply created directly with the resources. Then the tags can be used to filter objects respectively with the help of the Powerfilter (see section *Powerfilter* (page 139)). This presents very powerful and granular filter possibilities.



New Tag

Name	target:server
Comment (optional)	Servertype
Value (optional)	mail
Resource Type	Target
Resource ID (optional)	849f14e4-000d-4262-8863-8373b9d0eb6d
Active	● Yes ○ No

Fig. 11.10: Tags are discretionary strings that can be assigned a value.

Afterwards these tags can be used in filter expressions. With the filter `tag=target:server` the specific tag must be set in order to be included. The assigned value is irrelevant and can be empty. With `tag="target:server=mail"` the exact tag with the respective value must be set.

CHAPTER 12

Scan Configuration

The GSM appliance comes with various pre-defined scan configurations. However, they can be customized and expanded by your on configurations. The following configurations are already available from Greenbone:

Empty This is an empty template.

Discovery Only NVTs are used that provide information of the target system. No vulnerabilities are being detected.

Host Discovery Only NVTs are used that discover target systems. This scan only reports the list of systems discovered.

System Discovery Only NVTs are used that discover target systems including installed operating systems and hardware in use.

Full and Fast For many environments this is the best option to start with. This configuration is based on the information gathered in the prior port scan and uses almost all plugins. Only plugins are used that will not damage the target system. Plugins are optimized in the best possible way to keep the potential false negative rate especially low. The other configurations only provide more value only in rare cases but with much more required effort.

Full and fast ultimate This configuration expands the **Full and Fast** configuration with plugins that could disrupt services or systems or even cause shut downs.

Full and very deep This configuration differs from the **Full and Fast** configuration in the results of the port scan not having an impact on the selection of the plugins. Therefore plugins will be used that will have to wait for a timeout. This scan is very slow.

Full and very deep ultimate This configuration adds the dangerous plugins that could cause possible service or system disruptions to the **Full and very deep** configuration. This scan is also very slow.

The available scan configurations can be viewed under *Configuration/Scan Configs*. Remember that by default only the first 10 configurations are always displayed.

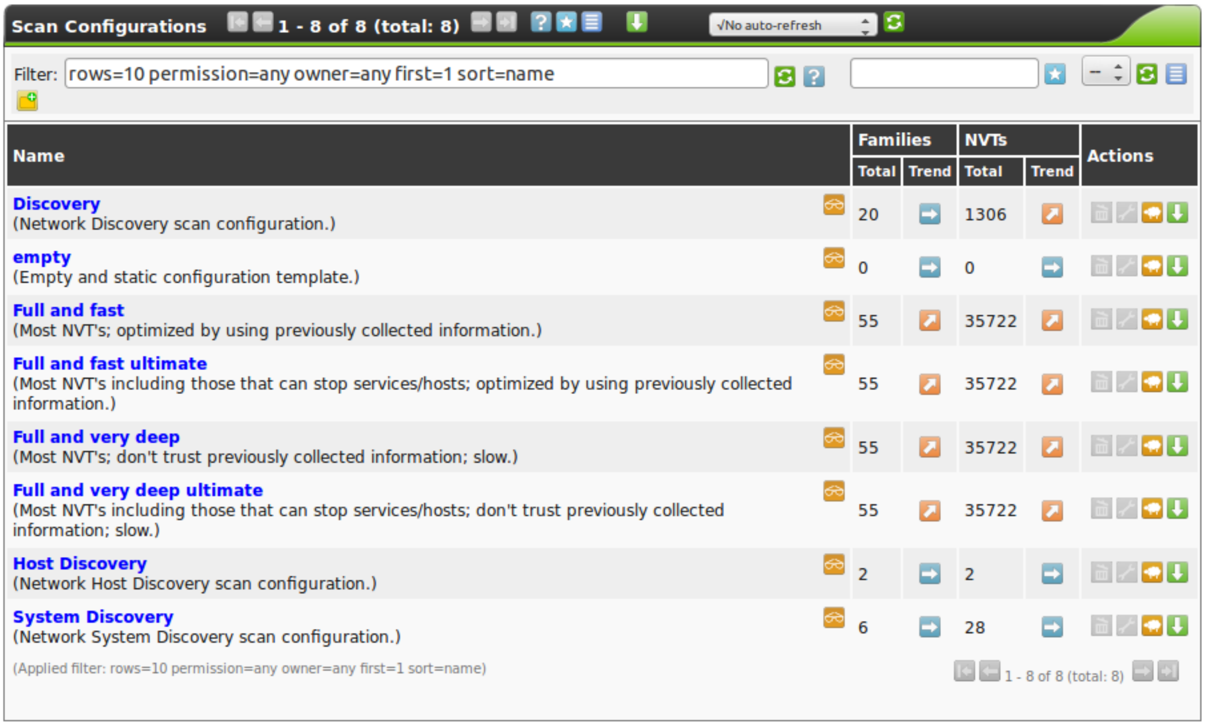
In figure *The GSM comes with various scan configurations.* (page 146) one can identify how many NVT families and how many NVYs are activated in in a configuration. Additionally it shows the trend if a scan configuration was configured dynamically ↗ or statically ➡.

Greenbone publishes new plugins regularly (NVTs). Also new NVT families can be introduced through the Greenbone Security Feed.

- ↗ dynamic

  Scan configurations that are configured dynamically will include and activate new NVT families and new NVTs of the respective activated families automatically after a NVT Feed update. This ensures that new NVTs are available immediately and without any interaction by the administrator.

- ➡ static



Scan Configurations 1 - 8 of 8 (total: 8) √No auto-refresh

Filter: rows=10 permission=any owner=any first=1 sort=name

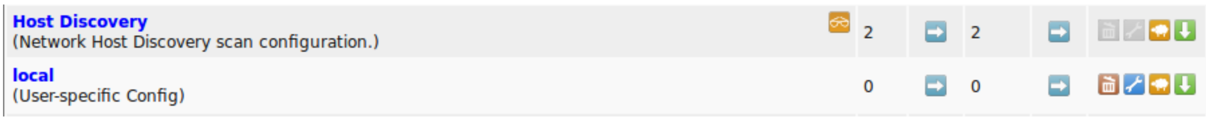
Name	Families		NVTs		Actions
	Total	Trend	Total	Trend	
Discovery (Network Discovery scan configuration.)	20	→	1306	↗	
empty (Empty and static configuration template.)	0	→	0	→	
Full and fast (Most NVT's; optimized by using previously collected information.)	55	↗	35722	↗	
Full and fast ultimate (Most NVT's including those that can stop services/hosts; optimized by using previously collected information.)	55	↗	35722	↗	
Full and very deep (Most NVT's; don't trust previously collected information; slow.)	55	↗	35722	↗	
Full and very deep ultimate (Most NVT's including those that can stop services/hosts; don't trust previously collected information; slow.)	55	↗	35722	↗	
Host Discovery (Network Host Discovery scan configuration.)	2	→	2	→	
System Discovery (Network System Discovery scan configuration.)	6	→	28	→	

(Applied filter: rows=10 permission=any owner=any first=1 sort=name) 1 - 8 of 8 (total: 8)

Fig. 12.1: The GSM comes with various scan configurations.

Scan configurations that are configured statically will not change after an NVT Feed update.

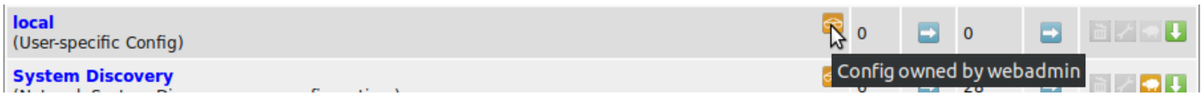
The 👓 icon indicates if the scan configuration is available to and can be used by other users.



Host Discovery (Network Host Discovery scan configuration.)	2	→	2	→
local (User-specific Config)	0	→	0	→

Fig. 12.2: User's scan configurations are only visible to them.

To make a configuration available the respective user, role or group must be assigned the *get_configs* permission. Then this configuration will be visible to the respective users as well.



local (User-specific Config)	0	→	0	→
System Discovery				

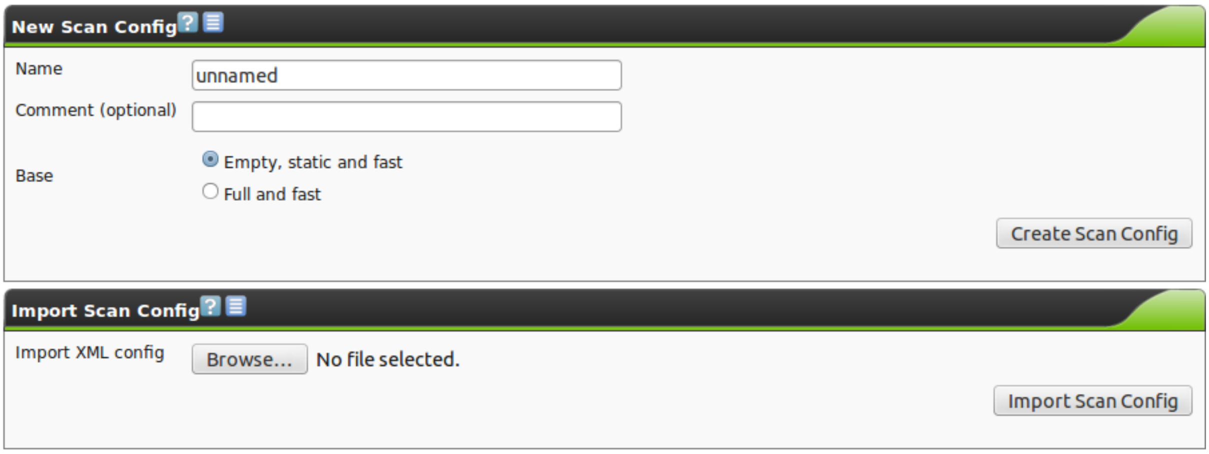
Config owned by webadmin

Fig. 12.3: With the appropriate permissions other users can use the configuration.

12.1 Creating a New Scan Configuration

To create a new scan configuration first select *Configuration/Scan Configs*. Then by clicking on ★ a new scan configuration can be created.

On the following screen there is the option to import a scan configuration or to created manually. Greenbone themselves offer different scan configurations on their web site. In addition scan configurations can be exported on other GSM appliances and then imported.



New Scan Config

Name	unnamed
Comment (optional)	
Base	● Empty, static and fast ○ Full and fast

Create Scan Config

Import Scan Config

Import XML config Browse... No file selected.

Import Scan Config

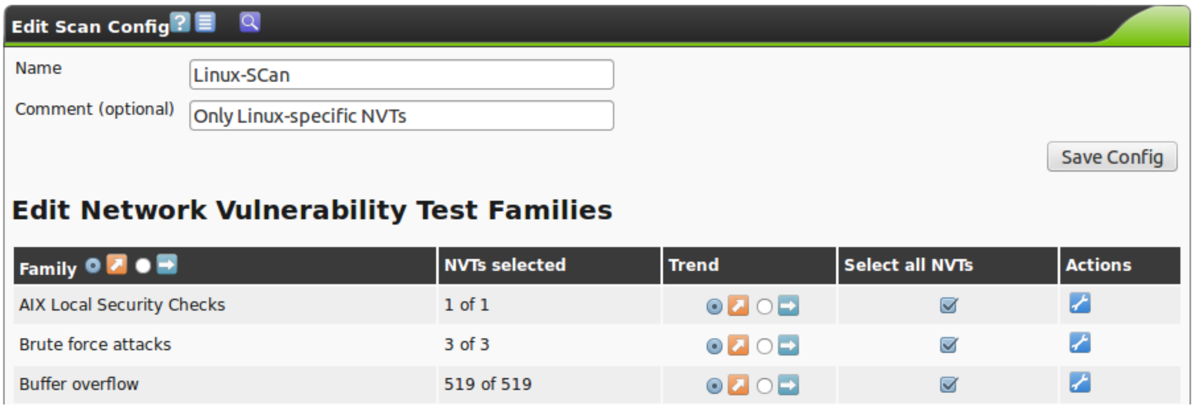
Fig. 12.4: A new scan configuration can be created manually or imported.

When manually creating a scan configuration enter the name and an optional comment and decide which scan configuration to use a template. You can chose between:

- Empty, static and fast
- Full and fast

If another scan configuration should be used as a template it can be cloned on the overview page . Then the configuration can be edited and given its own name and comment and further customized.

On the next page you will be presented with the configuration initially. To edit the configuration use the respective icon with the wrench.



Edit Scan Config

Name	Linux-SCan
Comment (optional)	Only Linux-specific NVTs

Save Config

Edit Network Vulnerability Test Families

Family ● ○	NVTs selected	Trend	Select all NVTs	Actions
AIX Local Security Checks	1 of 1	● ○	☑	
Brute force attacks	3 of 3	● ○	☑	
Buffer overflow	519 of 519	● ○	☑	

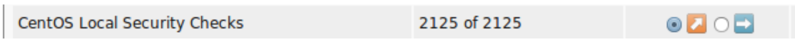
Fig. 12.5: The configuration offers many customization options.

Now the configuration can be customized. Of importance are the following settings:

Family Trend Here it can be decided if a new family should be activated in this scan configuration.

Family ● ○

NVT Trend In every family it can be decided if all NVTs in this family should be activated automatically.

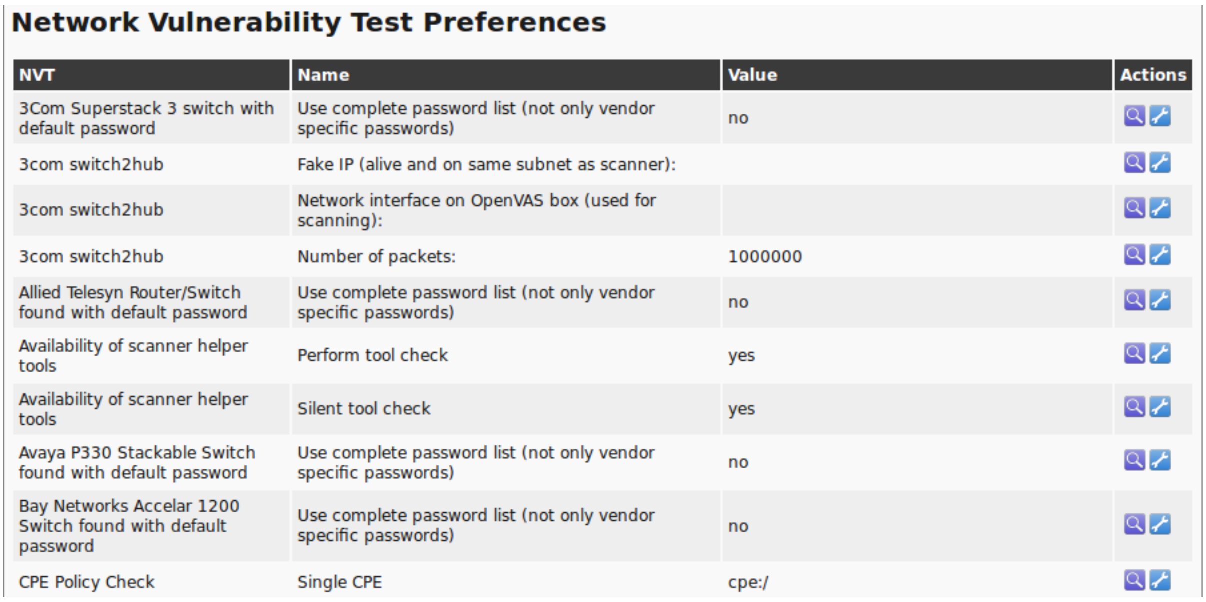


CentOS Local Security Checks	2125 of 2125	● ○

Select All In this column it can be configured if all NVTs of a family should be selected.

Action With this icon you can jump directly into a family to select the individual NVTs if you do not want to use all of them.

When scrolling further down the *Scanner Preferences* will appear (see section *Scanner Preferences* (page 149)). Here additional settings for the scan can be performed. Also, there are the NVT preferences that are being used by the NVTs. They can be customized here. Furthermore there is the possibility to define the settings directly within the respective NVTs.



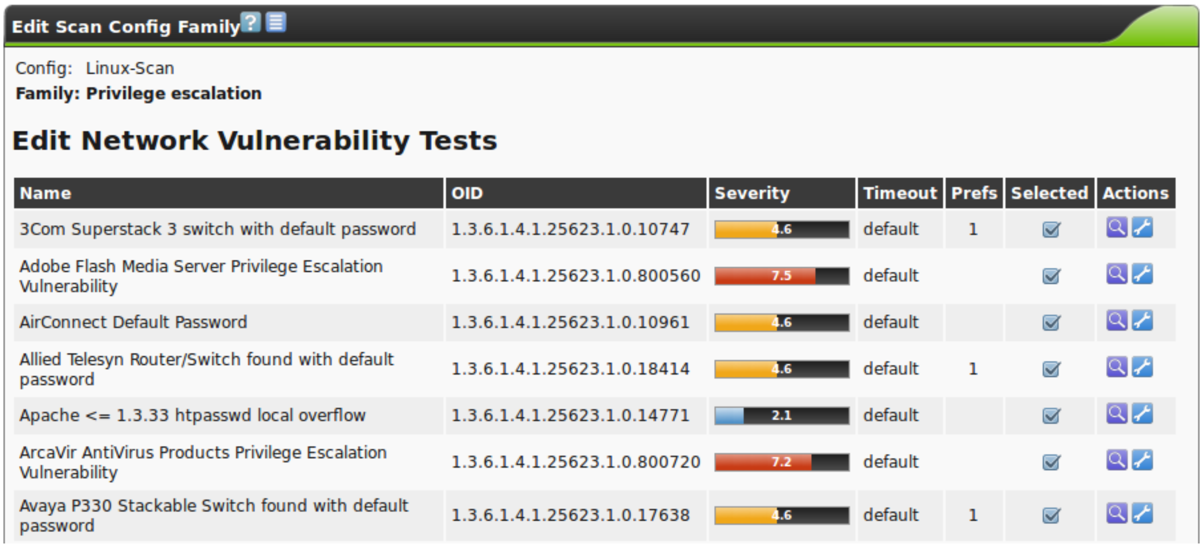
Network Vulnerability Test Preferences

NVT	Name	Value	Actions
3Com Superstack 3 switch with default password	Use complete password list (not only vendor specific passwords)	no	🔍 🔧
3com switch2hub	Fake IP (alive and on same subnet as scanner):		🔍 🔧
3com switch2hub	Network interface on OpenVAS box (used for scanning):		🔍 🔧
3com switch2hub	Number of packets:	1000000	🔍 🔧
Allied Telesyn Router/Switch found with default password	Use complete password list (not only vendor specific passwords)	no	🔍 🔧
Availability of scanner helper tools	Perform tool check	yes	🔍 🔧
Availability of scanner helper tools	Silent tool check	yes	🔍 🔧
Avaya P330 Stackable Switch found with default password	Use complete password list (not only vendor specific passwords)	no	🔍 🔧
Bay Networks Accelar 1200 Switch found with default password	Use complete password list (not only vendor specific passwords)	no	🔍 🔧
CPE Policy Check	Single CPE	cpe:/	🔍 🔧

Fig. 12.6: The configuration allows for specific customization of the NVTs as well.

To make changes to the NVTs you must switch into the respective family.

After selecting a family the individual NVTs can be accessed. The NVTs that are part of a family and their severity can be viewed.



Edit Scan Config Family

Config: Linux-Scan
Family: Privilege escalation

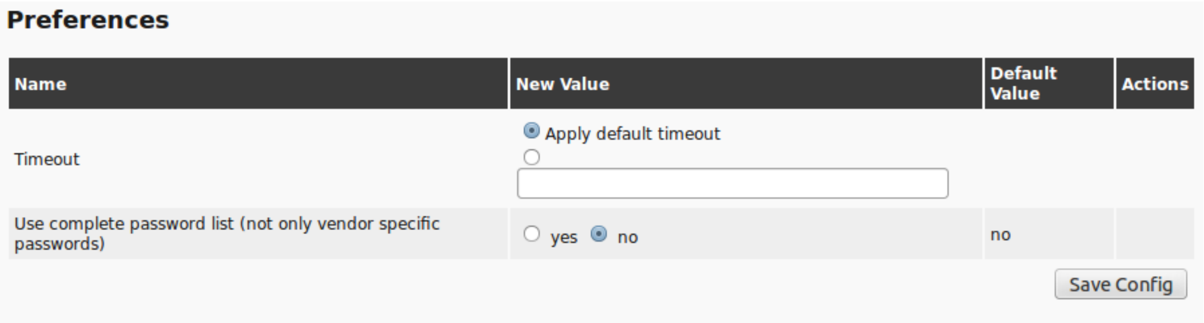
Edit Network Vulnerability Tests

Name	OID	Severity	Timeout	Prefs	Selected	Actions
3Com Superstack 3 switch with default password	1.3.6.1.4.1.25623.1.0.10747	4.6	default	1	☑	🔍 🔧
Adobe Flash Media Server Privilege Escalation Vulnerability	1.3.6.1.4.1.25623.1.0.800560	7.5	default		☑	🔍 🔧
AirConnect Default Password	1.3.6.1.4.1.25623.1.0.10961	4.6	default		☑	🔍 🔧
Allied Telesyn Router/Switch found with default password	1.3.6.1.4.1.25623.1.0.18414	4.6	default	1	☑	🔍 🔧
Apache <= 1.3.33 htpasswd local overflow	1.3.6.1.4.1.25623.1.0.14771	2.1	default		☑	🔍 🔧
ArcaVir AntiVirus Products Privilege Escalation Vulnerability	1.3.6.1.4.1.25623.1.0.800720	7.2	default		☑	🔍 🔧
Avaya P330 Stackable Switch found with default password	1.3.6.1.4.1.25623.1.0.17638	4.6	default	1	☑	🔍 🔧

Fig. 12.7: When accessing a family the individual NVTs can be seen.

Also the status (enabled/disabled) and the timeout of the NVT plugin can be viewed and verified as well if the NVT can be configured further via a configuration (column Prefs). If this is the case the configuration can be accessed via the respective wrench icon 🔧. The settings can be found all the way at the bottom of the page the opens next.

The customized settings of the NVTs are then visible on the overview page of the scan configuration (see figure *The configuration offers many customization options.* (page 147) and *The configuration*



Preferences

Name	New Value	Default Value	Actions
Timeout	● Apply default timeout ○		
Use complete password list (not only vendor specific passwords)	○ yes ● no	no	

Save Config

Fig. 12.8: The preferences can be configured for each NVT individually.

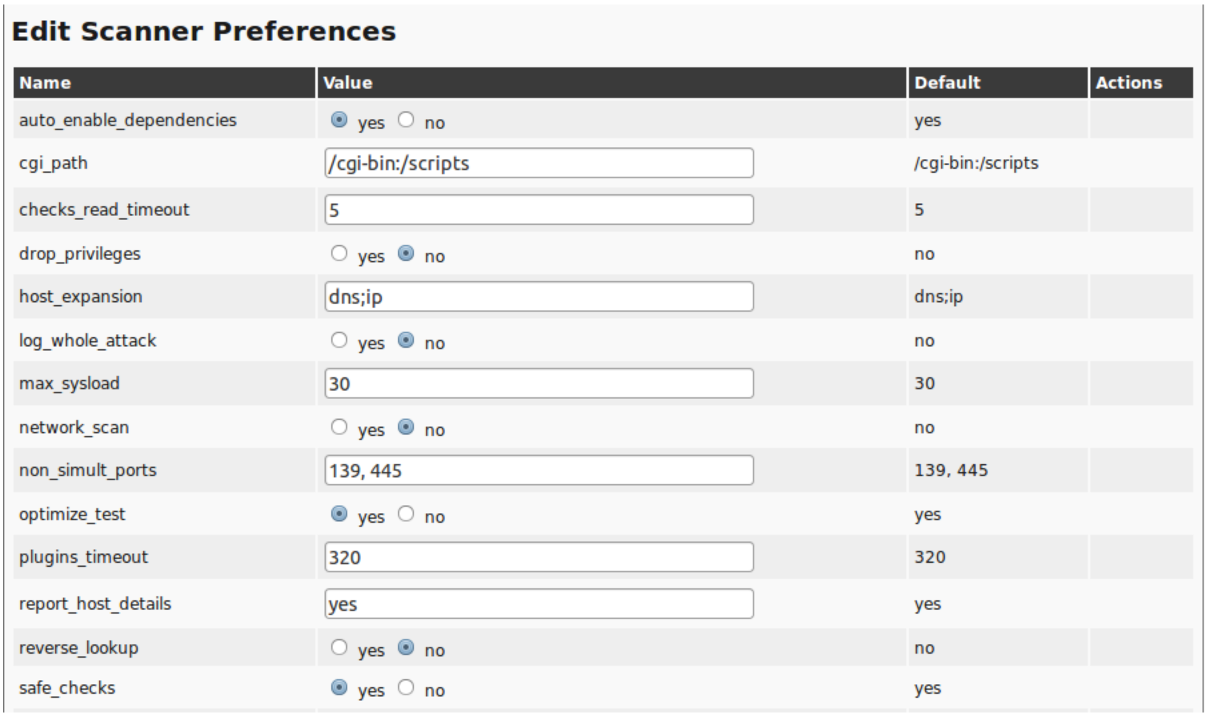
allows for specific customization of the NVTs as well. (page 148)).

For practical use especially the settings of the Port Scanner in use are of interest. The GSM appliance utilizes Nmap and Ping as port scanner. Nmap is being used via the NASL wrapper. This allows for the greatest flexibility.

12.2 Scanner Preferences

To document all scanner and NVT preferences is out of scope of this document. Therefore only the most important general settings and specific settings of the Ping and Nmap-scanners will be covered.

12.2.1 General Preferences



Edit Scanner Preferences

Name	Value	Default	Actions
auto_enable_dependencies	● yes ○ no	yes	
cgi_path	/cgi-bin:/scripts	/cgi-bin:/scripts	
checks_read_timeout	5	5	
drop_privileges	○ yes ● no	no	
host_expansion	dns;ip	dns;ip	
log_whole_attack	○ yes ● no	no	
max_sysload	30	30	
network_scan	○ yes ● no	no	
non_simult_ports	139, 445	139, 445	
optimize_test	● yes ○ no	yes	
plugins_timeout	320	320	
report_host_details	yes	yes	
reverse_lookup	○ yes ● no	no	
safe_checks	● yes ○ no	yes	

Fig. 12.9: These settings will be used in general by the configuration.

- *auto_enable_dependencies*: NVTs that are required by other NVTs will be activated automatically.
- *cgi_path*: This is the path that will be used by the NVTs to access CGI scripts.

- *checks_read_timeout*: This is the timeout for the network sockets during a scan.
- *drop_privileges*: With this parameter the OpenVAS scanner gives up *root* privileges before the start of the NVTs. This increases the security but results in fewer findings with some NVTs.
- *host_expansion*: Three different values are allowed:
  - `dns`: Performs an AXFR zone transfer on the target system and tests the systems that were found.
  - `nfs`: Tests the systems that are allowed access to NFS shares on the target system.
  - `ip`: Scans the specified subnet.
- *log_whole_attack*: If this option is enabled the system logs the run time of each individual NVT. Otherwise only that start and completion of a scan is being logged. This reduces required storage space on the hard disk.
- *network_scan*: Experimental option, which scans the entire network all at once instead of starting Nmap for each individual host. This can save time in specific environments.
- *non_simult_ports*: These ports are not being tested simultaneously by NVTs.
- *optimize_test*: NVTs will only be started if specific pre-requisites are met (i.e. open port).
- *plugins_timeout*: Maximum run time of a NVT.
- *report_host_details*: Detailed information of the host are being saved to the report.
- *safe_checks*: Some NVTs can cause damage on the host system. This setting disables those respective NVTs.
- *unscanned_closed*: This parameter defines if TCP ports that were not scanned should be treated like closed ports.
- *unscanned_closed_udp*: This parameter defines if UDP ports that weren't scanned should be treated as closed ports.
- *use_mac_addr*: Systems will be identified by MAC address and not by IP address. This could be beneficial in a DHCP environment.
- *vhosts*: If the GSM is to scan a web server with name based virtual hosts then the settings *vhosts* and *vhosts_ip* can be used. In the setting *vhosts* the names of the virtual hosts a entered comma separated.
- *vhosts_ip*: If the GSM is to scan a web server with name based virtual hosts then the settings *vhosts* and *vhosts_ip* can be used. In the setting *vhosts_ip* the IP address of the web server is being entered. In the report it can not be referenced in which virtual instance a NVT discovered a vulnerability.

12.2.2 Ping Preferences

The Ping-Scanner-NVT contains the following configurations parameters.

Remember that the `Alive Test` settings of a target object can overwrite some settings of the Ping-Scanner.

- *Do a TCP ping*: Here it can be selected if the reachability of a host should be tested using TCP. In this case the following ports will be tested: 21,22,23,25,53,80,135,137,139,143,443,445. Default: No.
- *Do an ICMP ping*: Here it can be selected if the reachability of host should be tested using ICMP. Default: Yes.
- *Mark unreachable Hosts as dead*: Here it can be selected if a system that are not discovered by this NVT should be tested by other NVTs later. Default: No.

- *Report about reachable Hosts*: Here it can be selected if the systems discovered by this NVT should be listed. Default: No.
- *Report about unreachable Hosts*: Here it can be selected if the systems that are not discovered by this system should be listed. Default: No.
- *TCP ping tries also TCP-SYN ping*: The TCP ping uses by default a TCP-ACK packet. Here a TCP-SYN packet can be used additionally. Default: No.
- *Use ARP*: Here it can be selected if hosts should be searched for in the local network using the ARP protocol. Default: No.
- *Use Nmap*: Here it can be selected if the Ping-NVT should use Nmap. Default: Yes.
- *nmap: try also with only –sP*: If Nmap is used the Ping-Scan will be performed using the –sP option.
- *nmap additional ports for –PA*: Here additional ports for the TCP-Ping-Test can be specified. This is only the case if *Do a TCP ping* is selected. Default: 8080,3128.

12.2.3 Nmap NASL Preferences

The following options will be directly translated into options for the execution of the nmap command. Therefore additional information can be found in the documentation for nmap[131].

- *Do not randomize the order in which ports are scanned*: Nmap will scan the ports in ascending order.
- *Do not scan targets not in the file*: Only meaningful in conjunction with *File containing grepable results*.
- *Fragment IP packets*: Nmap fragments the packets for the attack. This allows to bypass simple packet filters.
- *Get Identd info*: Nmap queries the UNIX-Ident-Daemon. It is currently no longer being used.
- *Identify the remote OS*: Nmap tried to identify the operating system.
- *RPC port scan*: Nmap tests the system for Sun RPC ports.
- *Run dangerous ports even if safe checks are set*: UDP and RPC scans can cause problems and usually are disabled with the setting *safe_checks*.
- *Service scan*: Nmap will try to identify services.
- *Use hidden option to identify the remote OS*: Nmap will try to identify more aggressively.
- *Host Timeout*: Defines the host timeout.
- *Initial RTT timeout*: This is the initial round trip timeout. Nmap can adjust this timeout dependent on the results.
- *Max RTT timeout*: This is the maximum RTT.
- *Min RTT timeout*: This is the minimum RTT.
- *Minimum wait between probes*: This regulates the speed of the scan.
- *Ports scanned in parallel (max)*: Defines how many ports should be scanned simultaneously.
- *Ports scanned in parallel (min)*: see above
- *Source port*: Defines the source port. This is of interest when scanning through a firewall if connections are in general allowed from a specific port.
- *File containing grepable results*: Allows for the specification of a file in which line entries in the form of `Host: IP address` can be found. If the option *Do not scan targets not in the file* is set at the same time only systems contained in the file will be scanned.

[131] http://nmap.org/docs.html

- *TCP scanning technique*: Define the actual scan technique.
- *Timing policy*: Instead of changing the timing values individually the timing policy can be modified.

The timing policy uses the following values:

	initial_rtt_timeout	min_rtt_timeout	max_rtt_timeout	max_parallelism	scan_delay	max_scan_delay
Paranoid	5 min	100 ms	10 sec	Serial	5 min	1 sec
Sneaky	15 sec	100 ms	10 sec	Serial	15 sec	1 sec
Polite	1 sec	100 ms	10 sec	Serial	400 ms	1 sec
Normal	1 sec	100 ms	10 sec	Parallel	0 sec	1 sec
Aggressive	500 ms	100 ms	1250 ms	Parallel	0 sec	10 ms
Insane	250 ms	50 ms	300 ms	Parallel	0 sec	5 ms

Scanners

Additional Scanners may be enabled through the GOS-Admin-Menu. The GSM comes with the OpenVAS scanner configured by default. No other scanner is enabled.

Note: Starting with GOS 3.1.17 pilot users can choose additional scanners. This feature will be available for all users through a later update. To become a pilot user, contact the Greenbone Support.

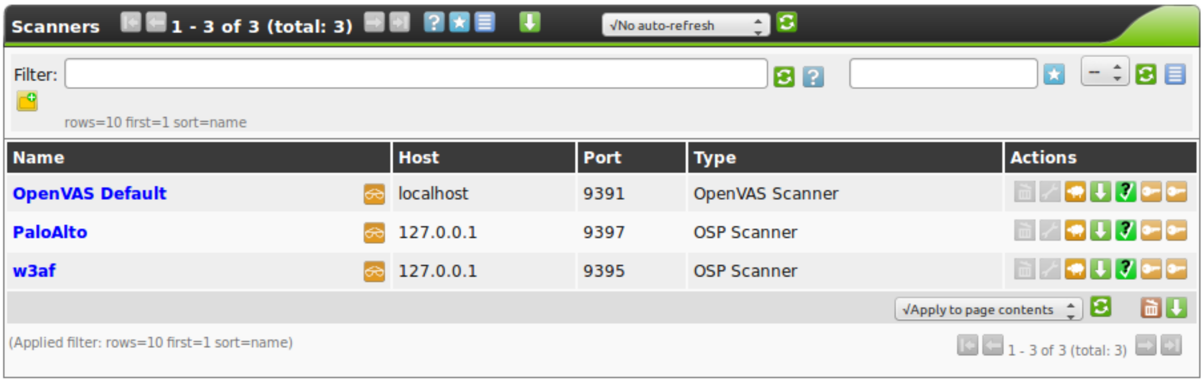
To enable additional scanner please refer to section *Enabling additional OSP Scanners* (page 223).

This chapter shows the usage of these additional scanner modules.

13.1 w3af scanner

w3af is a Web Application Attack and Audit Framework. The project's goal is to create a framework to help you secure your web applications by finding and exploiting all web application vulnerabilities.

Once you enabled the scanner using the GOS-Admin-Menu (see section *Enabling additional OSP Scanners* (page 223)), you need to configure the w3af Scanner. Use the WebUI for the configuration. Select *Configuration* followed by *Scanners*. You will see all currently enabled OSP Scanners:



Scanners 1 - 3 of 3 (total: 3)

√No auto-refresh

Filter:

rows=10 first=1 sort=name

Name	Host	Port	Type	Actions
OpenVAS Default	localhost	9391	OpenVAS Scanner	
PaloAlto	127.0.0.1	9397	OSP Scanner	
w3af	127.0.0.1	9395	OSP Scanner	

√Apply to page contents

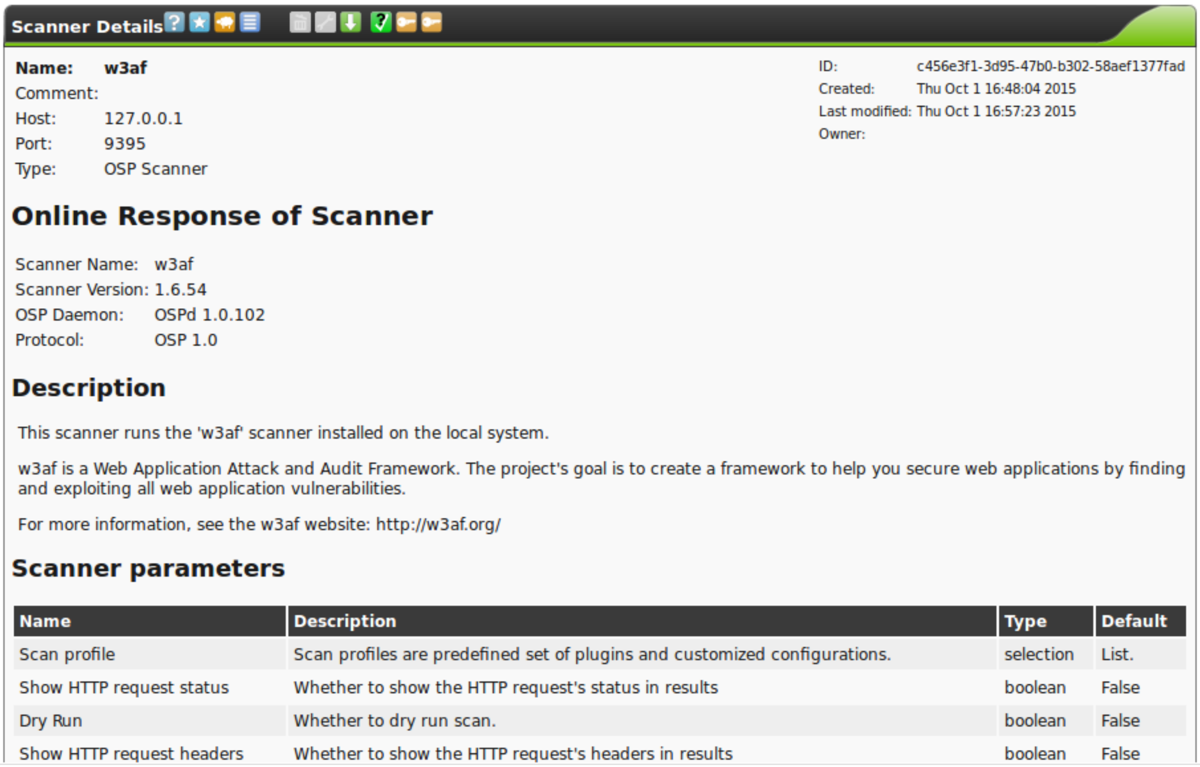
(Applied filter: rows=10 first=1 sort=name)

1 - 3 of 3 (total: 3)

Fig. 13.1: All configured OSP scanners

Select the w3af scanner. You will then be able to see the current configuration:

The default configuration may not be changed in this dialog. To setup and modify these parameters you need to create a appropriate scan configuration.



Scanner Details

Name: **w3af**
Comment:
Host: 127.0.0.1
Port: 9395
Type: OSP Scanner

ID: c456e3f1-3d95-47b0-b302-58aef1377fad
Created: Thu Oct 1 16:48:04 2015
Last modified: Thu Oct 1 16:57:23 2015
Owner:

Online Response of Scanner

Scanner Name: w3af
Scanner Version: 1.6.54
OSP Daemon: OSPd 1.0.102
Protocol: OSP 1.0

Description

This scanner runs the 'w3af' scanner installed on the local system.

w3af is a Web Application Attack and Audit Framework. The project's goal is to create a framework to help you secure web applications by finding and exploiting all web application vulnerabilities.

For more information, see the w3af website: http://w3af.org/

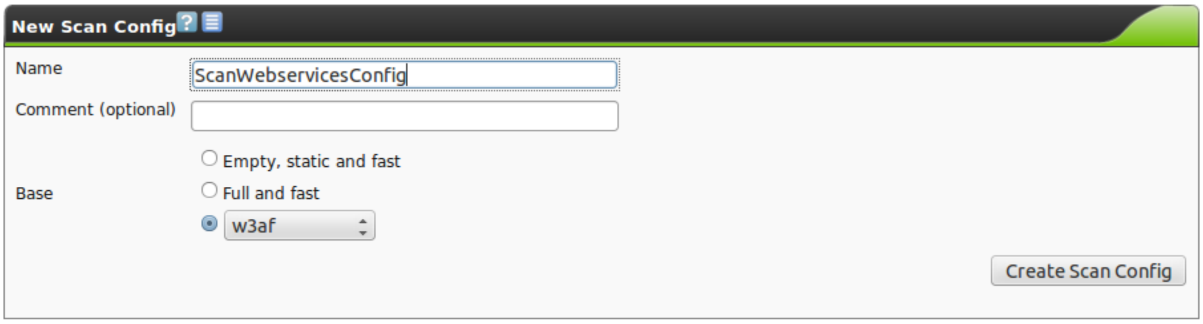
Scanner parameters

Name	Description	Type	Default
Scan profile	Scan profiles are predefined set of plugins and customized configurations.	selection	List.
Show HTTP request status	Whether to show the HTTP request's status in results	boolean	False
Dry Run	Whether to dry run scan.	boolean	False
Show HTTP request headers	Whether to show the HTTP request's headers in results	boolean	False

Fig. 13.2: w3af configuration

13.1.1 w3af scan configuration

Go to *Configuration/Scan Configs*. Create a new scan configuration and select w3af as base config:



New Scan Config

Name: ScanWebservicesConfig
Comment (optional):
Base: ○ Empty, static and fast
○ Full and fast
● w3af

Fig. 13.3: Create a w3af scan configuration

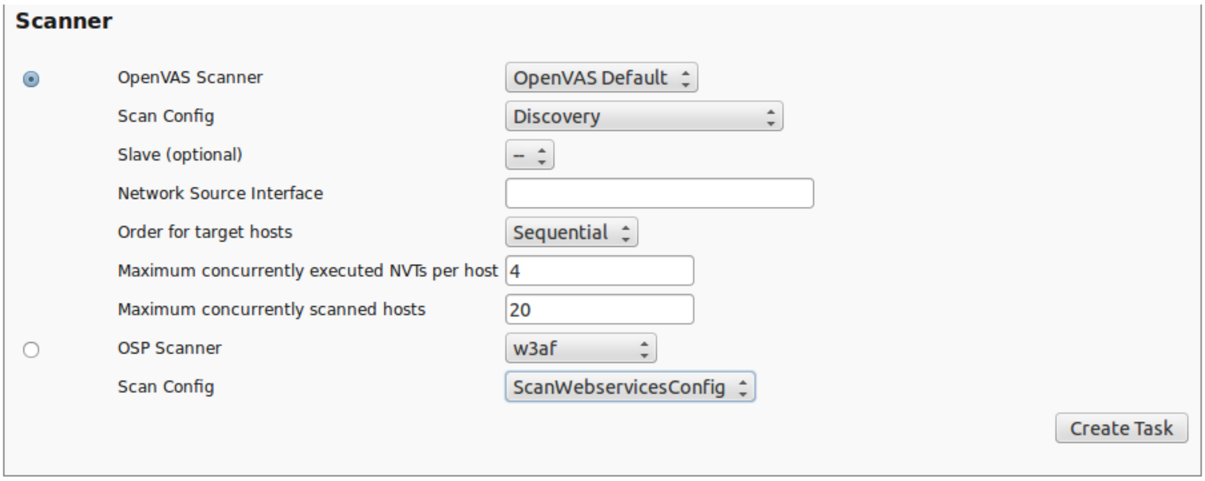
This configuration may now be modified. The following parameters are available:

- profile You can choose between these w3af profiles. The profiles are further documented on the w3af webpage http://w3af.org. These profiles are collections of configured w3af plugins.
  - fast_scan
  - audit_high_risk
  - full_audit
  - OWASP_TOP10
  - bruteforce
  - empty_profile

  - web_infrastructure
  - full_audit_spider_man
  - sitemap
- http_request_status This allows to toggle the respective functionality.
- http_request_headers This allows to toggle the respective functionality.
- http_response_status This allows to toggle the respective functionality.
- debug_mode This allows to toggle the respective functionality.
- dry_run This allows to toggle the respective functionality.
- use_https This allows to toggle the respective functionality.
- seed_path This defines the starting URL fir the w3af scanner.
- target_port This setting allows to set another port for the webserver that the default port 80, like 8080 or 443.

13.1.2 w3af scan task

To scan a system you need to setup an appropriate task. Go to *Scan Management* and create a new task. Enter the usual information at the top of the screen: name, target, alerts, schedule, etc. Scroll down and select the OSP scanner instead of the OpenVAS Scanner:



Scanner

●	OpenVAS Scanner	OpenVAS Default
	Scan Config	Discovery
	Slave (optional)	–
	Network Source Interface	
	Order for target hosts	Sequential
	Maximum concurrently executed NVTs per host	4
	Maximum concurrently scanned hosts	20
○	OSP Scanner	w3af
	Scan Config	ScanWebservicesConfig

Fig. 13.4: Create a w3af scan task

Create the scan and start the scan as usual.

13.2 PaloAlto Scanner

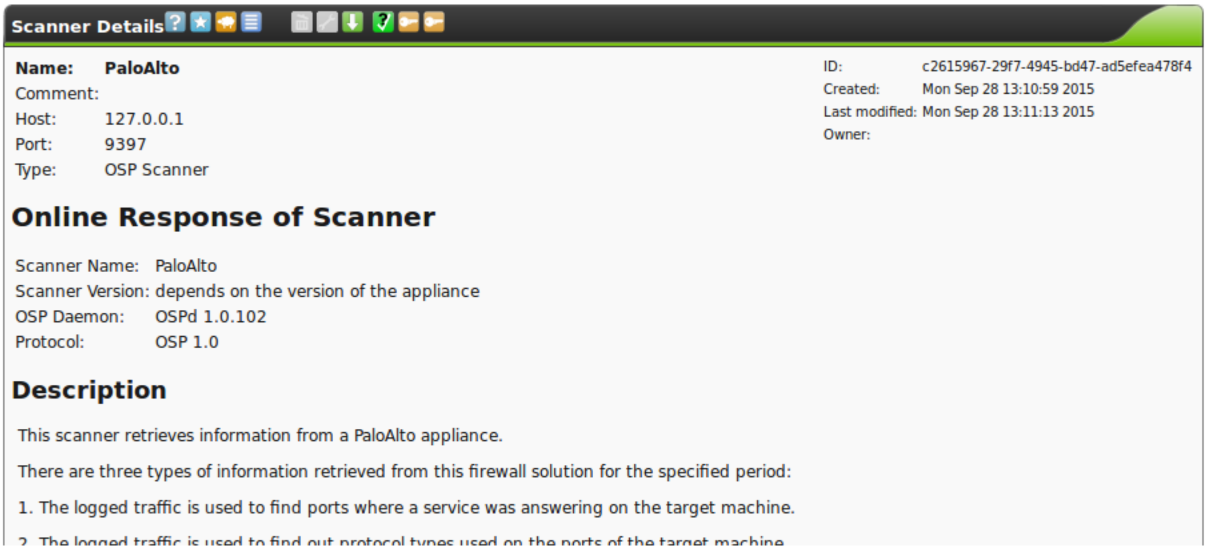
This OSP scanner module retrieves information from a PaloAlto next generation firewall appliance. The scanner may retrieve three different types of information from the firewall:

- The traffic logged by the firewall is used to identify ports with active services on the target.
- The traffic logged by the firewall is used to identify the protocols used by the target.
- The threats identified and logged by the firewall are searched for CVE references.

The PaloAlto firewall distinguishes 5 different severity classes. These classes are mapped to CVSS values as follows:

- Informational: 0.0
- Low: 3.0
- Medium: 5.0
- High: 8.0
- Critical: 10.0

You can check wether the PaloAlto scanner is functional using *Configuration/Scanners* followed by selecting the PaloAlto scanner:



Name: PaloAlto
Comment:
Host: 127.0.0.1
Port: 9397
Type: OSP Scanner

ID: c2615967-29f7-4945-bd47-ad5efea478f4
Created: Mon Sep 28 13:10:59 2015
Last modified: Mon Sep 28 13:11:13 2015
Owner:

Online Response of Scanner

Scanner Name: PaloAlto
Scanner Version: depends on the version of the appliance
OSP Daemon: OSPd 1.0.102
Protocol: OSP 1.0

Description

This scanner retrieves information from a PaloAlto appliance.

There are three types of information retrieved from this firewall solution for the specified period:

1. The logged traffic is used to find ports where a service was answering on the target machine.

2. The logged traffic is used to find out protocol types used on the ports of the target machine

Fig. 13.5: Verify PaloAlto scanner

If the scanner is online you can verify the response of the scanner. If the scanner is not online you will see “Offline”.

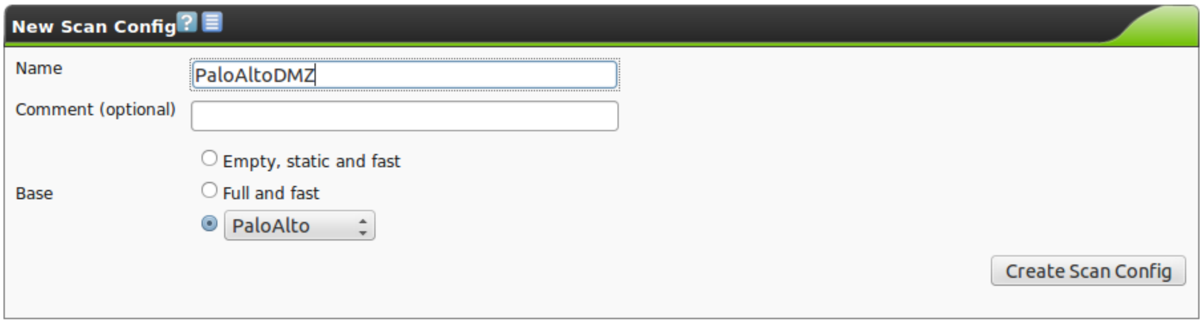
13.2.1 PaloAlto Scanner Configuration

Several steps need to be taken to use the PaloAlto Scanner.

Scan Configuration

To use the scanner, you need to setup a scan configuration. Go to *Configuration/Scan Configs*.

Create a new scan configuration and select PaloAlto as base.



Name: PaloAltoDMZ
Comment (optional):
Base: ○ Empty, static and fast
○ Full and fast
● PaloAlto

Fig. 13.6: Create a PaloAlto scan configuration

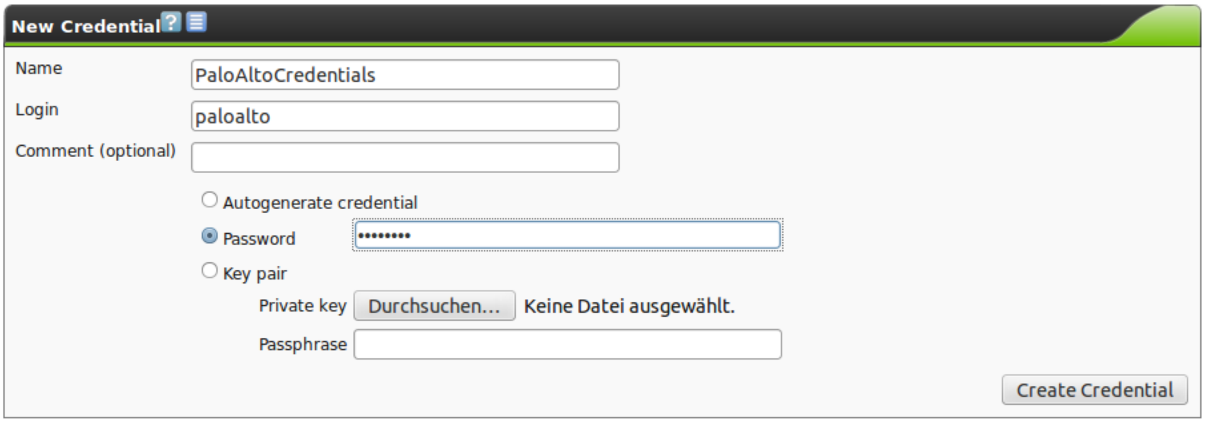
Here you can specify:

- dry_run This will just do a dry run.
- period For the time period the GSM will extract the logs from the PaloAlto appliance. The period should match the schedule the tasks are run at. If you run the task daily you should select last-24-hrs.
- debug_mode This will output additional debug information.
- ca-certificate This is the ca-certificate of the PaloAlto used to verify the appliance.
- address This is the ip address of the PaloAlto appliance.

Target

Now a specific target for the PaloAlto scan needs to be setup. Targets used in other scans may not be reused, because the login/password for accessing the PaloAlto firewall is configured using the credentials normally used for an authenticated scan.

First create the credentials for accessing the PaloAlto appliance (figure *PaloAlto credentials* (page 157)).



Name: PaloAltoCredentials

Login: paloalto

Comment (optional):

○ Autogenerate credential

● Password ••••••••

○ Key pair

Private key Keine Datei ausgewählt.

Passphrase

Fig. 13.7: PaloAlto credentials

Now create a target using these credentials (figure *PaloAlto target* (page 158)).

Task

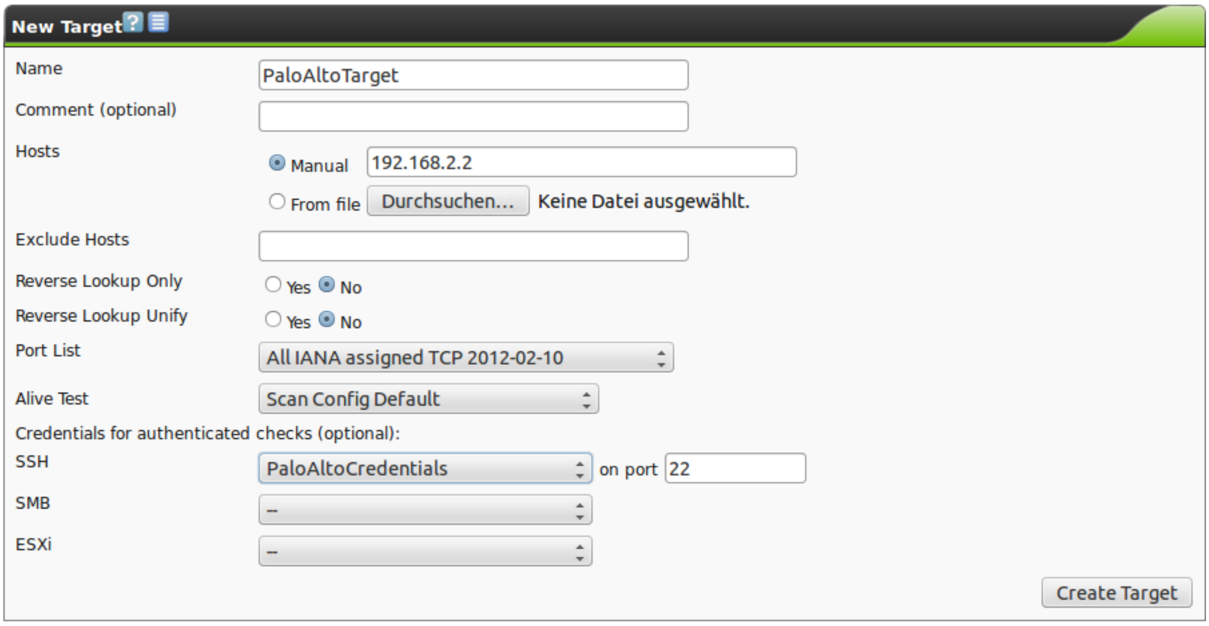
Once the scan configuration is in place you can setup a task using this scan configuration. Go to *Scan Management/Tasks*. Create a new task and select the OSP Scanner. Select PaloAlto and your scan configuration.

Start the task. Once the task is finished you may analyze the report.

13.2.2 PaloAlto Report

The report generated by the PaloAlto OSP scanner is very similar to the OpenVAS report although there are some differences. The PaloAlto next generation firewall includes an intrusion detection system and not a vulnerability scanner. Therefore the vulnerabilities presented in the report are not tested by the scanner. These are detected attacks done by some third party. The quality of the results depends very much on the tuning of the PaloAlto appliance.

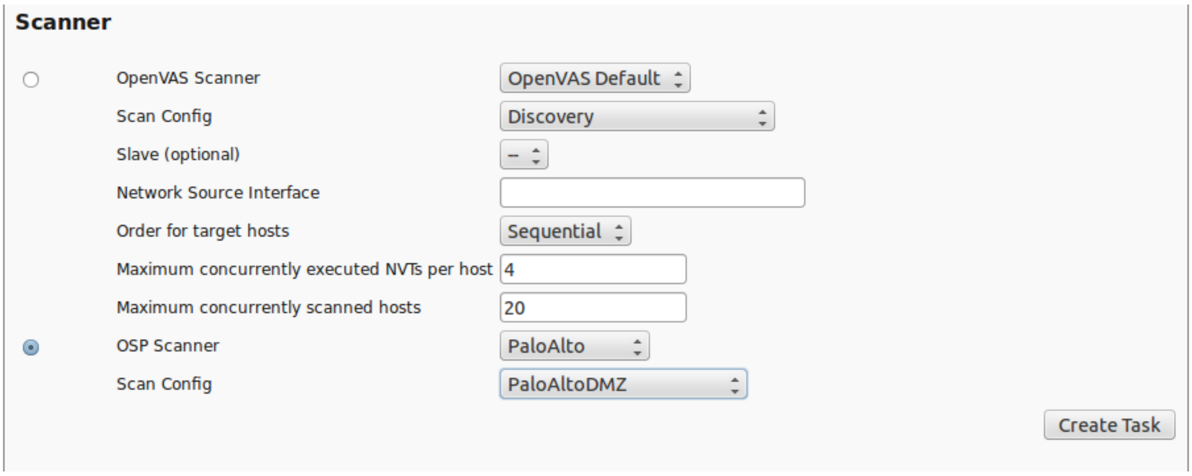
The following image displays a sample report:



New Target

Name	PaloAltoTarget
Comment (optional)	
Hosts	● Manual 192.168.2.2 ○ From file Durchsuchen... Keine Datei ausgewählt.
Exclude Hosts	
Reverse Lookup Only	○ Yes ● No
Reverse Lookup Unify	○ Yes ● No
Port List	All IANA assigned TCP 2012-02-10
Alive Test	Scan Config Default
Credentials for authenticated checks (optional):	
SSH	PaloAltoCredentials on port 22
SMB	–
ESXi	–

Fig. 13.8: PaloAlto target



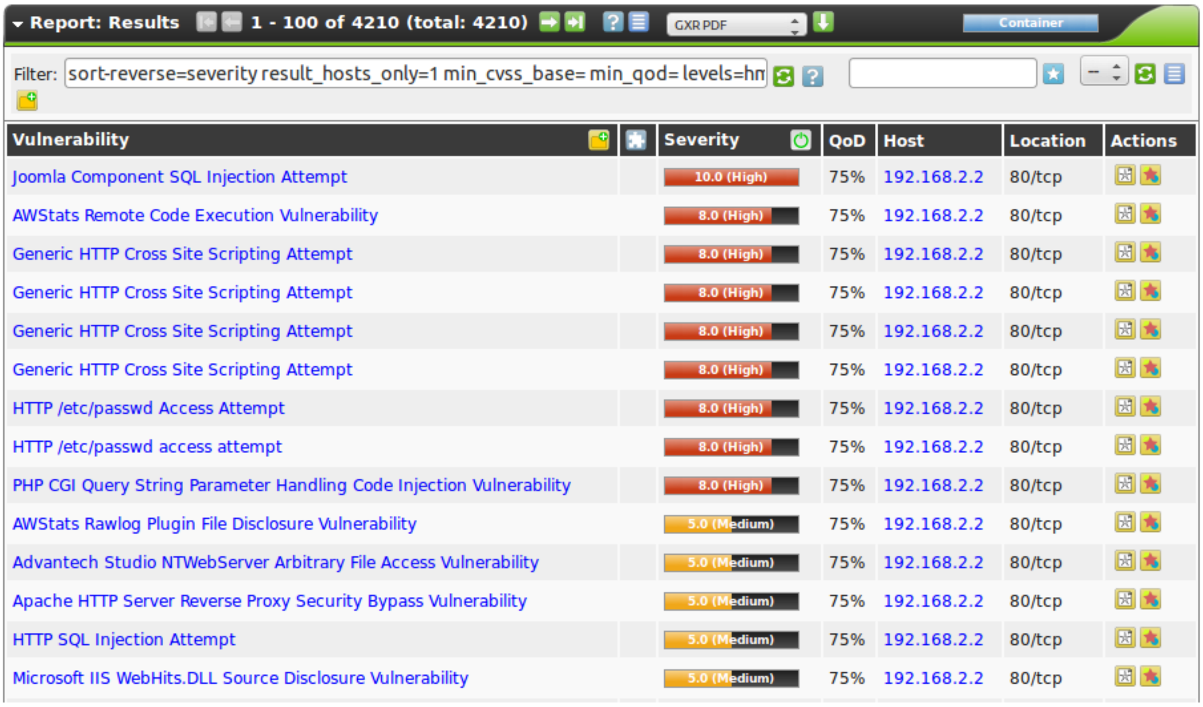
Scanner

○	OpenVAS Scanner	OpenVAS Default
	Scan Config	Discovery
	Slave (optional)	–
	Network Source Interface	
	Order for target hosts	Sequential
	Maximum concurrently executed NVTs per host	4
	Maximum concurrently scanned hosts	20
●	OSP Scanner	PaloAlto
	Scan Config	PaloAltoDMZ

Fig. 13.9: Create a PaloAlto task

The PaloAlto next generation firewall logs the possible false positive alerts using the term “attempt”. As can be seen in the sample report there are several “Generic HTTP Cross Site Scripting Attempt” and “HTTP SQL Injection Attempt”.

The PaloAlto detects the attack and in many cases stopps the attack from reaching its target. Therefore it is most often not possible to deduct whether the target actually has the vulnerability or not. This is why it makes sense to combine a regular vulnerability scan and IDS incidents within a vulnerability management solution.



Report: Results 1 - 100 of 4210 (total: 4210)

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= min_qod= levels=hm

Vulnerability		Severity	QoD	Host	Location	Actions
Joomla Component SQL Injection Attempt		10.0 (High)	75%	192.168.2.2	80/tcp	
AWStats Remote Code Execution Vulnerability		8.0 (High)	75%	192.168.2.2	80/tcp	
Generic HTTP Cross Site Scripting Attempt		8.0 (High)	75%	192.168.2.2	80/tcp	
Generic HTTP Cross Site Scripting Attempt		8.0 (High)	75%	192.168.2.2	80/tcp	
Generic HTTP Cross Site Scripting Attempt		8.0 (High)	75%	192.168.2.2	80/tcp	
Generic HTTP Cross Site Scripting Attempt		8.0 (High)	75%	192.168.2.2	80/tcp	
HTTP /etc/passwd Access Attempt		8.0 (High)	75%	192.168.2.2	80/tcp	
HTTP /etc/passwd access attempt		8.0 (High)	75%	192.168.2.2	80/tcp	
PHP CGI Query String Parameter Handling Code Injection Vulnerability		8.0 (High)	75%	192.168.2.2	80/tcp	
AWStats Rawlog Plugin File Disclosure Vulnerability		5.0 (Medium)	75%	192.168.2.2	80/tcp	
Advantech Studio NTWebServer Arbitrary File Access Vulnerability		5.0 (Medium)	75%	192.168.2.2	80/tcp	
Apache HTTP Server Reverse Proxy Security Bypass Vulnerability		5.0 (Medium)	75%	192.168.2.2	80/tcp	
HTTP SQL Injection Attempt		5.0 (Medium)	75%	192.168.2.2	80/tcp	
Microsoft IIS WebHits.DLL Source Disclosure Vulnerability		5.0 (Medium)	75%	192.168.2.2	80/tcp	

Fig. 13.10: PaloAlto sample report

CHAPTER 14

Alternate User Interfaces

The web user interface of the GSM is interchangeable. All web user interfaces use a built-in webserver that translates all actions into the OpenVAS Management Protocol and displays the results respectively. Therefor the web user interfaces do not possess any intelligence themselves. The intelligence is completely hidden in the OpenVAS manager. This is why the web user interfaces are interchangeable.

In the version GOS 3.1 the GSM offers two different web user interfaces:

- Classic: This is the classic view of the Greenbone Security Assistant.
- ITS: This is a simplified presentation in the form of an IT vulnerability Traffic Light.

To switch between the two interfaces access to the command line is required. The chosen interface is always active for all users of the GSM appliance. The selection can be controlled depending on the user.

14.1 IT Vulnerability Traffic Light

Note: This UI is only available in the German language.

Before switching to the IT Vulnerability Traffic Light several settings in the classic view should be changed. Otherwise you will receive warnings in the Vulnerability Traffic Light as displayed in figure *Scanning using the ITS Vulnerability Traffic Light.* (page 162).

- Import the ITS report format

  Download the ITS report format from http://greenbone.net/download/rfps/its-openvas.xml and import it under *Configuration/Report Formats*. Edit 🔧 the report format and activate it. Now just verify it by clicking on ?.

- Import the ITS scan configuration

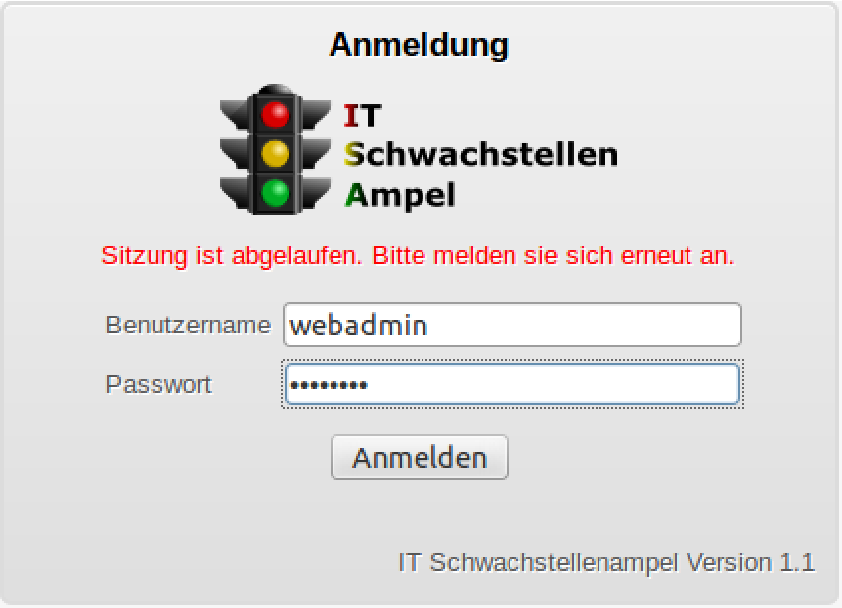
  Download the ITS scan configuration from http://www.greenbone.net/download/scanconfigs/its-scanconfig.xml and import it under *Configuration/Scan Configs*.

Once these prerequisites are completed it can be switched over. Possible some prerequisites have already been performed on your system. To change the interface enter the GOS-Admin-Menu. There under the menu option *Remote* configure the *HTTPS web interface*. The default value is `classic`. To switch to the IT Vulnerability Traffic Light change the value to `its`. After a *Commit* the change will be activated within a couple of minutes. A reboot is not required.

Alternatively the value can be changed in the command line directly:

```
gsm: set web_interface its
gsm *: commit
```

After a couple of minutes the ITS Vulnerability Traffic Light will be active. Now the log in displays the availability of the new interface (see figure *The log in of the ITS Vulnerability Traffic Light.* (page 162)).



Anmeldung

Sitzung ist abgelaufen. Bitte melden sie sich erneut an.

Benutzername: webadmin

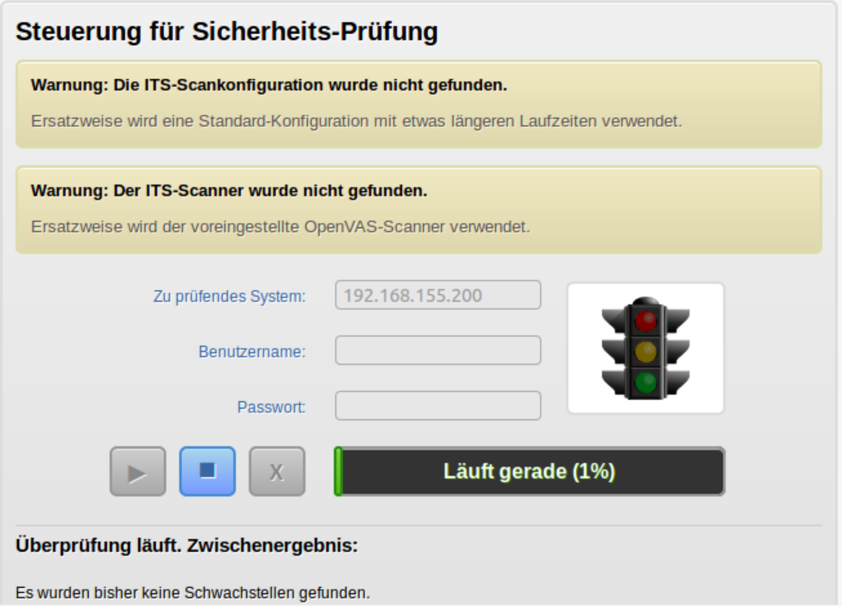
Passwort: ••••••••

IT Schwachstellenampel Version 1.1

Fig. 14.1: The log in of the ITS Vulnerability Traffic Light.

After logging in a wizard appears that allows for the simple starting of a scan.

For the scan an administrative user can be specified. The scanner then will log itself into the system and scan the system internally as well (see figure *Scanning using the ITS Vulnerability Traffic Light.* (page 162)). When the report format and the scan confirmation are imported and the ITS-Scanner is cloned then the warnings will no longer be displayed.



Steuerung für Sicherheits-Prüfung

Warnung: Die ITS-Scankonfiguration wurde nicht gefunden.

Ersatzweise wird eine Standard-Konfiguration mit etwas längeren Laufzeiten verwendet.

Warnung: Der ITS-Scanner wurde nicht gefunden.

Ersatzweise wird der voreingestellte OpenVAS-Scanner verwendet.

Zu prüfendes System: 192.168.155.200

Benutzername:

Passwort:

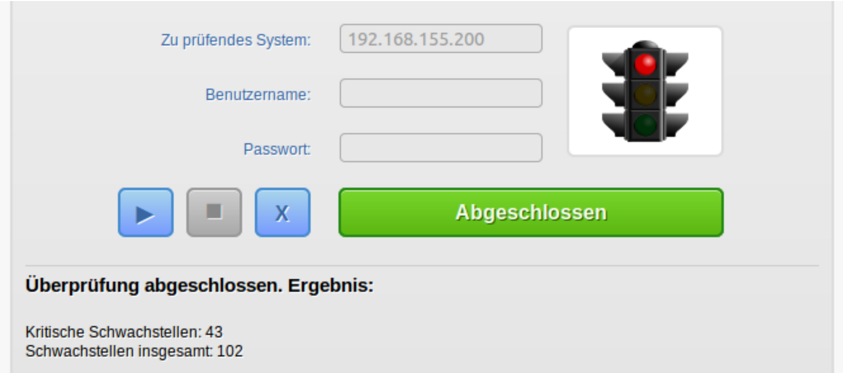
Überprüfung läuft. Zwischenergebnis:

Es wurden bisher keine Schwachstellen gefunden.

Fig. 14.2: Scanning using the ITS Vulnerability Traffic Light.

If vulnerabilities are discovered the displayed traffic light will flash in the respective colour during the scan. As soon as the scan is completed the traffic light will stop flashing and displays the status permanently (see figure *After completion of the scan the status of the traffic light is displayed* *permanently.* (page 163)).

Clicking the printer icon (see figure *The printer icon gives access to the report.* (page 163)) the PDF report can be downloaded.



Zu prüfendes System: 192.168.155.200

Benutzername:

Passwort:

Überprüfung abgeschlossen. Ergebnis:

Kritische Schwachstellen: 43
Schwachstellen insgesamt: 102

Fig. 14.3: After completion of the scan the status of the traffic light is displayed permanently.

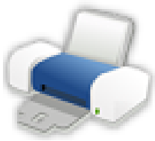


Fig. 14.4: The printer icon gives access to the report.

CHAPTER 15

User and Permission Management

This chapter covers the user, group, role and permission management in detail.

15.1 User Management

The Greenbone Security Manager allows for the definition and the management of different users with different roles and permissions. When initializing the GSM the first user, the web/scan administrator respectively, is being created via the GOS-Admin-Menu already. This user allows the login and management of additional users.

The GSM user management supports a role based permission concept when accessing the web interface. Various roles are already set up by default. Additional roles can be created and used by an administrator. The role defines which options of the web interface can be viewed and modified by the user. Thereby the roles are not realized in the web interface rather than the underlying OMP protocol hence affecting all OMP clients. Read and write access can be assigned to roles separately.

In addition to the roles the GSM user management supports groups as well. Groups allow the combining of users. This serves mainly for logical grouping. Aside from the management of permissions for the roles groups can be assigned specific permissions.

Additionally, via the user management users can be assigned an IP address range which scanning is allowed or denied. The GSM appliance will then refuse to scan any other IP addresses than the ones specified for the respective user. Also the access to specific interfaces of the GSM appliance can be allowed and denied.

The Greenbone Security Manager offers its own User Management for the management of roles and the specific permissions of users. However, in order not to store multiple passwords and to allow password synchronization the Greenbone Security Manager offers connecting the system to a central LDAP server. It will only be used to verify the password during the log in process of the user. All other settings are being performed in the User Management of the GSM appliance.

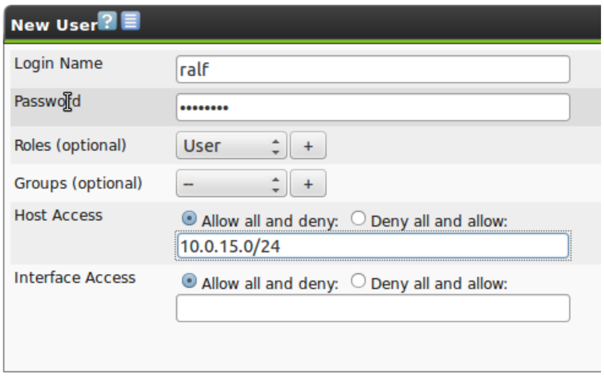
These functions are being covered in more detail below.

15.1.1 Creating and Managing Users

The dialog for the creation and management of users can be accessed via the *Administration* menu. This menu is only visible to the administrators as only they are allowed to create and manage additional users. The dialog to create a new user can be accessed via the white asterisk on blue background ✱ or by selecting the wrench an existing user can be modified.

When creating a new user the following options are available:

- *Login Name*: This is the name the user logs in with. If an LDAP server is used for central password management, the user needs to be created with the identical name (rDN) as in the LDAP server. The name can be a maximum of 80 characters and can contain letters and numbers.



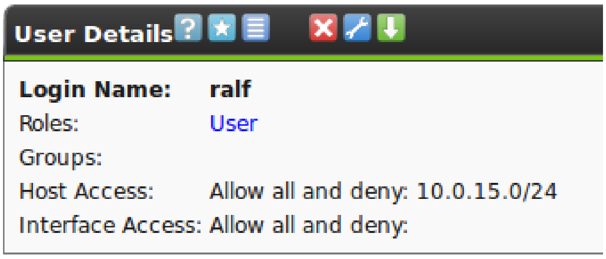
New User

Login Name	ralf
Password	••••••••
Roles (optional)	User +
Groups (optional)	– +
Host Access	● Allow all and deny: ○ Deny all and allow: 10.0.15.0/24
Interface Access	● Allow all and deny: ○ Deny all and allow:

Fig. 15.1: Creating a new user.

- *Password*: This is the password for the user. The password can be a maximum of 40 characters and can contain any type of character. Please note when using special characters that they are available on all keyboards and operating systems in use.
- *Roles (optional)*: Each user can have multiple roles. The roles define the permissions of a user when using the OMP protocol. Since the Greenbone Security Assistance utilized the OMP protocol the roles define directly the features in the web interface. While it is possible to add and configure additional roles, at the beginning, the roles *Administrator*, *User*, *Info*, *Observer*, and some others are available. These roles are discussed in more detail in section User Roles (page 167).
- *Groups (optional)*: Each user can be a member of multiple groups. Permissions management can be performed via groups as well (see section Permissions (page 173)).
- *Host Access*: Here it can be defined which systems a specific user can analyze in a scan and which systems should not be considered in a scan. These restrictions can also be set up for administrators. They can, however, remove these restrictions again themselves. This is why this function is simply a self-protection for administrators. Normal users (*User*) and roles without access to the user management respectively cannot circumvent this restriction. Basically is can be chosen between a whitelist (deny all and allow) and a blacklist (allow all and deny). In the first case the scanning of all systems is denied in general and only explicitly listed systems are allowed to be scanned. In the latter case the scanning of all systems is allowed except the listed systems. System names as well as IPv4 and IPv6 addresses can be entered. Furthermore individual IP addresses as well as address ranges and network segments can be specified. The following listing shows some examples:
  - 192.168.15.5 (IPv4 address)
  - 192.168.15.5-192.168.15.27 (IPv4 range long form)
  - 192.168.15.5-27 (IPv4 range short form)
  - 192.168.15.128/25 (CIDR notation)
  - 2001:db8::1 (IPv6 address)
  - 2001:db8::1-2001:db8::15 (IPv6 range long form)
  - 2001:db8::1-15 (IPv6 range short form)
  - 2001:db8::/120 (CIDR notation)

  All options can be mixed and matched and entered as a comma separated list. The netmask in the CIDR notation is restricted however to a maximum of 20 for IPv4 and 116 for IPv6. In both cases the result is a maximum of 4096 IP addresses.
- *Interface Access*: Here it can be specified which network adapter a user can run a scan. A comma separated list of network adapters can be entered and similar to the Host Access it can be chosen between a whitelist and blacklist methodology.



Login Name: **ralf**
Roles: User
Groups:
Host Access: Allow all and deny: 10.0.15.0/24
Interface Access: Allow all and deny:

Fig. 15.2: Displaying a user.

Tip: In general the whitelist methodology should be used and scans of systems denied except for the chosen systems. This is to ensure that users do not scan systems by accident or unknowingly that are outside of there are of responsibility, are located somewhere on the Internet or react to a malfunctioning scan.

After creating the user the user's properties are displayed. The display should be verified to ensure that the user does not have too many permissions assigned to him.

15.1.2 Simultaneous Log in

It is possible, of course, that two users are logged into a GSM at the same time. If the same user wants to log in multiple times the log in must be performed from a different PC or at least a different browser. Another log in in the same browser invalidates the first login.

15.1.3 User Roles

Starting with Greenbone OS 3.1 the Greenbone Security Assistant allows for the creation and configuration of your own user roles. Like in all other instances the modification of the included default roles is not possible. However they can be copied (cloned). This clone then can be modified. This ensures consistent behaviour when updating the software.

The User Management can be accessed via the web interface in the menu *Administration* in the submenu *Roles*. The following three roles are available by default:

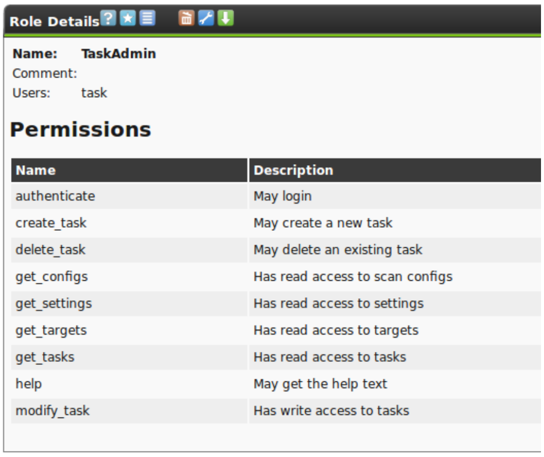
- *Admin*: This role by default has all permissions. It is especially allowed to create and manage other users.
- *Guest*: This role corresponds with the Info role. It merely is not allowed to change its settings.
- *Info*: This role (Information Browser) only has read access to the NVTs and SCAP information. All other information is not available.
- *Monitor*: This role has access to performance data of the GSM (see section *Monitoring and Debugging* (page 32)).
- *Observer*: This role has read access to the system. It is not allowed to start or create new scans. It has only read access to the scans for which the respective users have been set up as observers.
- *Super Admin*: This role has access to all objects of all users. It has no relation to the SuperUser in the command line. This role can not be configured in the web interface. The configuration is only possible in the GOS-Admin-Menu (see section *Super Admin* (page 170)),
- *User*: This role by default has all permissions with the exception of user, role and group management. Besides this role is not allowed to synchronize and manage the feeds. In the web interface there is no access to the menu option *Administration*. All other option, however, are available to this role.

Additional roles can easily be created. The simplest way is to copy one of the existing roles that reflects your needs the closest and modify it. In rare cases you might want to create a role that only supports limited functionality. Then it makes more sense to start with an empty role.

User can have more than one role. Therefore permissions can be grouped with the help of the roles. If more than more than one role is being assigned to a user the permissions will be added.

Hence a role *Maintenance* can be created for example. This role is being assigned the following permissions:

- *authenticate*
- *get_settings*
- *write_settings*
- *help*
- *describe_cert*
- *describe_feed*
- *describe_scap*
- *sync_cert*
- *sync_feed*
- *sync_scap*



Name: **TaskAdmin**
Comment:
Users: task

Permissions

Name	Description
authenticate	May login
create_task	May create a new task
delete_task	May delete an existing task
get_configs	Has read access to scan configs
get_settings	Has read access to settings
get_targets	Has read access to targets
get_tasks	Has read access to tasks
help	May get the help text
modify_task	Has write access to tasks

Fig. 15.3: The TaskAdmin role only has restricted access.

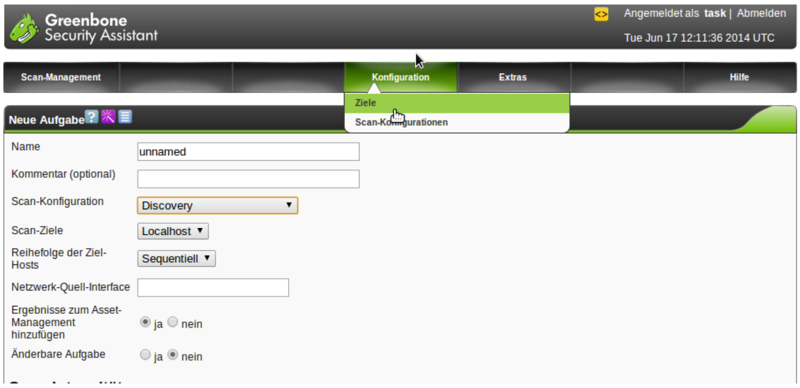
Additional roles then can have the name *TargetAdmin*, *ScanConfigAdmin*, *TaskAdmin* and *Scanner* and assigned permissions respectively. Important is the fact that roles have to have at minimum the permissions *authenticate* and *get_settings*. These are an imperative requirement to log into the web interface. The permission *write_settings* makes sense as well. Then a user can change their own password, time zone and other personal settings.

Users can be assigned different permutations of these roles. This allows specific users to configure target systems, scan configurations or configure and start the actual scan. In the selection of the permissions only the permissions that are not assigned are being displayed. This simplifies adding and the overview of the still available permissions.

If a user logs in with the role *TaskAdmin* later the menu options are restricted respectively.

15.1.4 Guest Log in

The GSM can be configured for guest log in. As guest the user is only allowed to access the SecInfo-Management (see chapter SecInfo Management (page 187)). This offers easy access to current infor-



Name	unnamed
Kommentar (optional)	
Scan-Konfiguration	Discovery
Scan-Ziele	Localhost
Reihenfolge der Ziel-Hosts	Sequentiell
Netzwerk-Quell-Interface	
Ergebnisse zum Asset-Management hinzufügen	● ja ○ nein
Änderbare Aufgabe	○ ja ● nein

Fig. 15.4: The menu selection for the TaskAdmin role is restricted.

mation without password.

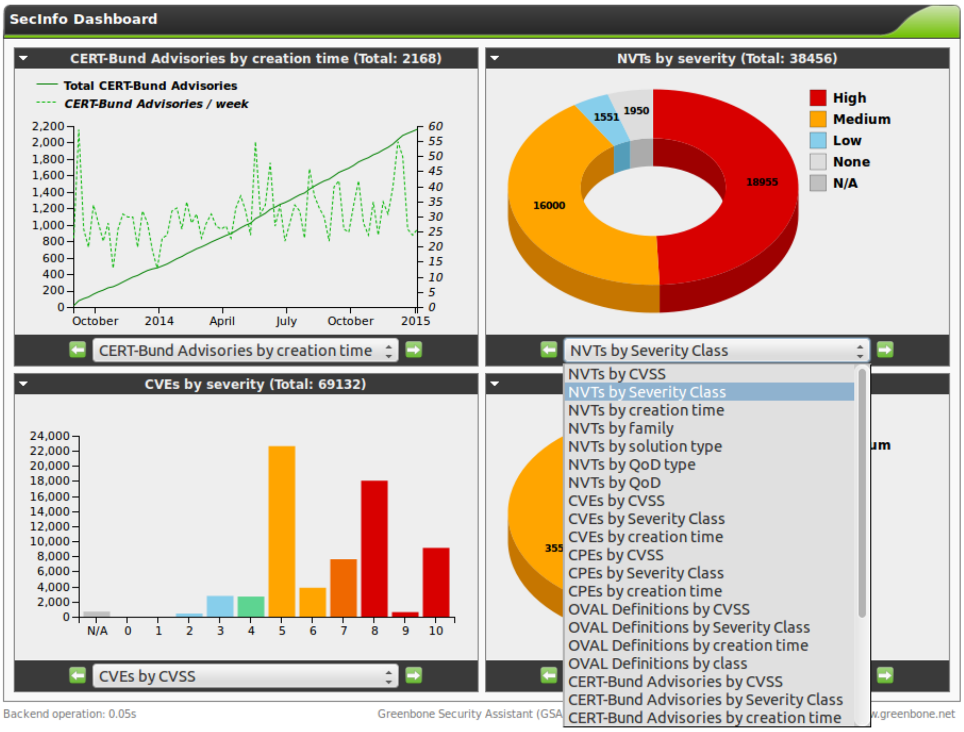


Fig. 15.5: The guest role has access to the SecInfo Dashboard.

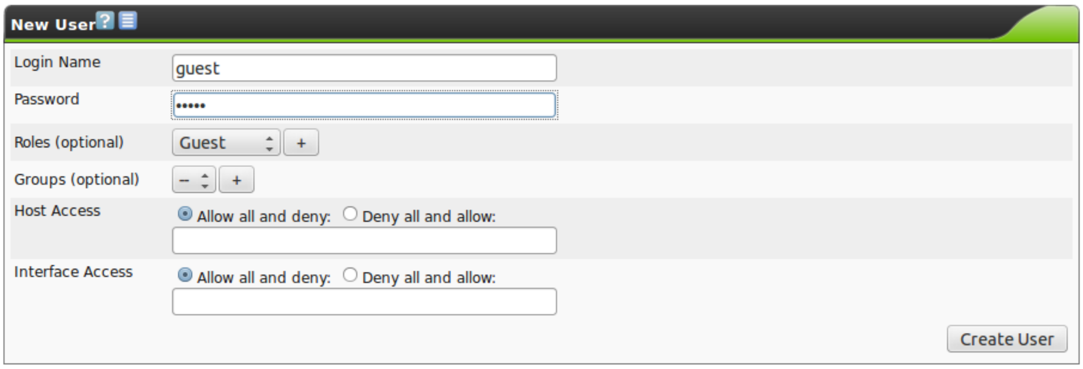
To allow this guest access a user can be created and assigned the *Guest* role.

Having knowledge of the password this user now can log in and is presented with the dashboard.

To allow a guest log in without password it must be activated on the command line first. To do so start the GOS-Admin-Menu and select the option *User*. Afterwards activate the *Guest login* in the respective option. Possible values are `disabled` and `enabled`. Then you to enter the name of the guest user and their password. This is done in the same menu under the *Guest User* option. This menu option appears as soon as the guest access is enabled.

Activate the changes by selecting *Commit* in the menu. Alternatively access can be enabled via `guest_login`:

```
gsm: get guest_login
s guest_login disabled
gsm: set guest_login enabled
```



New User

Login Name	guest
Password	•••••
Roles (optional)	Guest
Groups (optional)	–
Host Access	● Allow all and deny: ○ Deny all and allow:
Interface Access	● Allow all and deny: ○ Deny all and allow:

Fig. 15.6: Create a guest user.

```
gsm: set guest_user guest
gsm: set guest_password guest
gsm *: commit
gsm: get guest_login
s guest_login enabled
```

Afterwards a reboot is required. Now on the log in screen the guest log in is available (see figure *Log in as guest user without password.* (page 170))

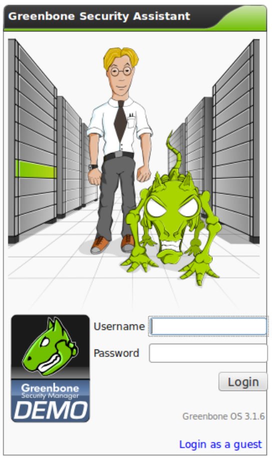


Fig. 15.7: Log in as guest user without password.

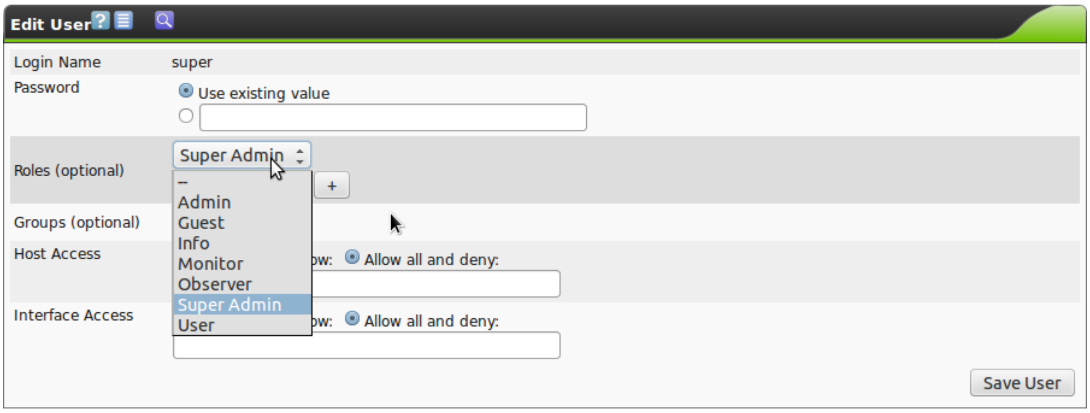
15.1.5 Super Admin

The Super Admin is the highest level of access. It was introduced with the new permission concept. Initially the regular admin role is equal to a simple user. However the admin user is allowed to create new users, modify and delete users. Additionally the admin can view, modify and delete any permissions on the system. However the admin is subject to those permissions. If a user creates a private scan configuration but does not share it, the Admin can not view the scan configuration. Of course the Admin could create respective permissions itself to the user created resource.

The Super Admin is excluded from this. The Super User is allowed to view and edit any configuration settings of any user.

The Super Admin can not be created in the web interface. To create the Super Admin access to the command line is required. This user and password can be created in Gos-Admin-Menu under the menu *User* submenu *Add Super Admin*.

Afterwards the user can be edited in the web interface.



Edit User

Login Name: super

Password: ● Use existing value ○

Roles (optional): Super Admin

Groups (optional)

Host Access: ● Allow all and deny:

Interface Access: ● Allow all and deny:

Fig. 15.8: The Super Admin **can not** be created in the web interface!

The Super Admin can not be modified by the regular admin. Only the Super Admin itself can modify the settings of this user!

Super Permissions

A role can be assigned with Super-Permissions. Then the role can access all objects in a group.

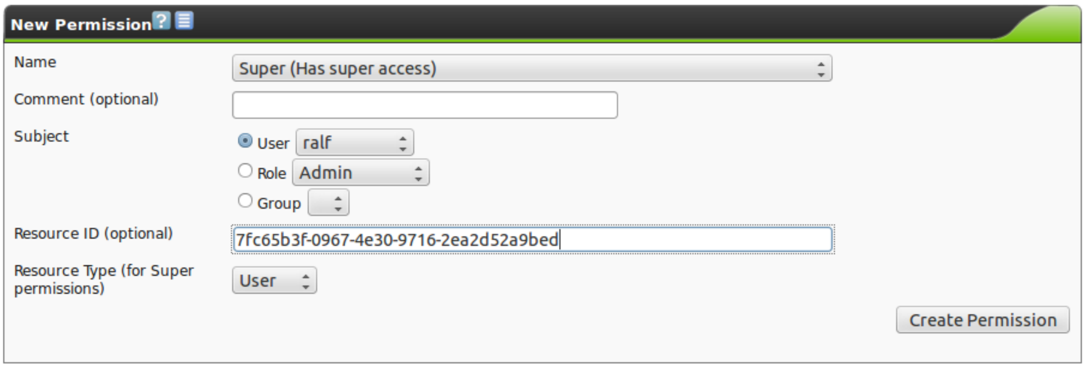
Any resource created on the GSM (scan, configuration, target, and so on) is either global or is owned by a specific user. Global resources are identified by the icon. Any resource that is not global can can be viewed and used by its user initially. Individual permissions are necessary to make the resource available to other users. This is very cumbersome. Therefore the Greenbone OS 3.1 offers the option to assign *Super Permissions*. A user can get these Super Permissions for:

- User
- Role
- Group
- Any

These Super Permissions then allow complete access to any resources of the respective user, role, group or effectively all resources. The any access can not be set explicitly. It is a privilege of the Super Admin (see section *Super Admin* (page 170)). This is why the last Super Permission can only be set by creating a Super Admin.

A user can only set Super Permissions for objects created he created himself. First the user must determine the Resource ID of the user, the role or the group for which to set the Super Permissions.

Afterwards the values can be entered in the dialog.



New Permission

Name: Super (Has super access)

Comment (optional):

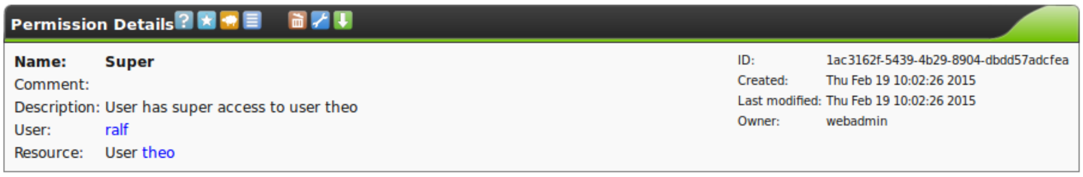
Subject: ● User ralf ○ Role Admin ○ Group

Resource ID (optional): 7fc65b3f-0967-4e30-9716-2ea2d52a9bed

Resource Type (for Super permissions): User

Fig. 15.9: For the Super Permission the Resource ID is required.

In the success message instead of the Resource ID the name is being displayed in clear text.



Permission Details

Name: **Super**
Comment:
Description: User has super access to user theo
User: ralf
Resource: User theo

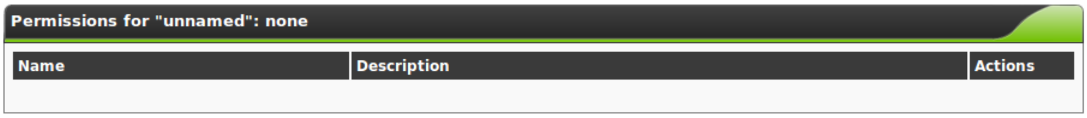
ID: 1ac3162f-5439-4b29-8904-dbdd57adcfea
Created: Thu Feb 19 10:02:26 2015
Last modified: Thu Feb 19 10:02:26 2015
Owner: webadmin

Fig. 15.10: The user Ralf has Super Access to the resources of the user Theo.

The Super Permissions simplify the permission management on the GSM. Super Permissions for entire groups can be assigned very easily. This allows all users of a group access to all resources that are being created by other members of the group.

GetUsers Role for Observers

The GSM allows for management of observers (see section *Permissions* (page 60)). These are users that have read access to specific tasks and their respective reports. These observers by default can only get permission to tasks and reports by administrators. Regular users can not give access to their own tasks to observers. Therefore they can not share their tasks with other users. For them the respective dialog to manage permissions in not functional.

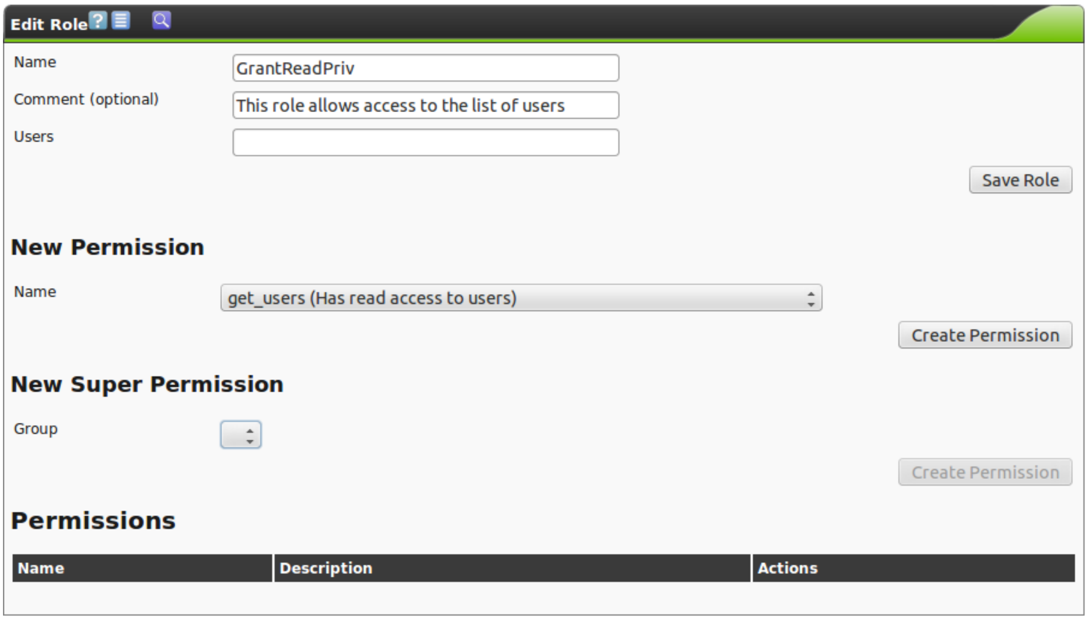


Permissions for "unnamed": none

Name	Description	Actions

Fig. 15.11: Regular users can not create observers.

For regular users to assign read permission to their tasks to other users as well they require the permission *get_users* to access the user database. This permission is being managed simply by its own role. For this create a role GrantReadPriv (see figure *The role GrantReadPriv allows to manage read access.* (page 172)). In a second step assign it the permission gos:perm:*get_users*. In doing this every user with this additional role is assigned the permission to share read access to their own tasks.



Edit Role

Name: GrantReadPriv
Comment (optional): This role allows access to the list of users
Users:

New Permission

Name: get_users (Has read access to users)

New Super Permission

Group:

Permissions

Name	Description	Actions

Fig. 15.12: The role GrantReadPriv allows to manage read access.

Then, in addition, this role must only be assigned to the respective users.

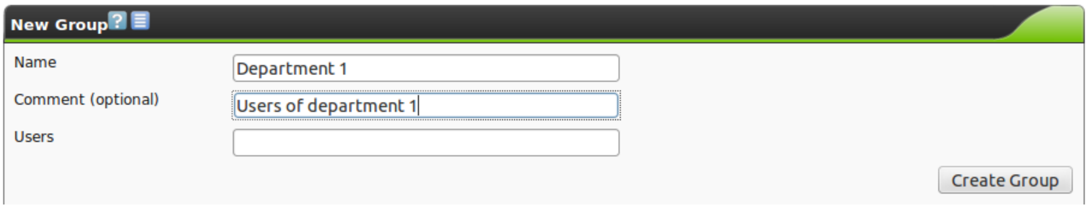
Note: In case the user is also allowed to share read access to groups or roles the *get_groups* and *get_roles* permissions must be assigned respectively.

15.1.6 Groups

Aside of the roles group management is also part of the Greenbone Security Assistant. These groups are used to logically group users. Additionally through the groups permissions can be assigned as well (see section *Permissions* (page 173)). By default no groups are set up. Indefinite groups can be created.

The following information must be included:

- Name: The name of the Group can be a maximum of 80 characters and can contain letters and numbers.
- Comment: An optional comment that describes the group in more detail.
- Users: The members of the group can be selected directly. The members can be separated by a space or comma. The length of the entry can be a maximum of 1000 characters. Alternatively, group memberships can be managed in the user profile directly.



Name	Department 1
Comment (optional)	Users of department 1
Users	

Fig. 15.13: Groups can be used to manage permissions.

15.1.7 Permissions

Under the menu option *Configuration/Permissions* every single permission assigned on the system can be viewed. This can easily reach hundreds of permissions if multiple roles are created. Each individual permission displayed always relates to exactly one subject.

A subject can be either

- a user
- a role
- or a group.

Normally permissions are being managed using the web interface vie the roles (see section *User Roles* (page 167)). Thereby the permissions of the role can be managed in the role management as well as here. Alternatively permissions can be assigned directly to users and groups.

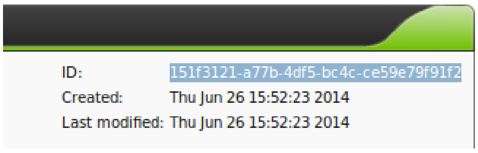
This option gives you the most possible flexibility when managing permissions. However adding and managing permissions using this dialog is only recommended for experienced users who are looking for a specific permission or who want to delete a specific user, for example.

Note: It is also possible to modify the permissions of the default roles with this dialog. This could have unwanted effects when updating and the permissions are reset again.

Sharing Individual Objects for Other Users

Every user can share indefinite objects created by the user. However, the user must be assigned the permission *get_users*. Otherwise the user will not have permission to determine the name of other users (see section *GetUsers Role for Observers* (page 172)).

To share an object, first determine the Object-ID. Sharing by name is not possible. To do so display the object that is to be shared in the browser (i.e. a filter). At the top right of the display you can find and copy the ID.



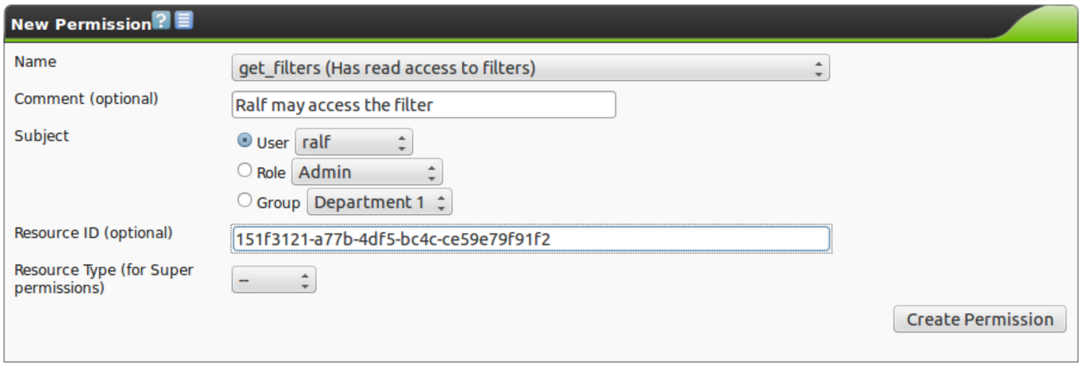
ID: 151f3121-a77b-4df5-bc4c-ce59e79f91f2
Created: Thu Jun 26 15:52:23 2014
Last modified: Thu Jun 26 15:52:23 2014

Fig. 15.14: Copying of the ID of an object to be shared.

Afterwards switch into the menu *Configuration/Permissions*. Create a new permission ★. Then select the proper permission for the object to be shared:

- Filter: *get_filters*
- Scan configuration: *get_configs*
- Alert: *get_alerts*
- Notes: *get_notes*
- Overrides: *get_overrides*
- Tags: *get_tags*
- Targets: *get_targets*
- Task with report: *get_tasks*
- Schedules: *get_schedules*

Select the appropriate subject (user, role or group) and paste the copied Resource ID into the respective field.



New Permission

Name	get_filters (Has read access to filters)
Comment (optional)	Ralf may access the filter
Subject	● User ralf ○ Role Admin ○ Group Department 1
Resource ID (optional)	151f3121-a77b-4df5-bc4c-ce59e79f91f2
Resource Type (for Super permissions)	--

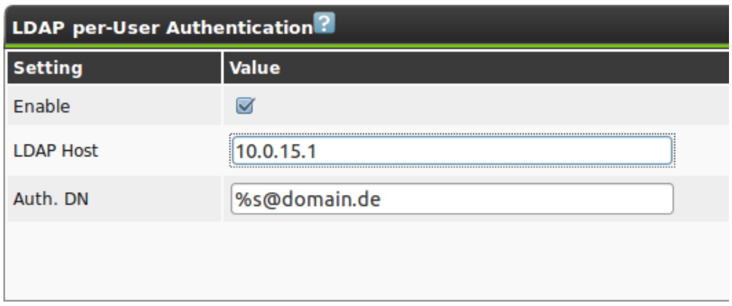
Fig. 15.15: Copying of the ID of an object to be shared.

15.1.8 Central User Management

Especially in larger environments with multiple users it is often difficult to achieve synchronization for passwords. The effort to create new or reset passwords is often very high. To avoid this, the GSM appliance supports the usage of a central password store via LDAP. The GSM will use the directory service only for authentication on a per user basis. This means that users who should be able to authenticate through the directory service have to exist on the GSM as well and have to be configured for authentication through the directory service as well.

Prerequisite for using central authentication is the naming of the users with the same name as the object in the LDAP tree.

Below the connection to a LDAP tree is covered. Thereby the GSM appliance uses a very simple interface. While other most systems supporting LDAP first search for the matching object in the LDAP tree and subsequently log in as this object afterwards (Search&Bind), the GSM appliance uses a simple bind with a hard coded object path.



LDAP per-User Authentication

Setting	Value
Enable	☑
LDAP Host	10.0.15.1
Auth. DN	%s@domain.de

Fig. 15.16: Central LDAP authentication requires entering the DN.

Then the distinguishedName of the objects can be defined distinctively. Thereby the wildcard %s replaces the username. Examples for the *Auth. DN* are:

- `uid=%s,ou=people,dc=domain,dc=de`
- `%s@domain.de`
- `domain.de\%s`

While the first example should work for any LDAP server with the correct attributes, the second and third example are typical formats used by Active Directory. Hereby the exact location of the user object is irrelevant.

The first example does not support users in different sub trees or different recursive depths of an LDAP tree. All users that need to log into the GSM must be in the same branch and in the same level of the LDAP tree!

The only other information required is the *LDAP Host*. Only one system with its IP address or name can be entered here.

Once you have enabled LDAP authentication, you will notice a new option Allow LDAP-Authentication only in the New User section which will be checked by default. Leave it checked if the new user should be able to login with the credentials configured in the directory service. For existing users you may enable this option through the Edit User dialog.

Please note that the user has to exist with this name in your directory service prior to use with the GSM. The GSM will not add, modify or remove users in your directory service. It will also not grant any user from your directory service automatically access to the GSM. You have to authorize every user separately by adding a user with the same name to the GSM with Allow LDAP-Authentication only checked as described above.

Also note that a locally configured user (i.e. a user which is not enabled for LDAP authentication) “Smith” on the GSM takes precedence over a user “Smith” in the connected directory service.

The LDAP authentication will only be functioning after a reboot. This reboot is uniquely mandatory after the LDAP authentication is being activated.

Note: The communication must be protected via SSL/TLS. If the LDAP server does not support this the GSM appliance will refuse working together. Details are covered in the following section.

LDAP with SSL/TLS

The GSM appliance uses either the command StartTLS via the LDAP protocol on port 389 or SSL via LDAPS on port 636. Therefore the LDAP server must make its services available via SSL. The exact configuration of all available LDAP servers is out of scope for this manual. Therefore the following are just a couple of references:

- Microsoft: http://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx
- OpenLDAP: http://www.openldap.org/doc/admin24/tls.html

In order for the GSM appliance to verify the identity of the LDAP server it must trust its certificate. For this the certificate of the issuing certificate authority must be stored on the GSM. To do so the certificate of the certificate authority must be exported as a BASE64 encoded file. A BASE64 encoded certificate is often using the file extension `.pem`. The file itself starts with `------BEGIN CERTIFICATE-------`.

The actual place where you may find this certificate may vary based on your environment.

- Univention Corporate Server (UCS)

  Here you may retrieve the CA certificate from the file `/etc/univention/ssl/ucsCA/CAcert.pem`. This file already contains the certificate in the correct format and may be used by the command `ldapcertdownload`.

- Active Directory LDAP

  If your Active Directory LDAP service does not yet use LDAPS, you may find the following article helpful: http://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx The Active Directory LDAP — CA certificates can then be exported using the following procedure which must be performed from a desktop or server that has access to the Certification Authority console.

  - Open the Certification Authority console from any domain-joined computer or server.
  - Right-click the name of the certification authority and then select Properties.
  - In the CA certificates dialog box, choose the General tab, and then select the certificate for the certification authority you want to access.
  - Choose View Certificate.
  - In the Certificate dialog box, choose the Certification Authority tab. Select the name of the root certification authority and then choose View Certificate.
  - In the Certificate dialog box, choose the Details tab and then choose Copy to File.
  - The Certificate Export Wizard appears. Choose Next.
  - On the Export File Format page, select the Base-64 encoded X.509 (.CER) option.
  - Choose Next.
  - In the File to Export box, choose the path and name for the certificate, and then choose Next.
  - Choose Finish. The .cer file will be created in the location that you specified in the previous step.
  - A dialog box appears to inform you that the export was successful. Choose OK to finish.

  The contents of the file may be used for the command `ldapcertdownload`.

This the file now must be transferred to the GSM. It is best to connect to the appliance via SSH (i.e. Putty). Open the certificate in an editor and copy it to the clipboard. Execute the command `ldapcertdownload` on the GSM command line and paste the certificate. Complete the copy process with Enter and Ctrl-D thereafter.

If the LDAP authentication does not work please verify that the entry in *LDAP Host* matches the commonName of the certificate of the LDAP server. If there are deviations the GSM appliance will refuse using the LDAP server.

OpenVAS Management Protocol

The entire control of the GSM appliance is done via the OpenVAS Management Protocol (OMP). The web interface is an OMP client as well and accesses the GSM functions via OMP.

The OMP protocol is documented at the Greenbone TechDoc portal: http://docs.greenbone.net/API/OMP/omp.html

This chapter covers the activation and use of the protocol by third party applications.

16.1 Activating the OMP Protocol

To be able to use the OMP protocol it first needs to be activated on the GSM appliance. The web interfaces uses the OMP protocol only locally on the appliance and not through the network. Activating the OMP protocol can either be performed directly through a variable on the command line (see section *OpenVAS Management Protocol (OMP)* (page 30)) or via the GOS-Admin-Menu under *Remote* and then *OMP*. It is important that in both cases the GSM appliance needs to be rebooted to activate this setting. Access to the OMP protocol is done in general SSL encrypted and authenticated. The same users as in the web interface are being used. The users are subject to the same restrictions and have the exact same permissions.

16.2 Access with `omp`

While with the help of the documentation of the OMP protocol your own application for access can be developed, Greenbone has developed a command line application for easy access and makes it available on the website for Linux and Windows.

- GNU/Linux omp[132]:
  - SHA1 checksum: d6b554361180b4b059bb7dd4be510cf58dcad18b
  - SHA256 checksum: 69d384088b8a84770e3ccfb81fe628d2cf12238e2fa9f2d320c7c4f6a615064b
- Microsoft Windows omp.exe[133] (digitally signed by Greenbone Networks GmbH)

The tool is a statically linked executable file that should work on most systems. Greenbone has released all components as open source so you can build the tool for other systems as well:

- GNU/Linux: * openvas-libraries-8.0.5.tar.gz (0.6 MB)[134] * openvas-cli-1.4.3.tar.gz (0.1 MB)[135]
- Microsoft Windows: omp-src-win.tar.gz (40 MB)[136]

[132] http://greenbone.net/download/tools/omp
[133] http://greenbone.net/download/tools/omp.exe
[134] http://www.greenbone.net/download/sources/openvas-libraries-8.0.5.tar.gz
[135] http://www.greenbone.net/download/sources/openvas-cli-1.4.3.tar.gz
[136] http://www.greenbone.net/download/sources/omp-src-win.tar.gz

The OMP protocol is XML based. Every command and every response is a OMP object.

The command line tool omp supplied by Greenbone Networks offers for one the direct sending and receiving of XML commands and XML responses. This is mostly helpful for batch mode (batch processing, scripting). Also the important commands are available as command line parameter including an option for human readable output. This is meant for spontaneous queries, tests and to create batch processes.

With this tool the OMP protocol can be used in a simple way:

```
omp --xml=<get_tasks/>
omp --get-tasks
omp --xml=<help/>
omp --help
```

In general the command line tool omp offers two uses. Via the --xml switch OMP commands are being sent in XML format. The answers will be in XML format as well. Using --pretty-print the output is formatted human readable.

Some commands are available as well as direct switches. --xml=<get_tasks/> corresponds to the switch --get-tasks. When using the latter the output will not be in XML format rather than a simple text table.

16.2.1 Configuring the Client

To use the omp command you need to log into the appliance. For this the required information is supplied via the options --user, --password, --host and --port. In order not to have to supply this information with each execution the connection data can be saved in the file omp.config for simplification in the home directory of the user. On Unix like systems it is $(HOME)/omp.config. On Windows systems the file can be found in %USERPROFILE%omp.config. Create the file with the following content (host, username and password need to be changed respectively of course) and pay attention to capitalization). If the password is left out, omp will ask for it when started.

```
[Connection]
host=gsm
port=9390
username=webadmin
password=password
```

16.2.2 Starting a Scan

A typical example for using the OMP protocol is the automatic scan of a new system. Below we assume that an Intrusion Detection System is in use that monitors the systems in the DMZ and immediately discovers new systems and unusual TCP ports not used up to now. If such an event is being discovered the IDS should automatically initiate a scan of the new system. This should be done with the help of a script. For the this omp is very suitable.

Starting point is the IP address of the new suspected system. For this IP address a target needs to be created in the GSM.

For this function there is no simple option in the omp command. This is why this must occur with the help of XML. Under http://docs.greenbone.net/API/OMP/omp-6.0.html#command_create_target the command create_target is described.

If the IP address is saved in the variable IPADDRESS the respective target can be created with the following command:

```
$ ./omp -X "<create_target><name>Suspect Host</name><hosts>$IPADDRESS</hosts>
</create_target>"
```

```
<create_target_response status="201" id="aa410e98-ff8d-45b6-be98-11fd7a895435"
status_text="OK, resource created"></create_target_response>
```

Now the task can be created. Using `-c` you specify the scan configuration. The target is specified using `-t`:

```
$ ./omp -C -c daba56c8-73ec-11df-a475-002264764cea --name "ScanSuspectHost" \
-t aa410e98-ff8d-45b6-be98-11fd7a895435

a4bdad7c-6135-45c1-884b-fd226a6e7a19
```

The output us the ID of the task. It is required for the start.

The other IDs used by the command may be retrieved using the following commands displaying the available targets and scan configs:

```
$ ./omp -T
b493b7a8-7489-11df-a3ec-002264764cea  Localhost
aa410e98-ff8d-45b6-be98-11fd7a895435  Suspect Host

$ ./omp -g
8715c877-47a0-438d-98a3-27c7a6ab2196  Discovery
085569ce-73ed-11df-83c3-002264764cea  empty
daba56c8-73ec-11df-a475-002264764cea  Full and fast
698f691e-7489-11df-9d8c-002264764cea  Full and fast ultimate
708f25c4-7489-11df-8094-002264764cea  Full and very deep
74db13d6-7489-11df-91b9-002264764cea  Full and very deep ultimate
2d3f051c-55ba-11e3-bf43-406186ea4fc5  Host Discovery
bbca7412-a950-11e3-9109-406186ea4fc5  System Discovery
```

Now the task needs to be started:

```
$ ./omp -S a4bdad7c-6135-45c1-884b-fd226a6e7a19

58f7f696-5ec7-49f4-9968-1d35991f8f2e
```

The output is the response of the report. Now it has to be waited until the task is fully completed. The status of the task can be displayed with the following command:

```
$ ./omp --get-tasks a4bdad7c-6135-45c1-884b-fd226a6e7a19

a4bdad7c-6135-45c1-884b-fd226a6e7a19  Running 20%  ScanSuspectHost
58f7f696-5ec7-49f4-9968-1d35991f8f2e  Running    0   0   1   2  2014-06-27T12:43:17Z
$ ./omp --get-tasks a4bdad7c-6135-45c1-884b-fd226a6e7a19

a4bdad7c-6135-45c1-884b-fd226a6e7a19  Done         ScanSuspectHost
58f7f696-5ec7-49f4-9968-1d35991f8f2e  Done       0   0   1   8  2014-06-27T12:43:17Z
```

As soon as the scan is completed the report can be downloaded. For this the ID that was output when the task was started is required. Also a meaningful report format must be entered. The IDs for the report formats can be displayed via:

```
$ ./omp --get-report-formats
910200ca-dc05-11e1-954f-406186ea4fc5  ARF
5ceff8ba-1f62-11e1-ab9f-406186ea4fc5  CPE
9087b18c-626c-11e3-8892-406186ea4fc5  CSV Hosts
c1645568-627a-11e3-a660-406186ea4fc5  CSV Results
35ba7077-dc85-42ef-87c9-b0eda7e903b6  GSR PDF
ebbc7f34-8ae5-11e1-b07b-001f29eadec8  GXR PDF
6c248850-1f62-11e1-b082-406186ea4fc5  HTML
77bd6c4a-1f62-11e1-abf0-406186ea4fc5  ITG
a684c02c-b531-11e1-bdc2-406186ea4fc5  LaTeX
9ca6fe72-1f62-11e1-9e7c-406186ea4fc5  NBE
c402cc3e-b531-11e1-9163-406186ea4fc5  PDF
```

```
9e5e5deb-879e-4ecc-8be6-a71cd0875cdd  Topology SVG
a3810a62-1f62-11e1-9219-406186ea4fc5  TXT
a994b278-1f62-11e1-96ac-406186ea4fc5  XML
```

Now the report can be loaded:

```
$ ./omp --get-report 58f7f696-5ec7-49f4-9968-1d35991f8f2e --format \
c1645568-627a-11e3-a660-406186ea4fc5 > report.csv
```

For a complete automatic processing of the data the task could be combined with an alert that could send out the report automatically at a specific severity level.

16.2.3 Updating the target host of an alterable task using OMP

The following example shows how the target of an alterable task can be changed through OMP, for example based on a list generated by another tool. Variables used in this example:

- TASK_UUID The UUID of the task for which you want to modify the target. The task must be set to "alterable".
- NEW_HOSTS The new list of hosts to use for the target.
- NEW_NAME The name for the new target object.

On UNIX-like systems

The following examples use the `xmlstarlet` tool to parse XML data. This can of course be replaced by other solutions if desired.

- Retrieve the UUID of the old target object from the task:

```
$ OLD_TARGET_UUID=$(omp --xml "<get_tasks task_id=\"$TASK_UUID\"></get_tasks>" | \
xmlstarlet sel -t -v /get_tasks_response/task/target/@id)
```

- Create a new target object by cloning the old target object:

```
NEW_TARGET_UUID=$(omp --xml "<create_target><copy>$OLD_TARGET_UUID</copy> \
<name>$NEW_NAME</name></create_target>" | \
xmlstarlet sel -t -v /create_target_response/@id)
```

- Update the new target object with the new list of hosts:

```
omp --xml "<modify_target target_id=\"$NEW_TARGET_UUID\"> \
<hosts>$NEW_HOSTS</hosts><exclude_hosts/></modify_target>"
```

- Update the task to use the new target object:

```
omp --xml "<modify_task task_id=\"$TASK_UUID\"> \
<target id=\"$NEW_TARGET_UUID\"/></modify_task>"
```

- Remove the now unused old target:

```
omp --xml "<delete_target target_id=\"$OLD_TARGET_UUID\"/>"
```

On Windows-like systems

The following examples use the "Select-XML" command of the PowerShell to parse XML data. This can of course be replaced by other solutions if desired.

- Retrieve the UUID of the old target object from the task:

```
omp --xml "<get_tasks task_id='$TASK_UUID'></get_tasks>" > get_tasks_response.xml
$OLD_TARGET_UUID = Select-Xml .\get_tasks_response.xml `
-xpath "/get_tasks_response/task/target[@id]" | ForEach-Object { $_.Node.id}
```

- Create a new target object by cloning the old target object:

```
omp --xml "<create_target><copy>$OLD_TARGET_UUID</copy>
<name>$NEW_NAME</name></create_target>" > create_target_response.xml
$NEW_TARGET_UUID = Select-Xml .\create_target_response.xml `
-xpath "/create_target_response[@id]" | ForEach-Object { $_.Node.id }
```

- Update the new target object with the new list of hosts:

```
omp --xml "<modify_target target_id='$NEW_TARGET_UUID'>
<hosts>$NEW_HOSTS</hosts><exclude_hosts/></modify_target>"
```

- Update the task to use the new target object:

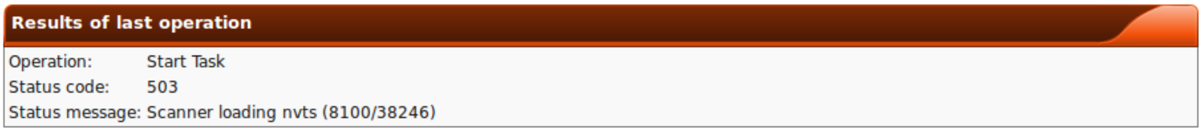
```
omp --xml "<modify_task task_id='$TASK_UUID'>
<target id='$NEW_TARGET_UUID'/></modify_task>"
```

- Remove the now unused old target:

```
omp --xml "<delete_target target_id='$OLD_TARGET_UUID'/>"
```

16.2.4 Status Codes

The OMP protocol uses status codes for communication. These status codes can be displayed in the web interface.



Results of last operation

Operation: Start Task
Status code: 503
Status message: Scanner loading nvts (8100/38246)

Fig. 16.1: The OMP protocol uses status codes and alerts to display statuses.

The status codes are similar to HTTP status codes. The following codes are being used:

2xx: The command was sent, understood and accepted successfully.

- 200: OK
- 201: Resource created
- 202: Request submitted

4xx: A user error occurred.

400: Syntax error This could be different syntax errors. Often elements or attributes in the OMP command are missing. The status text shows additional information. Currently this status code is also used for missing or wrong authentication.

401: Authenticate First This is the error code that is being used for missing or wrong authentication. Currently the value 400 is still being used.

403: Access to resource forbidden This is the error code that is being used for having not enough permissions. Often `400: Permission denied` will be displayed instead as well.

404: Resource missing The resource could not be found. The Resource ID was empty or wrong.

409: Resource busy This error code happens, for example, if the feed synchronization is being started while it is already in progress.

5xx: A server error occurred

500: Internal Error This could be entries that exceed an internal buffer size.

503: Scanner loading NVTs The scanner is currently busy loading the NVTs from its cache. Try again later.

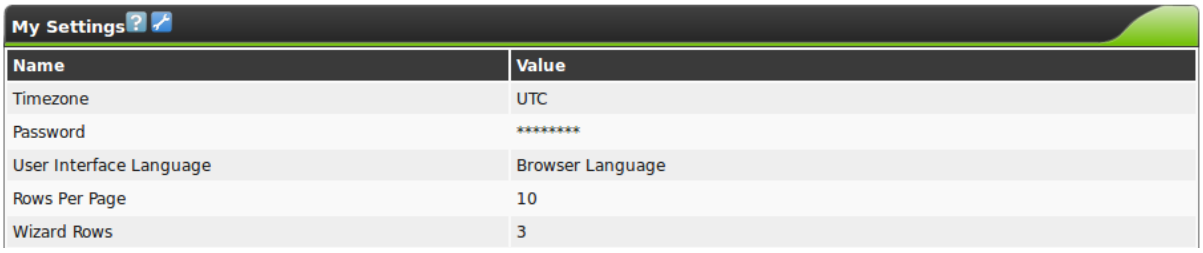
503: Service temporarily down Possibly the scanner daemon is not running. Often the problem could be expired certificates. Check the Readiness (see section *Readiness* (page 15))

503: Service unavailable: The OMP command is blocked on the GSM.

CHAPTER 17

My Settings

Every user of the GSM appliance can manage their own settings for the web interface. This setting can be accessed by either selecting *Extras* under the submenu *My Settings* or by clicking on the user name at the top right.



My Settings ? 🔧

Name	Value
Timezone	UTC
Password	********
User Interface Language	Browser Language
Rows Per Page	10
Wizard Rows	3

Fig. 17.1: Every user can manage their own settings.

By clicking the icon 🔧 the user can modify these settings. Important settings are:

Timezone: Internally the GSM saves all information in the UTC time zone. In order to display the data in the time zone of the user the respective selection is required here.

Password: Here the user can change their password.

User Interface Language: Here the language is defined. The default uses the browser setting. To always get an English or German interface use *english* or *german*.

Rows Per Page: This is the amount of results in a list.

Wizard Rows: This defines how long to display the wizard for. For example, if the value is set to 3 the wizard won't be displayed in the task overview as soon as a minimum of 4 tasks are available.

Details Export File Name: This defines the default name of the file for exported resource details. The format string can contain alphanumeric characters, hyphens, underscores and placeholders that will be replaced as follows:

- %C The creation date in the format YYYYMMDD. This gives the current date if a creation is not available, e.g. when exporting lists of resources
- %c The creation time in the format HHMMSS. Falls back to the current time similar to %C.
- %D The current date in the format YYYYMMDD
- %F The name of the format plugin used (XML for lists and types other than reports).
- %M The modification date in the format YYYYMMDD If the modification date is not available this gives either the creation date or the current date if a creation date is no available as well, e.g. when exporting lists of resources.
- %m The modification time in the format HHMMSS. Falls back to the createn time or current time similar to %M.

- %N The name fo the resource or the associated task for reports. Lists and types without a name will use the type (see %T).
- %T The resource type, e.g. "task", "port_list". Pluralized for lst pages.
- %t The current time in the format HHMMSS
- %U The unique ID of the resource or "list" for lists fo multiple resources.
- %u The name fo the currently logged in user.
- %% The percent sign (%).

***List Export File Name*:** This defines the default name of the file for exported resource lists (see above).

***Port Export File Name*:** This defines the default name of the file for exported reports (see above).

***Severity Class*:** Here the classification of the vulnerability respective to the score can be defined.

- NVD Vulnerabiliy Severity Ratings
  - 7.0 - 10.0: High
  - 4.0 - 6.9: Medium
  - 0.0 - 3.9: Low
- BSI Vulnerability Traffic Light
  - 7.0 - 10.0: Red
  - 4.0 - 6.9: Yellow
  - 0.0 - 3.9: Green
- OpenVAS classic
  - 5.1 - 10.0: High
  - 2.1 - 5.0: Medium
  - 0.0 - 2.0: Low
- PCI-DSS
  - 4.3 - 10.0: High
  - 0.0 - 4.2: None

***Filter*:** Here specific default filters for each page can be specified that are being activated automatically when the page is loaded.

CHAPTER 18

SecInfo Management

The *SecInfo Management* offers central access to different information relating to IT-Security. This includes the following information:

NVTs: These are the Network Vulnerability Tests. These tests test the target system for potential vulnerabilities.

CVEs: The Common Vulnerability and Exposures are vulnerabilities published by vendors and security researchers.

CPEs: The Common Platform Enumeration offers standardized names of the products that are being used information technology.

OVAL Definition: The Open Vulnerability Assessment Language offers a standardized language for the testing of vulnerabilities. OVAL definitions use this language to concretely discover vulnerabilities.

CERT-Bund Advisories: The CERT-Bund Advisories are published by the emergency response team[137] of the Federal Office for Information Security (German: Bundesamt für Sicherheit in der Informationstechnik, abbreviated as BSI). The main task of the CERT-Bund is the operation of a warning and information service publishing information regarding new vulnerabilities and security risks as well as threats for IT systems.

DFN-CERT Advisories: The DFN-CERT[138] is the emergency response team of the German Research Network (German: Deutsches Forschungsnetz, abbreviated as DFN).

The CVEs, CPEs and OVAL definitions are published and made accessible by NIST as part of the National Vulnerability Database (NVD) (see also section *Security Content Automation Protocol (SCAP)* (page 189)).

To get a quick overview over this information the Secinfo dashboard (see figure *The SecInfo Dashboard allows displaying data graphically.* (page 188)) exists. It allows for the graphical display of different information grouped by different aspects.

18.1 SecInfo Portal

SecInfo Data is being provided by Greenbone Networks online as well. This portal[139] can be accessed directly through the Internet. It corresponds to data that can be displayed in the GSM as well. The SecInfo Portal is a GSM ONE that has been configured especially for anonymous guest access. Contrary to a full-fledged GSM only the SecInfo management and the CVSS online calculator are available for the guest user.

The SecInfo portal achieves a multitude of functions:

[137] https://www.cert-bund.de/

[138] https://www.cert.dfn.de/

[139] https://secinfo.greenbone.net

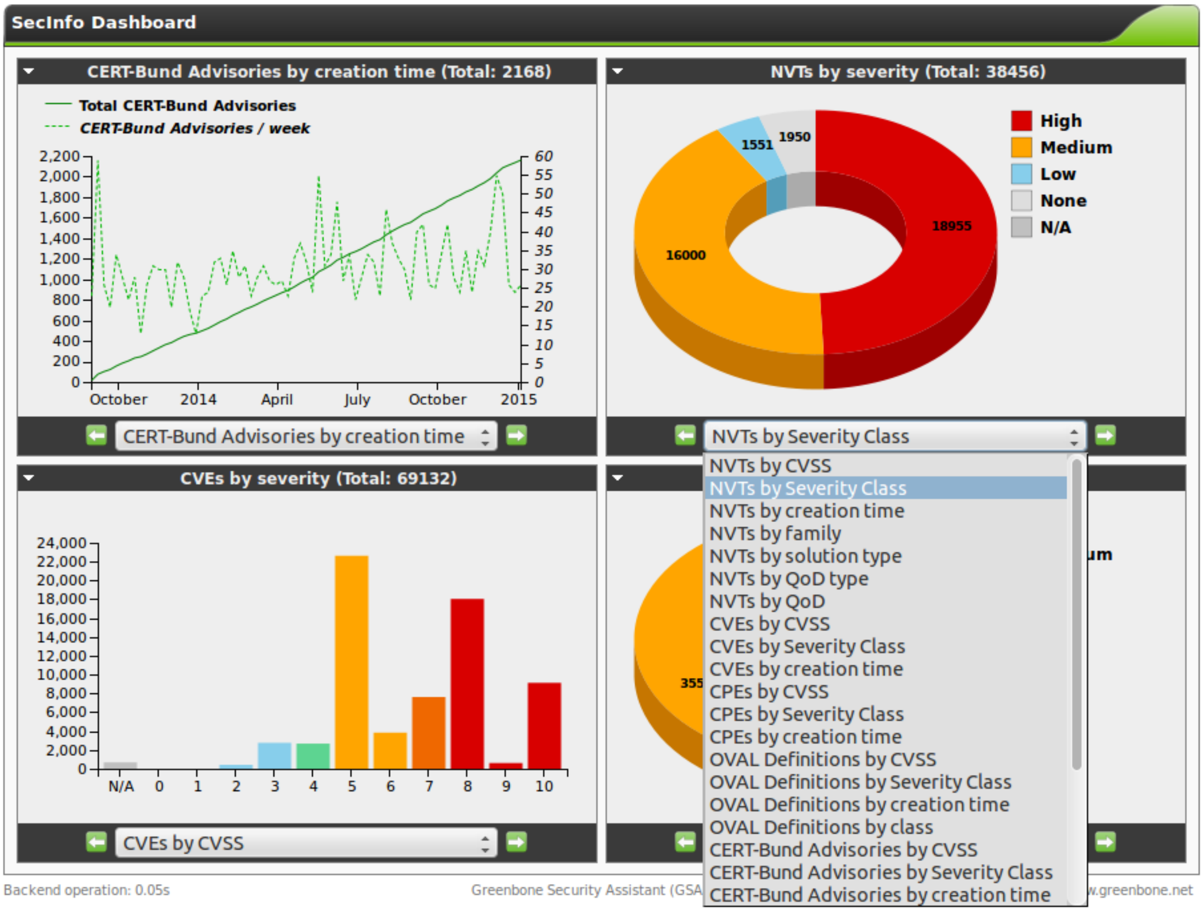


Fig. 18.1: The SecInfo Dashboard allows displaying data graphically.

- Anonymous access to details of the Greenbone vulnerability tests as well as SCAP data (CVE, CPE, OVAL) and messages of different CERTs. The data itself is referenced thus offering the possibility to browse by Security-Information regarding a product, a vendor or a specific vulnerability.
- Demo of the respective upcoming version of the Greenbone OS as soon as the SecInfo section reached beta status.
- Service for embedded diagrams as they are used on the Greenbone website for feed statistics for example.
- Service for direct links to details or specific selections, for example for a specific CVE (CVE-2014-0160, *Heartbleed*) or an overview: All published CVE notices in 2013.
- Service for links to CVSS vulnerability rating including CVSS online calculator: AV:N/AC:L/Au:N/C:P/I:P/A:P
- Example of how a GSM can be configured by yourself on an Intranet to allow direct links in internal reports and platforms.

Such access can be provided yourself by activating guest access (see section *Guest Log in* (page 168))

18.2 Network Vulnerability Tests

The abbreviation NVT stands for Network Vulnerability Test. These are test routines the GSM utilizes and that are updated regularly with the Greenbone Security Feed. Here you can find information when the test was developed, which systems are affected, what impact the vulnerabilities have and how they can be remediated.

Compared to the Greenbone OS 3.0 there are two new pieces of information, the Solution Type (see *Solution Type* (page 263)) and the Quality of Detection (QoD, see *Quality of Detection (QoD)* (page 261)).

With the introduction of the QoD the parameter `Paranoid` in the scan configuration (see chapter Scan Configuration (page 145)) is being removed without replacement. In the past a scan configuration without this parameter only used NVTs with a QoD of a minimum of 70%. Only with this parameter all NVTs were used. Now all NVTs are being used and executed in a scan configuration. The filtering of the results is done on based on QoD. That way all the results are always available in the database and can be turned on or off respectively.

18.3 Security Content Automation Protocol (SCAP)

The National Institute of Standards and Technology (NIST) in the USA provides the National Vulnerability Database[140] (NVD). NVD is a data repository for the vulnerability management of the US government. The goal is the standardized provision of the data for the automated processing and support for the function of vulnerability management and the implementation of compliance guide lines. The NVD provide different databases. They include

- check lists,
- vulnerabilities,
- misconfigurations,
- products and
- threat metrics.

For this the NVD utilizes the Security Content Automation Protocol[141] (SCAP). The Security Content Automation Protocol is a combination of different interoperable standards. Many standards were developed or derived from public discussion. The public participation of the community in the development is an important aspect for accepting and spreading of the SCAP standards. The SCAP protocol is currently specified in version 1.2 and includes the following components:

- Languages
  - XCCDF: The Extensible Configuration Checklist Description Format
  - OVAL: Open Vulnerability and Assessment Language
  - OCIL: Open Checklist Interactive Language
  - Asset Identification
  - ARF: Asset Reporting Format
- Collections
  - CCE: Common Configuration Enumeration
  - CPE: Common Platform Enumeration
  - CVE: Common Vulnerabilities and Exposure
- Metrics:
  - CVSS: Common Vulnerability Scoring System
  - CCSS: Common Configuration Scoring System
- Integrity
  - TMSAD: Trust Model for Security Automation Data

[140] https://nvd.nist.gov/

[141] http://scap.nist.gov/

OVAL, CCE, CPE and CVE are trademarks of NIST.

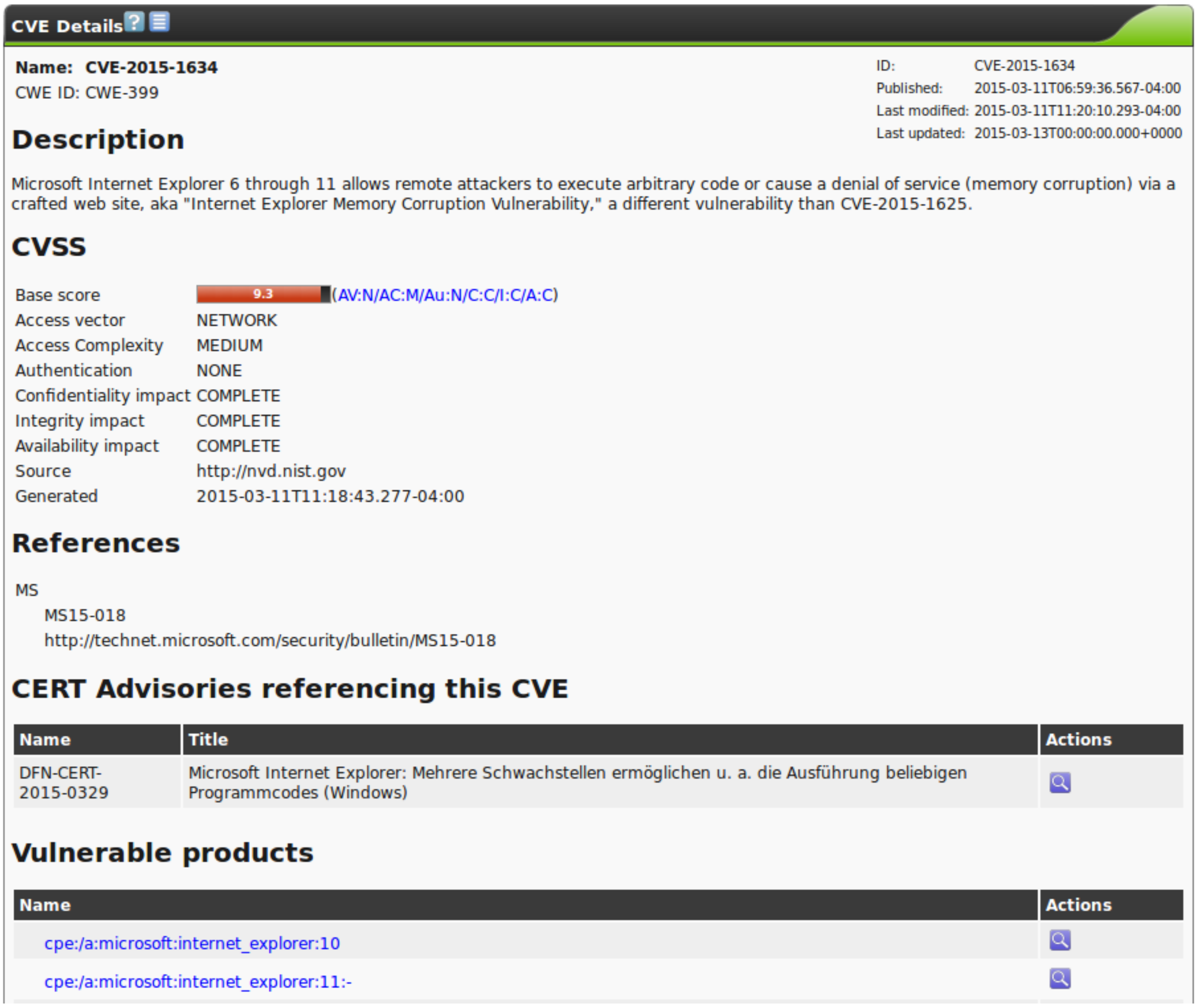
The Greenbone vulnerability scanner uses the OVAL standard, CVE, CPE and CVSS. By utilizing these standards the interoperability with other systems is guaranteed. These standards also allow comparing of the results.

Vulnerability scanners such as the Greenbone Security Manager can be validated by NIST respectively. The Greenbone Security Manager has been validated with respect to SCAP version 1.0[142].

Following, the standards utilized by the Greenbone Security Manager are being covered in more detail.

18.3.1 CVE

Due to the fact that in the past often multiple organizations discovered and reported vulnerabilities at the same time and assigned them different names, communication and comparison of the results was not easy. Different scanners reported the same vulnerability under different names. As a matter of fact instead of two different vulnerabilities it was actually the same vulnerability.



CVE Details

Name: CVE-2015-1634
CWE ID: CWE-399

ID:	CVE-2015-1634
Published:	2015-03-11T06:59:36.567-04:00
Last modified:	2015-03-11T11:20:10.293-04:00
Last updated:	2015-03-13T00:00:00.000+0000

Description

Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2015-1625.

CVSS

Base score	9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)
Access vector	NETWORK
Access Complexity	MEDIUM
Authentication	NONE
Confidentiality impact	COMPLETE
Integrity impact	COMPLETE
Availability impact	COMPLETE
Source	http://nvd.nist.gov
Generated	2015-03-11T11:18:43.277-04:00

References

MS
MS15-018
http://technet.microsoft.com/security/bulletin/MS15-018

CERT Advisories referencing this CVE

Name	Title	Actions
DFN-CERT-2015-0329	Microsoft Internet Explorer: Mehrere Schwachstellen ermöglichen u. a. die Ausführung beliebigen Programmcodes (Windows)	🔍

Vulnerable products

Name	Actions
cpe:/a:microsoft:internet_explorer:10	🔍
cpe:/a:microsoft:internet_explorer:11:-	🔍

Fig. 18.2: The CVEs include information regarding the severity and affected products.

To address this, MITRE [144], sponsored by the US-CERT, founded the CVE project in 1999. Every vulnerability is assigned a unique identifier consisting of the year and a simple number. This number then

[142] https://nvd.nist.gov/scapproducts.cfm

[144] MITRE (Massachusetts Institute of Technology Research & Engineering) Corporation is an organization for the management of research institutions for the United States government that was formed by splitting off from the Massachusetts Institute of Technology (MIT).

serves as central reference.

The CVE database of MITRE is not a vulnerability database. CVE was developed in order to connect the vulnerability database and other systems with each other. This allows for the comparison of security tools and services. This is why the CVE database does not contain any information regarding risk, impact or remediation of the vulnerability. Detailed technical information is also not included. A CVE only contains the identification number with status, a short description and references to reports and advisories.

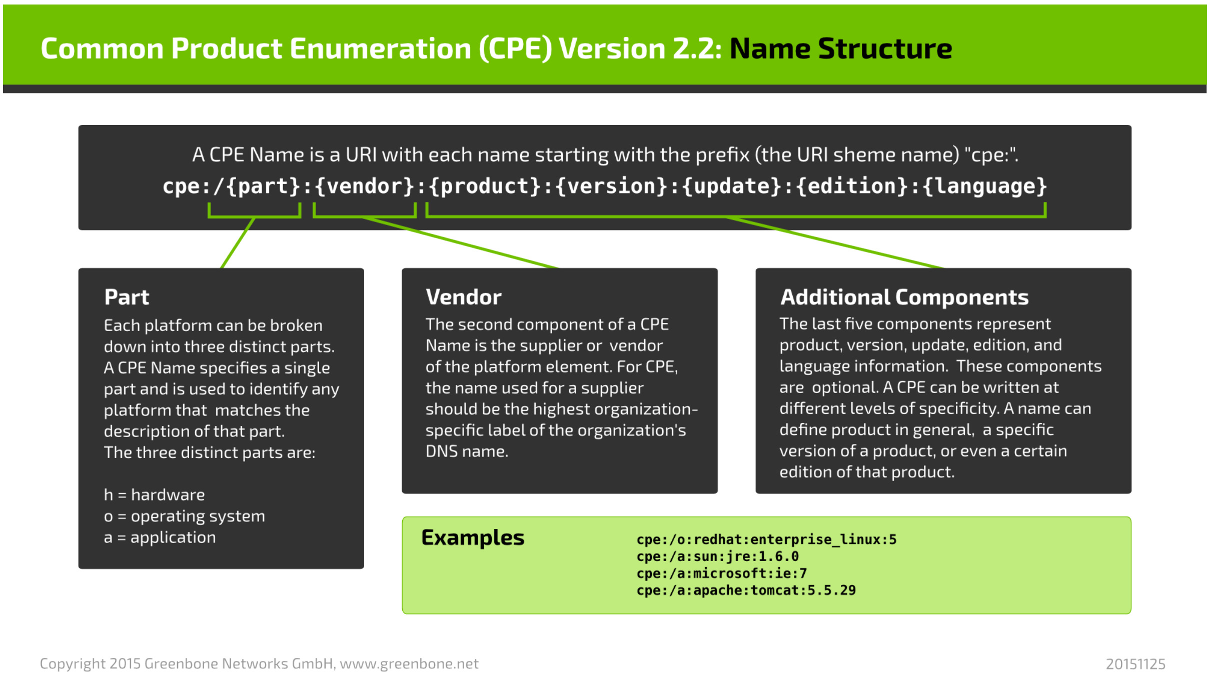
The National Vulnerability Database (NVD) refers to MITRE's CVE database and supplements this information with information in regards to remediation of the vulnerability, the severity, affected products and possible impact. Greenbone refers to the CVE database of the NVD so that information is included. At the same time does the GSM combine the information with the NVTs and the CERT-Bund and DFN-CERT advisories.

This information can be displayed comfortably in the web interface.

18.3.2 CPE

The abbreviation CPE stands for Common Platform Enumeration, modelled after CVE and started by MITRE as well, as an industry standard for a common naming convention for information technology systems. Hereby common naming exists for operating systems and applications allowing for global referencing.

Originally the Common Platform Enumeration (CPE) was initiated by MITRE. Today the CPE standard is maintained by the US American National Institute for Standards and Technology NIST as part f the National Vulnerability Database (NVD). NIST already had maintained the official CPE dictionary and the CPE specifications for many years. CPE is a structured naming schema for applications, operating systems and hardware devices. It is based on the generic syntax of the Uniform Resource Identifier (URI).



Common Product Enumeration (CPE) Version 2.2: Name Structure

A CPE Name is a URI with each name starting with the prefix (the URI sheme name) "cpe:".

`cpe:/{part}:{vendor}:{product}:{version}:{update}:{edition}:{language}`

Part

Each platform can be broken down into three distinct parts. A CPE Name specifies a single part and is used to identify any platform that matches the description of that part. The three distinct parts are:

h = hardware
o = operating system
a = application

Vendor

The second component of a CPE Name is the supplier or vendor of the platform element. For CPE, the name used for a supplier should be the highest organization-specific label of the organization's DNS name.

Additional Components

The last five components represent product, version, update, edition, and language information. These components are optional. A CPE can be written at different levels of specificity. A name can define product in general, a specific version of a product, or even a certain edition of that product.

Examples

```
cpe:/o:redhat:enterprise_linux:5
cpe:/a:sun:jre:1.6.0
cpe:/a:microsoft:ie:7
cpe:/a:apache:tomcat:5.5.29
```

Copyright 2015 Greenbone Networks GmbH, www.greenbone.net 20151125

Fig. 18.3: Common Product Enumeration: Name Structure

Due to the fact that the CPE standard is closely tied to the CVE standard, their combination allows for conclusion of existing vulnerabilities when discovering a platform or product.

CPE is composed of the following components:

Naming: The name specification describes the logical structure of well-formed names (WFNs), its binding to URIs and formatted character strings and the conversion of the WFNs and their bindings.

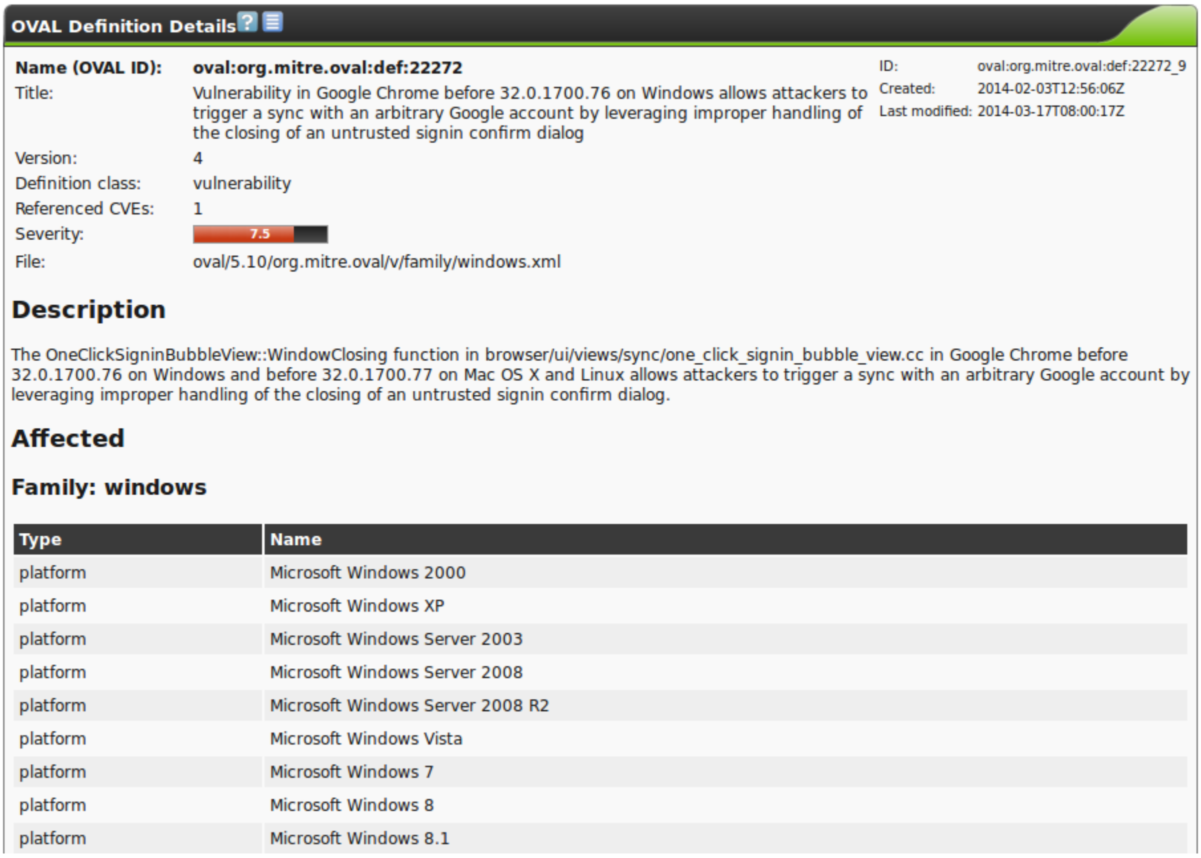
Name Matching: The name matching specification describes the methods to compare WFNs with each other. This allows for the testing if some or all refer to the same product.

Dictionary: The dictionary is a repository of CPE names and meta data. Every name defines an single class of an IT product. The dictionary specification describes the processes for the use of the dictionary, like the search for a specific name or entries, which belong to a more general class.

Applicability Language: The applicability language specification describes the creation of complex logical expressions with the help of the WFNs. These applicability statements can be used for the tagging of check lists, guide lines or other documentation and as such describe for which products these documents are relevant for.

18.3.3 OVAL

The Open Vulnerability and Assessment Language is also a Mitre project. It is a language to describe vulnerabilities, configuration settings (compliance), patches and applications (inventory). The XML based definitions allow for simple processing by automated systems. As such the OVAL definition `oval:org.mitre.oval:def:22127` of the inventory class describes the Adobe Flash Player 12 while the OVAL definition `oval:org.mitre.oval:def:22272` describes a vulnerability of Google Chrome under Windows.



OVAL Definition Details

Name (OVAL ID):	**oval:org.mitre.oval:def:22272**
Title:	Vulnerability in Google Chrome before 32.0.1700.76 on Windows allows attackers to trigger a sync with an arbitrary Google account by leveraging improper handling of the closing of an untrusted signin confirm dialog
Version:	4
Definition class:	vulnerability
Referenced CVEs:	1
Severity:	7.5
File:	oval/5.10/org.mitre.oval/v/family/windows.xml

ID:	oval:org.mitre.oval:def:22272_9
Created:	2014-02-03T12:56:06Z
Last modified:	2014-03-17T08:00:17Z

Description

The OneClickSigninBubbleView::WindowClosing function in browser/ui/views/sync/one_click_signin_bubble_view.cc in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allows attackers to trigger a sync with an arbitrary Google account by leveraging improper handling of the closing of an untrusted signin confirm dialog.

Affected

Family: windows

Type	Name
platform	Microsoft Windows 2000
platform	Microsoft Windows XP
platform	Microsoft Windows Server 2003
platform	Microsoft Windows Server 2008
platform	Microsoft Windows Server 2008 R2
platform	Microsoft Windows Vista
platform	Microsoft Windows 7
platform	Microsoft Windows 8
platform	Microsoft Windows 8.1

Fig. 18.4: OVAL describes the discovery of vulnerabilities.

These OVAL definitions are created made available in XML and describe the discovery of individual systems and vulnerabilities. The above mentioned OVAL definition 22272 has the following structure:

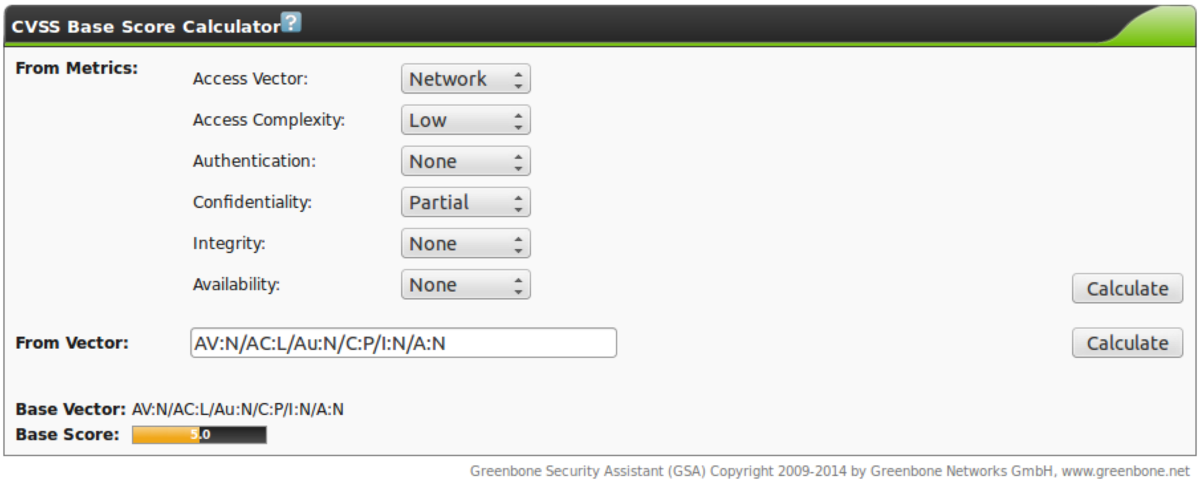
```xml
<definition id="oval:org.mitre.oval:def:22272" version="4" class="vulnerability">
  <metadata>
    <title>Vulnerability in Google Chrome before 32.0.1700.76 on Windows allows
           attackers to trigger a sync with an arbitrary Google account by
           leveraging improper handling of the closing of an untrusted signin
           confirm dialog</title>
    <affected family="windows">
      <platform>Microsoft Windows 2000</platform>
      <platform>Microsoft Windows XP</platform>
      <platform>Microsoft Windows Server 2003</platform>
      <platform>Microsoft Windows Server 2008</platform>
      <platform>Microsoft Windows Server 2008 R2</platform>
      <platform>Microsoft Windows Vista</platform>
      <platform>Microsoft Windows 7</platform>
      <platform>Microsoft Windows 8</platform>
      <platform>Microsoft Windows 8.1</platform>
      <platform>Microsoft Windows Server 2012</platform>
      <platform>Microsoft Windows Server 2012 R2</platform>
      <product>Google Chrome</product>
    </affected>
    <reference source="CVE" ref_id="CVE-2013-6643"
     ref_url="http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6643"/>
    <description>The OneClickSigninBubbleView::WindowClosing function in
      browser/ui/views/sync/one_click_signin_bubble_view.cc in Google
      Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac
      OS X and Linux allows attackers to trigger a sync with an arbitrary
      Google account by leveraging improper handling of the closing of an
      untrusted signin confirm dialog.</description>
    <oval_repository>
      <dates>
        <submitted date="2014-02-03T12:56:06">
          <contributor organization="ALTX-SOFT">Maria Kedovskaya</contributor>
        </submitted>
        <status_change date="2014-02-04T12:25:48.757-05:00">DRAFT</status_change>
        <status_change date="2014-02-24T04:03:01.652-05:00">INTERIM</status_change>
        <status_change date="2014-03-17T04:00:17.615-04:00">ACCEPTED</status_change>
      </dates>
      <status>ACCEPTED</status>
    </oval_repository>
  </metadata>
  <criteria>
    <extend_definition comment="Google Chrome is installed"
     definition_ref="oval:org.mitre.oval:def:11914"/>
    <criteria operator="AND" comment="Affected versions of Google Chrome">
      <criterion comment="Check if the version of Google Chrome is greater than
        or equals to  32.0.1651.2" test_ref="oval:org.mitre.oval:tst:100272"/>
      <criterion comment="Check if the version of Google Chrome is less than
        or equals to  32.0.1700.75" test_ref="oval:org.mitre.oval:tst:99783"/>
    </criteria>
  </criteria>
</definition>
```

This information are being processed graphically by the web interface and presented easily readable (see figure *OVAL describes the discovery of vulnerabilities.* (page 192)).

18.3.4 CVSS

A big problem for regular administrators is the interpretation of vulnerability with their own environment. How critical does he have to rate a vulnerability? To support personnel that do not work with the analysis and rating of vulnerabilities constantly the Common Vulnerability Scoring System (CVSS) was invented. CVSS is an industry standard for the description of the severity of security risks in computer systems. In the CVSS security risks are rated and compared using different criteria. This allows for the creation of a priority list of counter measures.

The CVSS score is continuously improved upon. Currently in general the CVSS score version 2 is being used. Version 3 is being developed by the CVSS Special Interest Group (CVSS-SIG) of the Forum of Incident Response and Security Teams[143] (FIRST).



CVSS Base Score Calculator

From Metrics:

Access Vector:	Network
Access Complexity:	Low
Authentication:	None
Confidentiality:	Partial
Integrity:	None
Availability:	None

From Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Base Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
Base Score: 5.0

Greenbone Security Assistant (GSA) Copyright 2009-2014 by Greenbone Networks GmbH, www.greenbone.net

Fig. 18.5: The CVSS calculator allows for the calculation of scores conveniently.

The CVSS score in version 2 supports Base Score Metrics, Temporal Score Metrics and Environmental Score Metrics.

The Base Score Metrics in general test the exploitability of a vulnerability and their impact on the target system. Hereby access, complexity and requirement of authentication are rated. At the same time they rate if the confidentiality, integrity or availability is threatened.

The Temporal Score Metrics test if completed example code exists, the vendor already supplied a patch and confirmed the vulnerability. The score will be changing drastically in the course of time.

The Environmental Score Metrics review if control damage has to be suspected, the target distribution, and if confidentiality, integrity of availability is required. This assessment is strongly depended on the environment in which the vulnerable product is being used.

Since the Base Score Metrics are merely meaningful in general and can be determined permanently the GSM provides them as part of the SecInfo data.

Hereby the following formula is being used and can be calculated with the CVSS calculator of the GSM as well (*Extras/CVSS-Calculator*, see figure *The CVSS calculator allows for the calculation of scores conveniently.* (page 194)).

$$BaseScore = roundTo1Decimal(((0.6 * Impact) + (0.4 * Exploitability) - 1.5) * f(Impact))$$

Hereby the impact is calculated as follows:

$$Impact = 10.41 * (1 - (1 - ConfImpact) * (1 - IntegImpact) * (1 - AvailImpact))$$

The exploitability is calculated as:

$$Exploitability = 20 * AccessVector * AccessComplexity * Authentication$$

The function $f(Impact)$ is 0, if the impact is 0. In all other cases the value is 1.176. The other values are constants:

- Access Vector
  - requires local access: 0.395

[143] https://www.first.org/cvss

  - adjacent network accessible: 0.646
  - network accessible: 1.0
- Access Complexity:
  - high: 0.35
  - medium: 0.61
  - low: 0.71
- Authentication
  - requires multiple instances of authentication: 0.45
  - requires single instance of authentication: 0.56
  - requires no authentication: 0.704
- ConfImpact:
  - none: 0.0
  - partial: 0.275
  - complete: 0.660
- IntegImpact
  - none: 0.0
  - partial: 0.275
  - complete: 0.660
- AvailImpact
  - none: 0.0
  - partial: 0.275
  - complete: 0.660

18.4 DFN-CERT

While the individual NVTs, CVEs, CPEs and OVAL definitions are being created primarily for processing by computer systems, the DFN-CERT publishes, like many other Computer Emergency Report Teams (CERTs), new advisories regularly. The DFN-CERT is responsible for hundreds of universities and research institutions that are associated with the German Research Network (German: Deutsches Forschungsnetz, abbreviated as DFN). An Advisory describes especially critical security risks that require fast reacting. These are being obtained by the GSM as well and stored to the database for reference. They can be displayed directly as well.

18.5 CERT-Bund

CERT-Bund offers a warning and information service (German: Warn- und Informationsdienst, abbreviated as WID). Currently this service offers two different types of Information (Excerpt from the website https://www.cert-bund.de/):

Advisories: This information service is only available to federal agencies as a closed list! The advisories describe current information about security critical incidents in computer systems and detailed measures to remediate security risks.

Short Information: Short information features the short description of current information regarding security risks and vulnerabilities. Please note that information sometimes is not verified and under some circumstances could be incomplete or even inaccurate.

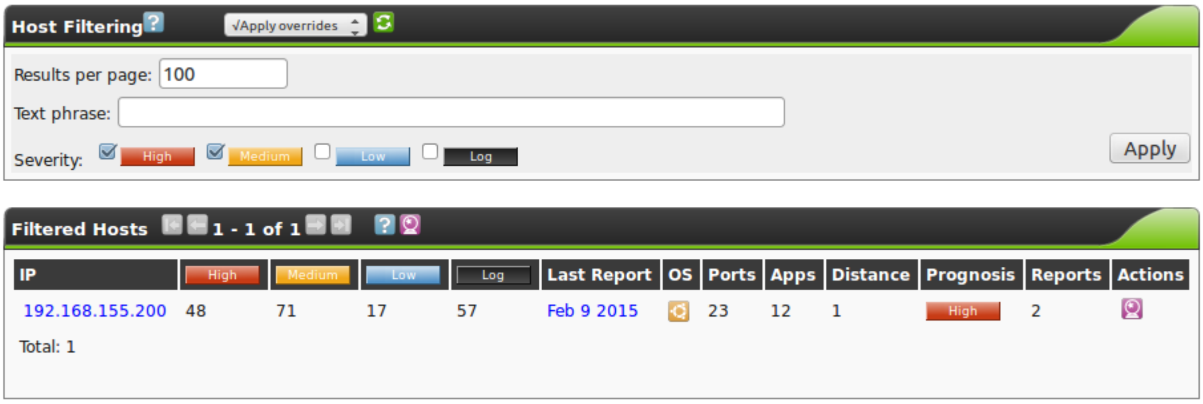
The Greenbone Security Feed contains the CERT-Bund Short Information. They can be identified by the K in the message (`CB-K14/1296`).

CHAPTER 19

Asset Management

The GSM can store all results of all scans in the Asset-Management. When defining a task it can be determined if the results of a scan should be recorded in the asset management (see section *Creating a Task* (page 59)).

To begin with, in the overview all the systems stored in the asset management can be viewed.



Host Filtering ? √Apply overrides

Results per page: 100

Text phrase:

Severity: ☑ High ☑ Medium □ Low □ Log

Apply

Filtered Hosts 1 - 1 of 1

IP	High	Medium	Low	Log	Last Report	OS	Ports	Apps	Distance	Prognosis	Reports	Actions
192.168.155.200	48	71	17	57	Feb 9 2015		23	12	1	High	2	

Total: 1

Fig. 19.1: The asset database displays the stored systems.

Here you can see how many security holes were discovered on the systems. In addition the overview displays the operating system with a logo (OS column) and the discovered ports and applications. Also it is being displayed how a scan of the system would possible turn out in this moment (Prognosis column, see also section *Prognosis* (page 198)). Via the a prognostic report can be created as well. Through the asset management you can always access the last report of the host. The date of the report is visible and can be accessed directly by clicking on the link. If multiple reports exist older reports can be accessed in the host details. By clicking on the host IP address the host details can be accessed. Here the amount of discovered vulnerabilities, the identified operating system, the discovered ports and the amount of detected applications on the system can be viewed

The host details contain additional information of the system:

Hardware: The GSM stores information about the hardware. If known then the MAC address is listed here. It can only be displayed though if the target system is on the same LAN as the GSM.

Detected Applications: Especially of interest are the detected applications. With this the Greenbone Security Manager can give a prognosis based on its SecInfo database without re-scanning if additional security risks would be found. This is especially of interest for systems that currently do not have any vulnerability and new scans are not being performed regularly.

19.1 Prognosis

The prognosis allows to forecast possible security risks without a new scan based on current information about known security holes from the *SecInfo Management* (SCAP, Security Content Automation Protocol) (see chapter SecInfo Management (page 187)). This is especially interesting for environments where by the use of the GSM most vulnerabilities have been removed or remediated. Of course new vulnerabilities are being discovered daily. Not every vulnerability justifies a new scan of the network or of individual systems. Due to the fact that the GSM has this information, based on the knowledge of the detected applications it can make a prognosis which security risks exist. If security risks become known it justifies the actual running of a scan to verify the prognosis. For this the asset database requires current data of course. This is why a scan of the systems should occur regularly in weekly or monthly intervals.

A prognostic scan can be performed as well. It will determine probable existing vulnerabilities

CHAPTER 20

Performance

When operating the Greenbone Security Manager a considerable amount of data can be transmitted by the target systems. The available scan results are also being analyzed, filtered and processed by the GSM. On larger GSM models this occurs generally at the same time and by many users and processes.

This chapter covers the diverse questions regarding performance and discusses optimization options.

20.1 Scan Performance

The speed of a scan depends on many parameters This section points out the most important settings and makes some recommendations.

20.1.1 Selecting a Port List for a Scan

Which port list being configured for a target and as such for the tasks and the scans has a big impact, for one on the discovery performance and on the other hand regarding the scan duration.

One needs to weigh up between those two aspects when planning the vulnerability testing.

About Ports

Ports are the connection points of network communication whereby each port of the one system connects with the port port on another system.

Every system has 65535 TCP ports and 65535 UDP ports. To be precise there is one more namely the special port 0. In a connection between two ports data transmission occurs in both directions for UDP only in one direction. Due to the fact that data received by UDP are not necessarily confirmed, the testing of UDP ports usually takes longer.

Ports 0 to 1023 need to be highlighted as so called privileged or system ports and usually can not be opened by user applications.

At the IANA (Internet Assigned Numbers Authority) standard protocol ports can be reserved that then are assigned a protocol name like port 80 for `http` or port 443 for `https`.

At IANA over 5000 ports are registered. However it is absolutely possible for software to use one of these ports for different purposes if the port is not being used on the respective system.

From analysis, in which all ports of all systems of all internet accessible systems were analyzed, lists of the most used ports were created. Those do not necessarily reflect the IANA list because there is no obligation to register a specific service type for a respective port.

Typically desktop systems have fewer ports open than servers. Active network components such as routers, printers and IP phones in general have only very few ports open, namely only those they require for their actual task and for their maintenance.

Which Port List for which Scan Task

The choice of the port list always needs to be weighed up between discovery performance and scan duration.

The duration of a scan is mostly determined by the amount of ports to be tested and the network configuration. For example, starting with a certain amount of ports to be tested, throttling by the network elements or the tested systems could occur.

For the discovery performance it is obvious that services that are not bound to ports on the list, are not being tested for vulnerabilities. Additionally malicious applications that are bound to such ports won't be discovered of course. The malicious application mostly open ports that are usually not being used and are far form the system ports.

Other criteria are the defence mechanisms that are being activated by often exhaustive port scans and initiate counter measures or alerts. Even with normal scans firewalls can simulate that all 65535 ports are active and as such slow down the actual scan of those ports that are being scanned for nothing, with so called time outs.

Also to remember that for every port that is being queried the service behind it reacts at least with one log entry. For organizational reasons some services possibly should be scanned or at at least at a specific time only.

The following table outlines which port list could be most meaningful for which task.

Task/Problem	Port List
Initial Suspicion, Penetration Test, High Security, First scan of unknown systems in limited numbers	• All TCP and All UDP
Background test of an environment with known or defined environment (servers) in large numbers or with high frequency	• Specific List of Known Services • All IANA TCP
First scan of unknown systems in large numbers or with high frequency	• All IANA TCP • Nmap Top 1000 TCP and Top 100 UDP

The final decision needs to be made by the person(s) responsible for the scans. There should be at least documentation of the targets or problem to justify the selection of the ports.

On the one hand one can *play it safe*, meaning always scan all ports, will not achieve the desired outcome because all systems simply can not be scanned in time or because it will interrupt business operations.

On the other hand *super fast*, meaning only scan all privileged ports, will seem inadequate for unknown systems with high security requirements if during a later incident a vulnerability is being discovered that was rather easy to be identified. Examples for this are database services.

Also to be remembered, some systems do not use a static port allocation rather than constantly changing them even during operation. This, of course, makes it more difficult for a specific port list.

Scan Duration

In some situations with port throttling scanning all TCP and UDP ports can take 24 hours or more for a single system. Since the scans are being performed in parallel two systems will of course only take marginally more time than a single system. However the parallelizing has its limits due to system resources or network performance.

However all IANA TCP ports do usually take no more than a couple of minutes.

Since some counter measures can increase the duration of a scan there is the option to prevent throttling by making configuration changes on the defense system.

All in all at the end one will learn over time network ranges to be scanned and how they will react to scans and routine tasks can be optimized in that regard.

In suspected cases of a compromise or highest security breaches a fully inclusive scan is unavoidable.

Total Security

For port scans the basic principle that no total security exists is also true. This means that even when `All TCP and All UDP` are being used the pre set timeout of the port testing can be too short to coax a hidden malicious application into a response.

Or especially with a large amount of ports it comes directly down to defense through infrastructure. Less could sometimes even mean more.

If an initial suspicion exists an experienced penetration tester who combines the use of the actual scan tools with experience and professionally related intuition and has a good command of detailed parameterization should be consulted.

20.1.2 Scan Configuration

The scan configuration has an impact on the scan duration as well. The GSM offers four different scan configurations for vulnerability scans:

- Full and fast
- Full and fast ultimate
- Full and very deep
- Full and very deep ultimate

Both the `Full and fast` and `Full and fast ultimate` scan configurations optimize their process using already found information. This allows for the optimization of many NVTs and in doubt do not need to be tested. The two other scan configurations ignore already discovered information and therefore will execute all NVTs. This includes those NVTs as well that are not useful based on previously discovered information.

20.1.3 Tasks

During the progress of a scan a progress bar is being created. This progress bar should reflect the progress of the scan in percent. In most cases this is a rough estimate since it is difficult for the GSM to project how the systems or services that haven't been scanned yet behave compared to the already scanned systems and services.

This can be understood best when looking at an example. Assumed is a network 162.168.0.0/24 with 5 hosts: 192.168.0.250-254. A scan is being configured for this network. The scan will be performed in sequence. Due to the fact that the IP addresses at the beginning of the network are not being used the scan will run very quickly and reaches 95%. Then however, systems are being discovered that use many services. The scan will slow down respectively and since all these services are being tested. The progress bar only jumps very little. To adjust for this behaviour in the scanner dialog the `Order for target hosts` can be adjusted. The setting `Random` makes sense.

20.2 Backend Performance

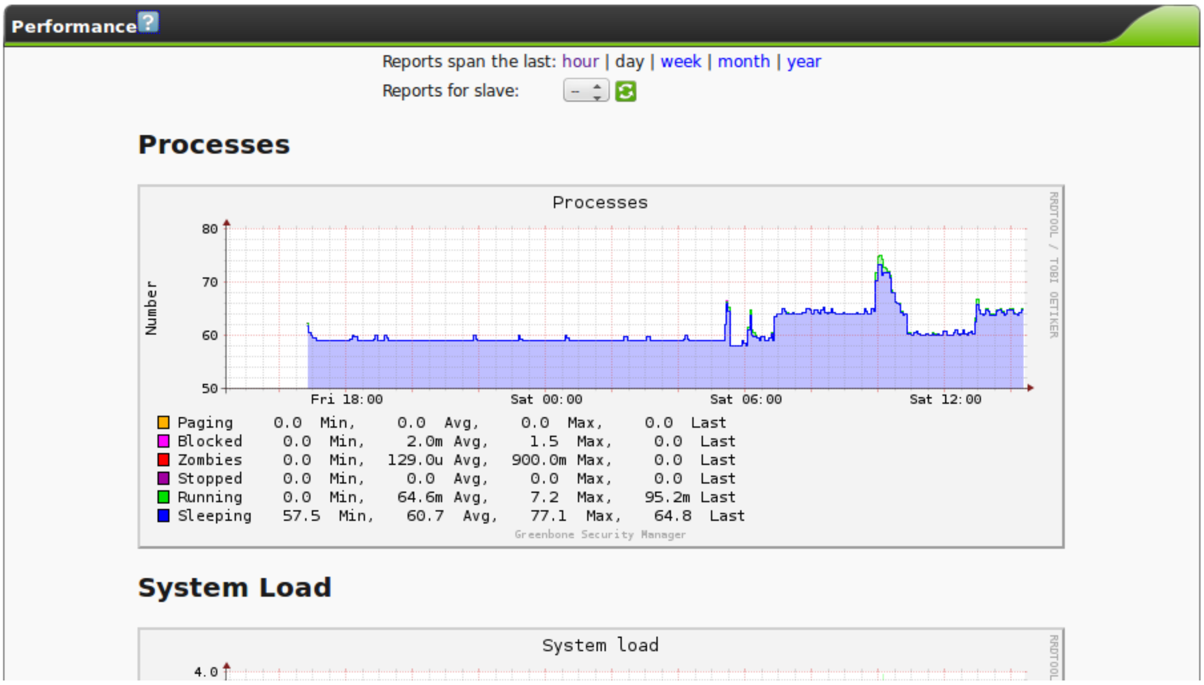
The web interface accesses the GSM utilizing the OMP protocol. Some operations require more time than others. To allow an analysis and examination of the speed of the OMP backend every web page displays the time required to prepare the data at the bottom of the web page.

Backend operation: 0.14s

Fig. 20.1: The processing times of the backend are being displayed.

20.3 Appliance Performance

The overall performance of the GSM can be monitored with the integrated monitoring. Under *Extras* the GSM provides its own *Performance* monitoring. Here the resource utilization of the GSM for the last hour, day, week, month and year can be displayed.



```
Paging     0.0  Min,     0.0  Avg,     0.0  Max,     0.0  Last
Blocked     0.0  Min,     2.0m Avg,     1.5  Max,     0.0  Last
Zombies     0.0  Min,  129.0u Avg,  900.0m Max,     0.0  Last
Stopped     0.0  Min,     0.0  Avg,     0.0  Max,     0.0  Last
Running     0.0  Min,    64.6m Avg,     7.2  Max,    95.2m Last
Sleeping   57.5  Min,    60.7  Avg,    77.1  Max,    64.8  Last
```

Fig. 20.2: The processing times of the backend are being displayed.

Here the following points are important:

Processes A high amount of processes is not critical. However, primarily only sleeping and running processes should be displayed.

System Load An ongoing high utilization is critical. Hereby a load of 4 on a system with 4 cores is considered ok.

CPU Usage Here especially a high Wait-IO is critical.

Memory Usage The GSM uses aggressive caching. The usage of most of the memory as cache is okay.

Swap A use of the Swap memory points to a potential system overload.

Master and Slave Setup

The Greenbone Security Manager allows for the building of a distributed scan system. Hereby it is possible that one GSM remotely controls another GSM for this purpose.

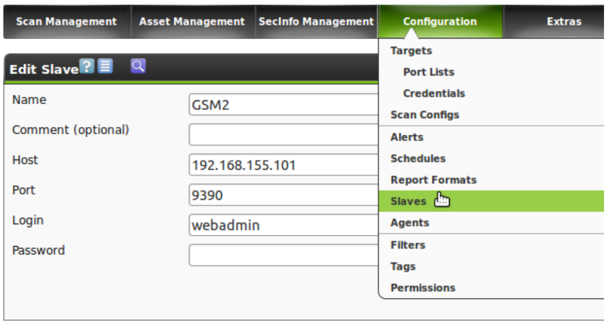
Thereby the controlling GSM is called master and the controlled GSM slave. As soon as two GSMs are configured as master and slave a user can individually configure a scan for the scan slave via the web interface of the scan master depending on requirements and permissions. Every GSM starting from the midrange models upwards can be used as scan master and control one or more slaves. Every GSM can function as a slave.

The scan slaves are independent GSMs. This is why the administrator must configure the feed updates and release updates locally on the slaves as well and ensure their execution. A scan slave also provides their own graphical interface and own management. This allows for it being able to be used completely independently, however some scans being executed from the master.

Additionally the slave can be configured as sensor. A scan sensor is a GSM that exclusively is being used for the function of scan slave and also completely being managed by the assigned master. This management includes automatic updates of the feeds as well as the automatic updates of release updates. A sensor does not require any network connectivity other than to a sensor master and after initial setup no further administrative tasks.

Scan sensors and slaves can be integrated into a scan master, in order to test those network segments for vulnerabilities that are not accessible in any other way.

Basically the master establishes the connection to the delegated scan slaves. The connection is established by using the OpenVAS management protocol (OMP) which uses TCP port 9390. Additionally for feed and release updates on a scan sensor port 22/tcp (ssh) is required.



Edit Slave

Name	GSM2
Comment (optional)	
Host	192.168.155.101
Port	9390
Login	webadmin
Password	

Fig. 21.1: Selecting a task on the slave.

21.1 Connecting a Slave

Like with any other GSM the basic setup of a scan slave is being performed via the serial port. In addition to the network configuration and the administrative access two other basic parameters for the use as slave are required:

- Configuring of a scan administrator on the slave that allows the master to control the slave. It is being enabled on the slave in the GOS-Admin-Menu under *User* and then *Add Web Admin*.
- Activation of the remote OMP features. This can be enabled in the GOS-Admin-Menu under *Remote* and *OMP*. Alternatively it can enabled directly on the command line with the variable `public_omp`:

```
    set public_omp enabled
```

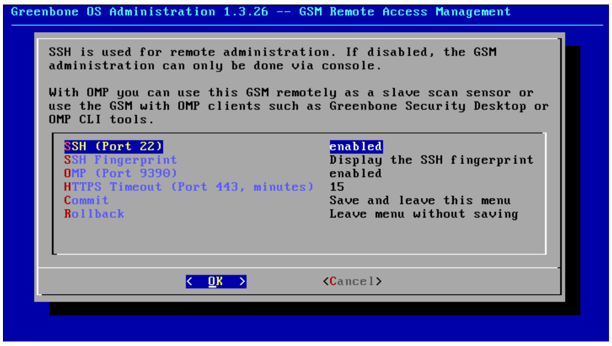
Please note: Activating the remote OMP features requires a reboot of the scan slaves.

Afterwards the slaves can be set up on the master and a task delegated to the slave.

21.2 Sensor

For security reasons often it is not possible to scan network segments directly. Most of the time direct access of this segment to the Internet is not desired. In order for a sensor to have the latest NVTs available, in these cases it possible to transfer the Greenbone Security Feed from the master to the slave and as such allow for a feed synchronization with the sensor. After set up this occurs automatically. As soon as the master synchronized itself with the feed server it will transfer the information to the sensor as well.

To achieve this the master uses the SSH protocol. The following steps allow the master to log into the senor without the use of a password for the transfer of the information.



```
Greenbone OS Administration 1.3.26 -- GSM Remote Access Management

SSH is used for remote administration. If disabled, the GSM
administration can only be done via console.

With OMP you can use this GSM remotely as a slave scan sensor or
use the GSM with OMP clients such as Greenbone Security Desktop or
OMP CLI tools.

SSH (Port 22)                          enabled
SSH Fingerprint                        Display the SSH fingerprint
OMP (Port 9390)                        enabled
HTTPS Timeout (Port 443, minutes)      15
Commit                                 Save and leave this menu
Rollback                               Leave menu without saving
```

Fig. 21.2: Activating SSH access.

First the public key of the master (Masterkey) must be copied to the sensor. Then the master can automatically establish a SSH connection with the sensor.

For this display the key on the master. Use the command `show masterkey`. Copy the key that is being displayed to the clipboard:

```
gsm-master> show masterkey
ssh-dss AAAAB3 .... root@gsm
```

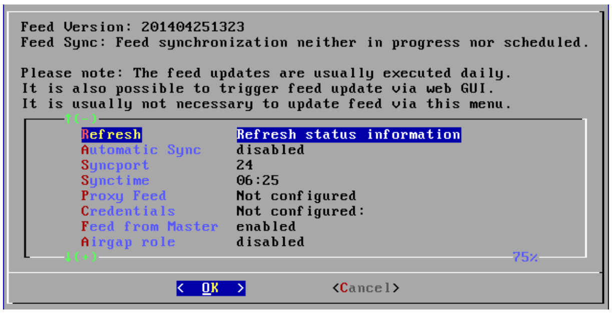
Afterwards connect to the sensor and enter the command `masterkeydownload` on the command line. Then copy the key from the clipboard onto the command line and close the entry with `CTRL-D`:

```
gsm-sensor> masterkeydownload
Please paste the master key into the CLI , END with CTRL -D
ssh-dss AAAAB3 .... root@gsm
```

```
gsm-sensor> show sensormasterkey
ssh-dss AAAAB3 .... root@gsm
```

Subsequently it is recommended to verify the especially when using a USB/Serial adapter. On older GOS versions (< 3.0.20) the last command is called show masterkey. Many such adapters transfer individual characters inaccurately.

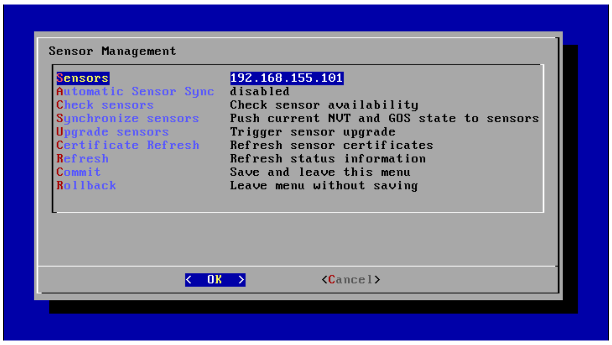
Additionally the administrator must activate the SSH access on the sensor. This can be done with the variable `ssh` or via the GOS-Admin-Menu.



```
Feed Version: 201404251323
Feed Sync: Feed synchronization neither in progress nor scheduled.

Please note: The feed updates are usually executed daily.
It is also possible to trigger feed update via web GUI.
It is usually not necessary to update feed via this menu.

Refresh            Refresh status information
Automatic Sync     disabled
Syncport           24
Synctime           06:25
Proxy Feed         Not configured
Credentials        Not configured:
Feed from Master   enabled
Airgap role        disabled
                                                  75%
```

Fig. 21.3: The feed of the sensor is being transferred from the master.

So that the sensor is not trying to access the feed directly this function must be deactivated. The administrator can find this setting in the GOS-Admin-Menu in *Feed* under *Automatic Sync*. Additionally the administrator must activate the feed synchronization through the master (*Feed from Master*). Finally the settings must be confirmed with a *Commit*.



```
Sensor Management

Sensors                 192.168.155.101
Automatic Sensor Sync   disabled
Check sensors           Check sensor availability
Synchronize sensors     Push current NVT and GOS state to sensors
Upgrade sensors         Trigger sensor upgrade
Certificate Refresh     Refresh sensor certificates
Refresh                 Refresh status information
Commit                  Save and leave this menu
Rollback                Leave menu without saving
```

Fig. 21.4: Entering the sensors on the master.

Since the master establishes the connection to the sensors the sensors must be included into the management of the master. This option can be found on the master in the GOS-Admin-Menu under *Sensors*. Here activate the option *Automatic Sensor Sync*. Afterwards add the IP address of the sensor to the sensor list (*Sensors*). This is a list of IP addresses that are separated by spaces.

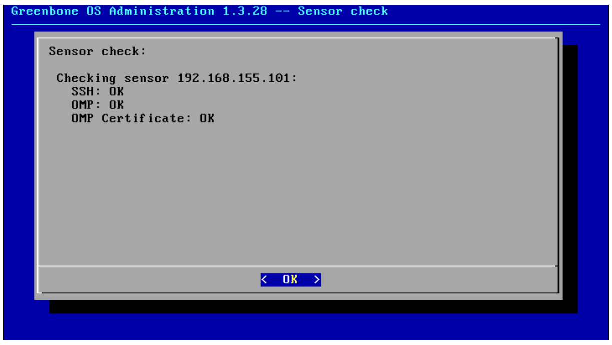
With a sensor check the reachability of sensors can be tested.

21.2.1 Manual Synchronization

Using the GOS-Admin-Menu a manual synchronization of the NVT the the GOS-state is possible. This manual step is only needed if the automatic synchronization is not enabled. Both the feed and the GOS-updates are then synchronized to the sensors. The GOS-updates are just synchronized but not installed by default.

Use *Sensors/Synchronize sensors* to trigger the synchronization.

While the synchronization is in progress the menu options *Synchronize sensors* and *Upgrade sensors* are not available.



Greenbone OS Administration 1.3.28 -- Sensor check

```
Sensor check:

 Checking sensor 192.168.155.101:
   SSH: OK
   OMP: OK
   OMP Certificate: OK
```

Fig. 21.5: With the sensor check the GSM tests the reachability.

21.2.2 Upgrade Sensors

Once the manual synchronization has finished the sensors may be upgraded. This is triggered via *Sensors/Upgrade sensors*.

21.2.3 Communicating with the Sensors

The slaves/sensors communicate using two protocols: OMP (slaves and sensors) and SSH (sensor only). These protocols must be allowed through possible existing firewall systems. Hereby the master always establishes the connection to the slave/sensor.

The feed update of the delegated scan sensors is being performed selectively either directly from the Greenbone Update Servers or through the master. For updates from the master to the scan sensor SSH (TCP per 22) is being used. If this option is not being used it has to be remembered that a possible firewall situated between the master and the scan sensor blocks this connection without notification (*Drop* or *Deny* setting). Instead the establishing of the connection should be allowed (*Accept* or *Permit*) or rejected (*Reject*) with notification as the master will always try to transfer the feed updates to the scan sensor.

CHAPTER 22

Integration with other Systems

The Greenbone GSM appliance can be connected to other systems. This chapter covers the possible options. Some systems have been integrated already into the GSM by Greenbone Networks. This includes the verinice ITSM system, the Sourcefire IPS Defense Center and the Nagios Monitoring System. A couple of further integrations such as Palo Alto, are described in chapter Scanners (page 153). The following sections will instruct in these possibilities and give instructions for the configuration.

22.1 Integration with third-party vendors

The GSM has numerous interfaces that allow for the communication with third-party vendors. This section covers the options for an integration and connection with other systems.

Hereby the GSM offers the following interfaces:

OpenVAS Management Protocol (OMP) The OpenVAS Management Protocol allows to completely remote control the GSM appliance. The protocol supports the creating of users, creating and starting of scan tasks and downloading reports, and so on.

Connecting additional scanners via OSP The OpenVAS Scanner Protocol (OSP) is a standardized interface for different vulnerability scanners. Arbitrary scanners can be integrated seamless into the GSM vulnerability management. Controlling the scanners and handling the results works in the same way for all scanners.

Report Format The GSM can present the scan results in any format. To do so the GSM already comes with a multitude of pre-installed report formats. Additional report formats can be downloaded from Greenbone or developed in collaboration with Greenbone.

Alert via Syslog, E-Mail, SNMP-Trap or HTTP.

Automatic result forwarding through connectors. These connectors are being created by Greenbone, verified and integrated into the GSM.

Monitoring via SNMP On the web site http://docs.greenbone.net/API/SNMP/snmp-gos-3.1.en.html provides the current MIB file (Management Information Base). MIB files describe the files that can be queried by SNMP about the equipment.

22.1.1 OSP Scanner

The OpenVAS Scanner Protocol resembles the OpenVAS Management Protocol (OMP, see chapter OpenVAS Management Protocol (page 179)). It is XML based, stateless and does not require a permanent connection for communication. The design allows for embedding of additional scanners seemlessly into GSM.

The GSM comes with a number of OSP scanners on board, see chapter Scanners (page 153).

The open format allows to develop arbitrary own OSP scanners. Greenbone provides the protocol documentation and a base framework for programmers, see chapter OpenVAS Scanner Protocol (page 223).

22.2 Verinice

Verinice (see http://verinice.org/en/) is a free OpenSource Information Security Management System (ISMS), developed by the company SerNet (see http://sernet.de/en/).

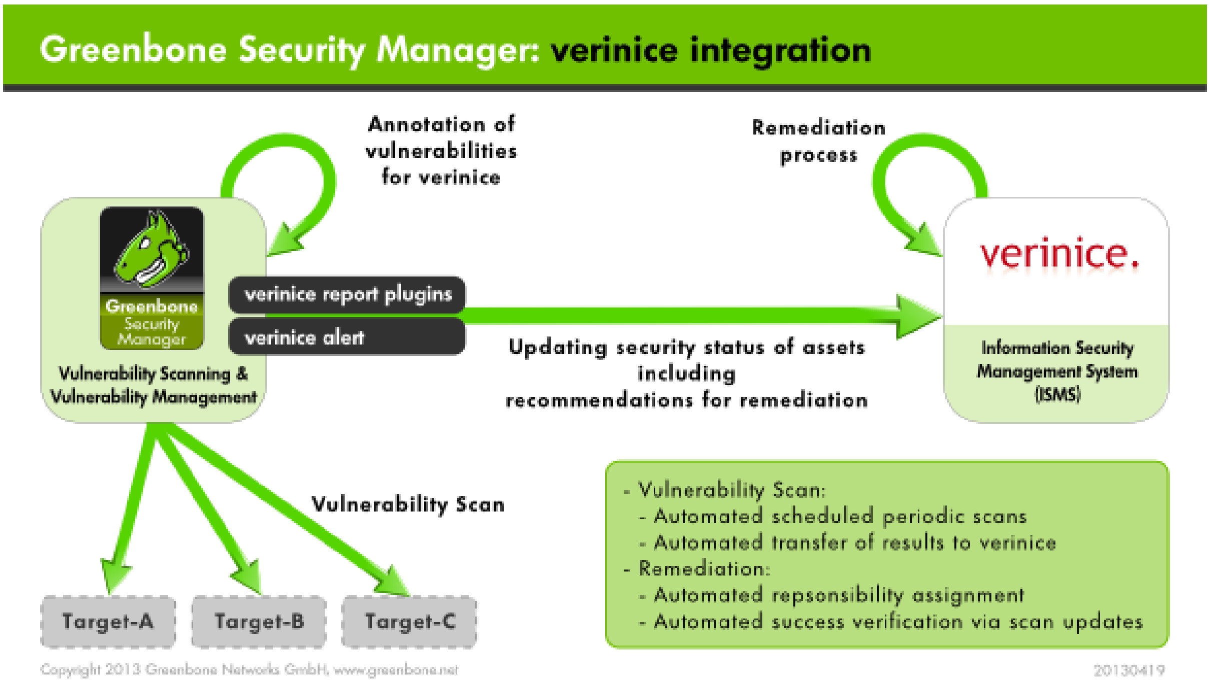

Greenbone Security Manager: verinice integration
Annotation of vulnerabilities for verinice
Remediation process
Greenbone Security Manager
verinice report plugins
verinice alert
Vulnerability Scanning & Vulnerability Management
verinice.
Information Security Management System (ISMS)
Updating security status of assets including recommendations for remediation
Vulnerability Scan
Target-A
Target-B
Target-C
- Vulnerability Scan:
- Automated scheduled periodic scans
- Automated transfer of results to verinice
- Remediation:
- Automated repsonsibility assignment
- Automated success verification via scan updates
Copyright 2013 Greenbone Networks GmbH, www.greenbone.net
20130419

Fig. 22.1: The GSM may be integrated with verinice.

Verinice is suitable for:

- vulnerability remediation workflow
- implementing the BSI IT-Baseline Protection Catalogues
- performing risk analysis based on ISO 27005
- operating an ISMS based on ISO 27001
- performing an IS assessment per VDA specifications
- proof of Compliance with standards such as ISO 27002, IDW PS 330

The Greenbone Security Manager can support the modelling and implementation of IT Baseline Protection as well as the operation of an ISMS.

For this Greenbone offers two report plugins for the export of data from the GSM into verinice:

- `Verinice-ISM` containing all scan results
- `Verinice-ITG` containing the scan results of a BSI IT-Baseline Protection scan

The option exists to transfer data completely automated from the Greenbone Security Manager to verinicePRO, the server extension of verinice.

Following the manual import of reports from the GSM in the free verinice version is covered. For support with the use of the connector please contact SerNET or Greenbone.

22.2.1 IT Security Management

The report plugin for verinice is pre-configured and is available as `Verinice-ISM`.

With this report plugin Greenbone supports the vulnerability remediation workflow in verinice.

Hereby the notes (notes objects, see section *Notes* (page 78)) of the scan results play a central role for the `Verinice-ISM` plugin. Verinice uses the notes to create objects for processing. If there are no notes in a task only the assets will be imported as well as the complete vulnerability report. Exclusively such vulnerabilities that have a note will be imported by verinice as vulnerabilities. This allows controlling the import in fine detail.

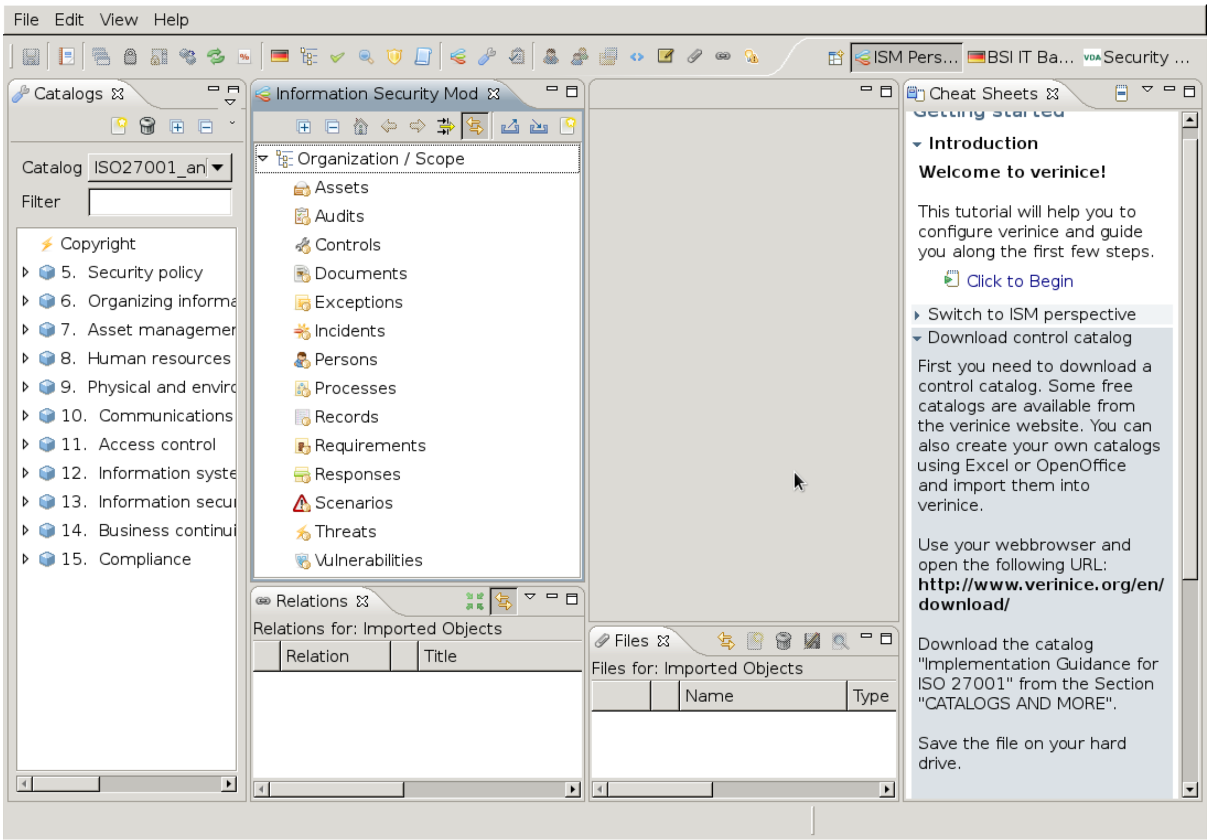
Note: Why are only vulnerabilities transferred where a note is attached?

Within the entire security process for vulnerabilities, there must be a single point where the decision is made which vulnerability must be resolved and which are tolerable. This decision is made in the vulnerability management, by tagging the vulnerabilities accordingly.

The remediation workflow targets at solving any of the managed issues. Within the remediation workflow it is not allowed to decide about tolerating an issue.

Afterwards the report needs to be saved as `Verinice ISM-Report`. A `.vna` file will be created. This is a zip file containing the data of the GSM scan.

Start verinice to import. In verinice open the ISM perspective. Import the catalogue `Implementation Assistance for ISO27001`. Create an organization. Afterwards the screen should look like figure *Verinice offers an ISM perspective.* (page 209).



Welcome to verinice!

This tutorial will help you to configure verinice and guide you along the first few steps.

First you need to download a control catalog. Some free catalogs are available from the verinice website. You can also create your own catalogs using Excel or OpenOffice and import them into verinice.

Use your webbrowser and open the following URL: **http://www.verinice.org/en/download/**

Download the catalog "Implementation Guidance for ISO 27001" from the Section "CATALOGS AND MORE".

Save the file on your hard drive.

Fig. 22.2: Verinice offers an ISM perspective.

Importing of the ISM Scan

In the verinice interface chose the import option in the Information Security Model.

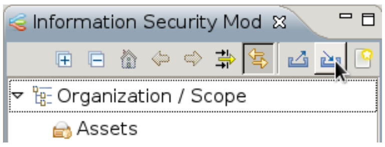
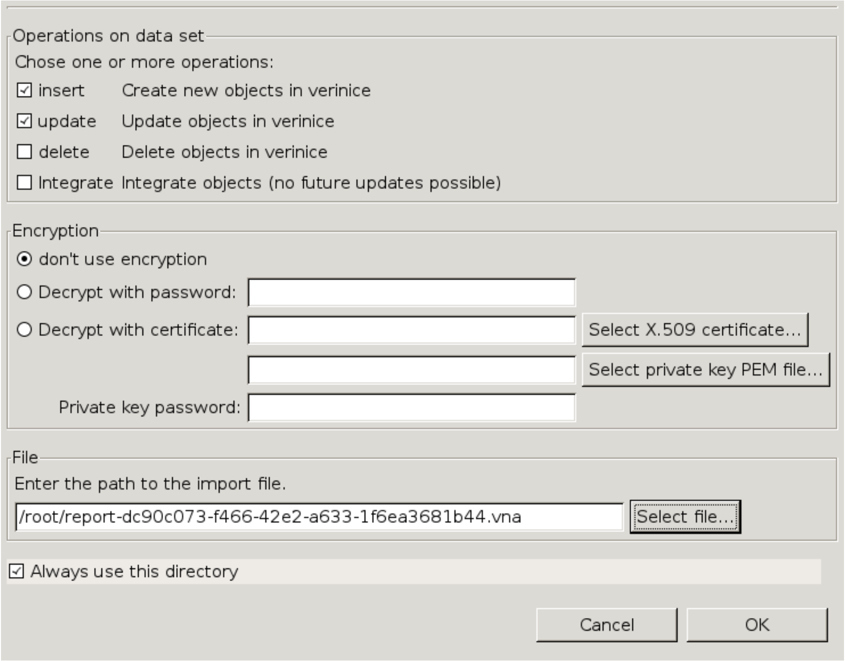


Fig. 22.3: The import button is located in the Information Security Model window.

Now select your ISM report. The remaining parameters can be kept with their default settings.



Operations on data set

Chose one or more operations:

☑ insert Create new objects in verinice

☑ update Update objects in verinice

□ delete Delete objects in verinice

□ Integrate Integrate objects (no future updates possible)

Encryption

● don't use encryption

○ Decrypt with password:

○ Decrypt with certificate: Select X.509 certificate...

Select private key PEM file...

Private key password:

File

Enter the path to the import file.

/root/report-dc90c073-f466-42e2-a633-1f6ea3681b44.vna Select file...

☑ Always use this directory

Cancel OK

Fig. 22.4: Select the report in the dialog.

The results of the ISM report were imported and can be unfolded in Vernice. Thereby only the results were imported that had notes included in the GSM report.

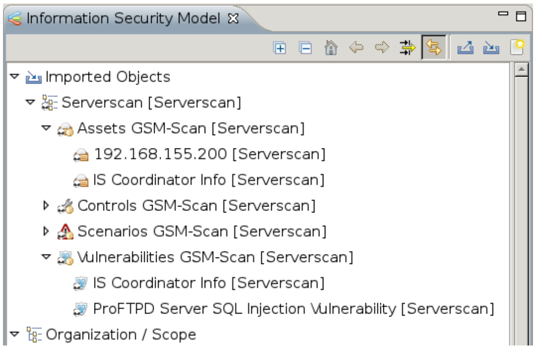
The process to track vulnerabilities for the imported organization can be separated into two sub processes:

- Creation of tasks
- Remediation of vulnerabilities

Creation of Tasks

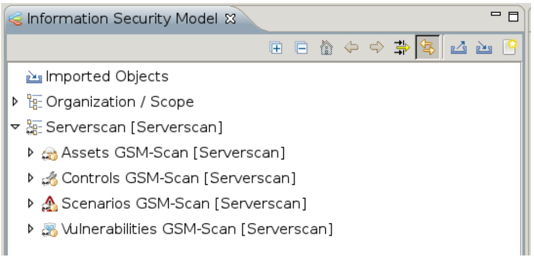
Before creating tasks the data for the organization must be prepared with the following steps:

- After the first import of an organization it must be moved to the top level from the group of imported objects. Cut the organization and paste it back into the top level again.
- The assets and controls must be grouped. In the context menu in the top most asset and control group select the option `Group with Tags...` In figure *The assets have already been grouped.* (page 211) this has already been done.



- Imported Objects
  - Serverscan [Serverscan]
    - Assets GSM-Scan [Serverscan]
      - 192.168.155.200 [Serverscan]
      - IS Coordinator Info [Serverscan]
    - Controls GSM-Scan [Serverscan]
    - Scenarios GSM-Scan [Serverscan]
    - Vulnerabilities GSM-Scan [Serverscan]
      - IS Coordinator Info [Serverscan]
      - ProFTPD Server SQL Injection Vulnerability [Serverscan]
- Organization / Scope

Fig. 22.5: Through the creation of notes the import of vulnerabilities can be controlled.



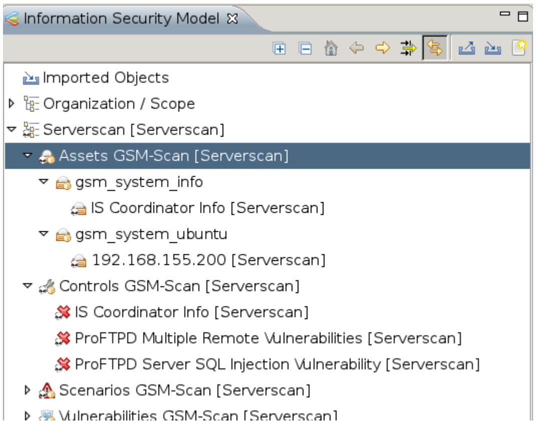
- Imported Objects
- Organization / Scope
- Serverscan [Serverscan]
  - Assets GSM-Scan [Serverscan]
  - Controls GSM-Scan [Serverscan]
  - Scenarios GSM-Scan [Serverscan]
  - Vulnerabilities GSM-Scan [Serverscan]

Fig. 22.6: The imported organization must be moved to the top level.

- All assets groups must be assigned a person responsible. Assign a person to one or more asset groups. Hereby create the person and assign them with drag&drop. The successful assignment is being displayed in the `Relations` window.
- After all the asset groups have been assigned to a person responsible, the process to remediate the vulnerabilities can be started from the context menu of the organization. Select from the context menu of an organization the task `Greenbone: Start Vulnerability Tracking`. First it will be verified if all asset groups are assigned to a person and controls are grouped. The result of the verification will be displayed in a dialog. The user can continue and create tasks or cancel the creation.

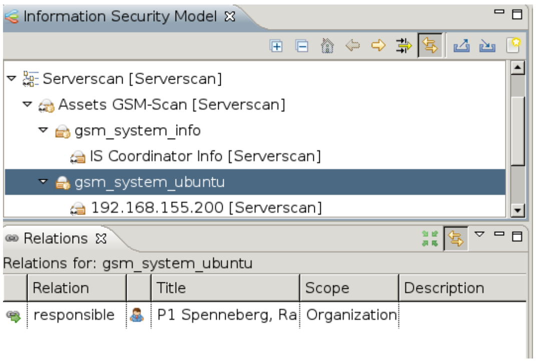
Remediation of Vulnerabilities

The created tasks can be managed with the help of the task view or the web fronted of the verinice.Pro version (under: ISO 27000 tasks). The task to remediate vulnerabilities is called Remediate Vulnerabilities. A task contains controls, scenarios and assets that are connected to a control group and are



- Imported Objects
- Organization / Scope
- Serverscan [Serverscan]
  - Assets GSM-Scan [Serverscan]
    - gsm_system_info
      - IS Coordinator Info [Serverscan]
    - gsm_system_ubuntu
      - 192.168.155.200 [Serverscan]
  - Controls GSM-Scan [Serverscan]
    - IS Coordinator Info [Serverscan]
    - ProFTPD Multiple Remote Vulnerabilities [Serverscan]
    - ProFTPD Server SQL Injection Vulnerability [Serverscan]
  - Scenarios GSM-Scan [Serverscan]
  - Vulnerabilities GSM-Scan [Serverscan]

Fig. 22.7: The assets have already been grouped.



- Serverscan [Serverscan]
  - Assets GSM-Scan [Serverscan]
    - gsm_system_info
      - IS Coordinator Info [Serverscan]
    - gsm_system_ubuntu
      - 192.168.155.200 [Serverscan]

Relations for: gsm_system_ubuntu

Relation	Title	Scope	Description
responsible	P1 Spenneberg, Ra	Organization	

Fig. 22.8: The connection of individual objects can be confirmed in the in the Relations window.

assigned to a person responsible.

This process now takes place with the following steps:

- The person responsible must remediate the vulnerabilities for all assets.
- If the deadline for the task Remediate Vulnerabilities expires a reminder email will be sent to the person responsible.
- After completion of a task called Remediate Vulnerabilities all connection between assets and scenarios that were assigned to a task are being deleted.
- A control is marked as implemented if no asset is assigned to the scenario anymore. If other connections to assets still exist the status is being marked as partly. Afterwards the process is being completed.

22.2.2 IT Security Baseline

Greenbone provides a special configuration (IT Security Baseline scan including discovery for verinice) as well as an IT Security Baseline report plugin (Verinice ITG), which allows for the export of a report suited for verinice.

For optimum results the scan configuration needs to be imported. The report plugin is now shipped with the GSM. A manual import is not required anymore.

For optimum results in the scan it is helpful to perform an authenticated scan (see section *Authenticated Scan* (page 67)).

As soon as the scan is completed export it in the verinice ITG format. A file with the extension `.vna` is being created. This is a ZIP archive in which the results of the scans are stored. This file can be loaded by verinice directly.

Following for clarity purposes a scan is being used with only one host.

Open verinice and change into the IT Security Baseline start perspective (see figure *Verinice opens the already modelled IT bond.* (page 213)). If no IT bond has been created yet the middle view will still be empty.

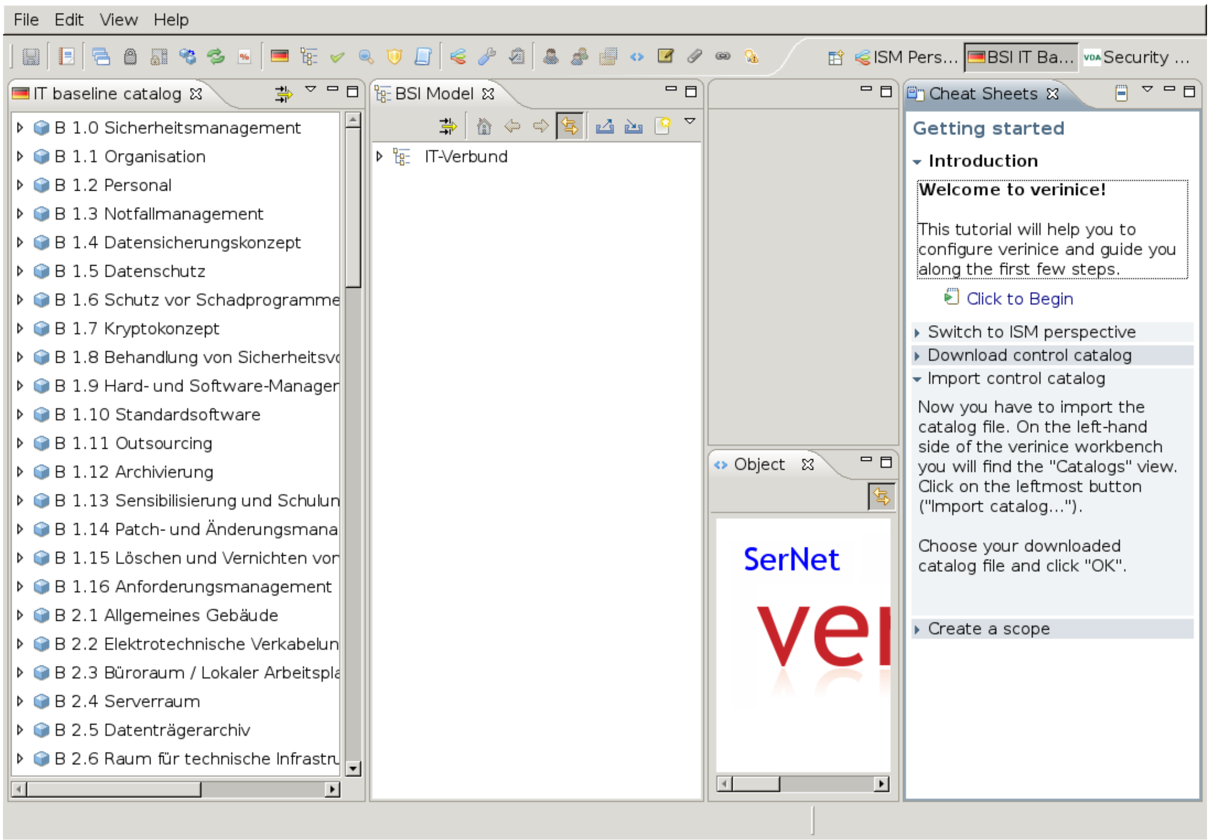
Importing of the ITG Scan

In the verinice interface select the import function in the IT Security Baseline model.

Now select the ITG report. The remaining parameters can be kept with their default settings.

The results of the ISM report were imported and can be unfolded in Vernice.

The imported objects are named by the target in the GSM or their IP address. Every imported object has a sub-object GSM result with the activity results of the scan.



B 1.0 Sicherheitsmanagement
B 1.1 Organisation
B 1.2 Personal
B 1.3 Notfallmanagement
B 1.4 Datensicherungskonzept
B 1.5 Datenschutz
B 1.6 Schutz vor Schadprogramme
B 1.7 Kryptokonzept
B 1.8 Behandlung von Sicherheitsv
B 1.9 Hard- und Software-Manager
B 1.10 Standardsoftware
B 1.11 Outsourcing
B 1.12 Archivierung
B 1.13 Sensibilisierung und Schulun
B 1.14 Patch- und Änderungsmana
B 1.15 Löschen und Vernichten vor
B 1.16 Anforderungsmanagement
B 2.1 Allgemeines Gebäude
B 2.2 Elektrotechnische Verkabelun
B 2.3 Büroraum / Lokaler Arbeitspla
B 2.4 Serverraum
B 2.5 Datenträgerarchiv
B 2.6 Raum für technische Infrastru

Getting started

Introduction

Welcome to verinice!

This tutorial will help you to configure verinice and guide you along the first few steps.

Click to Begin

Switch to ISM perspective

Download control catalog

Import control catalog

Now you have to import the catalog file. On the left-hand side of the verinice workbench you will find the "Catalogs" view. Click on the leftmost button ("Import catalog…").

Choose your downloaded catalog file and click "OK".

Create a scope

Fig. 22.9: Verinice opens the already modelled IT bond.

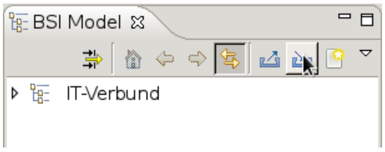


Fig. 22.10: The Import button is located in the BSI model window.

Now the IT Security Baseline modules can be added. For this select a server by right clicking on it. In the context menu select `Greenbone: Automatically assign components`. Verinice now will be choosing the appropriate components to model the system based on the tags set by the GSM.

Now the results of the scans can be added into the control catalogue. Hereby select the server object and select the option `Greenbone: Automatic Base Security Check` from the context menu.

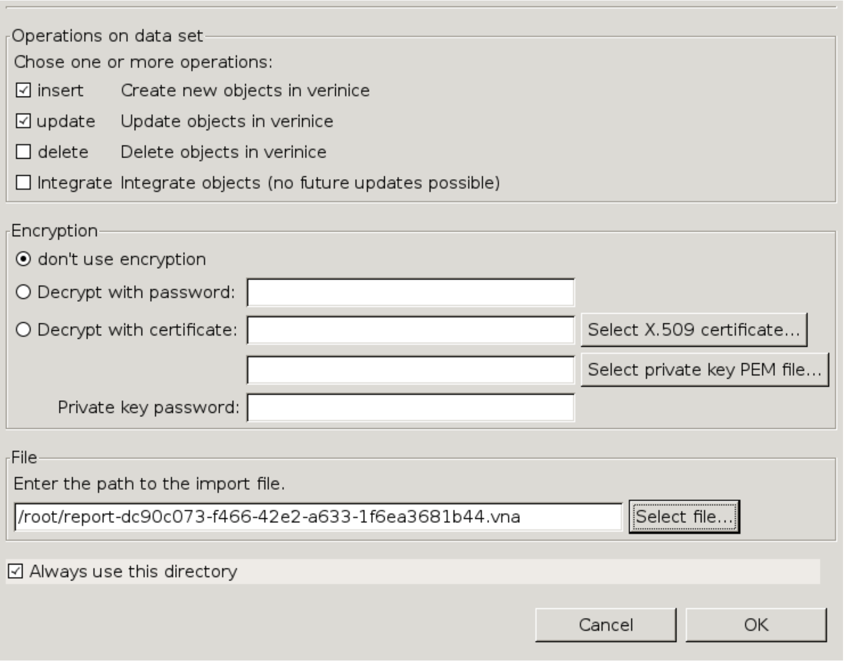
22.3 Nagios

Nagios can integrate the scan results in its monitoring tasks as additional test. In this case the scanned systems are automatically matched with the monitored systems. With this the scan results are eventually available for the alert rules and other processes of Nagios.

When linking Nagios with GSM, Nagios will assume the controlling role. Nagios regularly and automatically retrieves the newest scan results from Greenbone Security Manager. This is done via a Nagios plugin (“check_omp”).

Follow the step-by-step instructions to connect the GSM to Nagios as part of the Open Monitoring Distribution[145] (OMD) are covered as an example. Other products like Icinga, Centreon etc. might re-

[145] http://omdistro.org/



Operations on data set

Chose one or more operations:

- ☑ insert Create new objects in verinice
- ☑ update Update objects in verinice
- ☐ delete Delete objects in verinice
- ☐ Integrate Integrate objects (no future updates possible)

Encryption

- ● don't use encryption
- ○ Decrypt with password:
- ○ Decrypt with certificate: [Select X.509 certificate...] [Select private key PEM file...]
- Private key password:

File

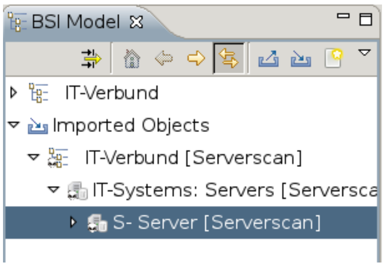
Enter the path to the import file.

/root/report-dc90c073-f466-42e2-a633-1f6ea3681b44.vna [Select file...]

☑ Always use this directory

[Cancel] [OK]

Fig. 22.11: Select the report on the dialog.



BSI Model

- ▷ IT-Verbund
- ▽ Imported Objects
  - ▽ IT-Verbund [Serverscan]
    - ▽ IT-Systems: Servers [Serversca
      - ▷ S- Server [Serverscan]

Fig. 22.12: The imported data can be unfolded in verinice.

quire small adjustments to the described steps.

22.3.1 Configuration of the GSM User

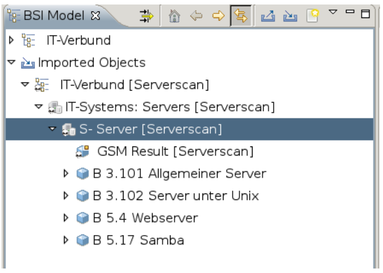
For access the plugin requires a user used to login to the appliance. On the GSM and for this user, a scan target (or multiple ones) must be set up with all hosts of which the security status is to be monitored. The sample configuration used here assumes that there is only one relevant target but technically it is possible to link complex setups with multiple targets and multiple GSMs.

The GSM user account provided for queries by the Nagios plugin must be owner of the relevant scan targets or at least have unrestricted reading access to them. The tasks should be run as scheduled scans regularly.

In addition network access via OMP to the GSM appliance must be possible. Therefore the OMP access must be activated in the GOS-Admin-Menu via the command line (see sections *Activating the OMP Protocol* (page 179) and *OpenVAS Management Protocol (OMP)* (page 30))

22.3.2 Installation of the Plugin

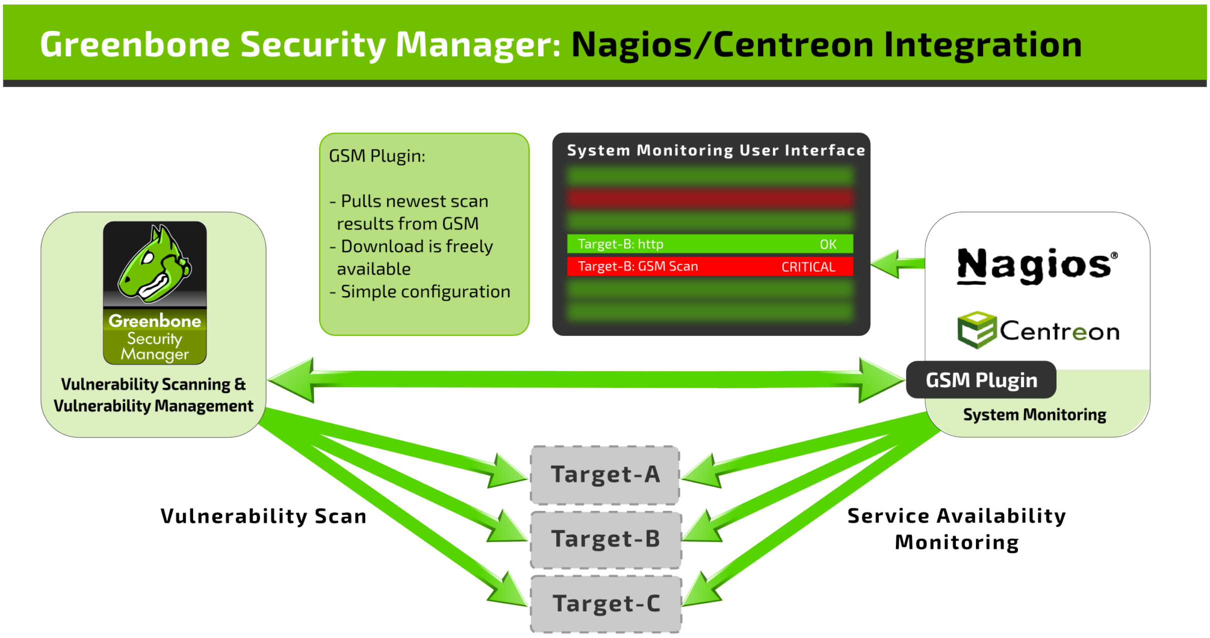
Greenbone provides the `check_omp` under http://greenbone.net/download/tools/check_omp, For the analysis of the source code, it can be viewed at http://greenbone.net/download/sources/check_omp-src.r18825.tar.gz.



BSI Model

- IT-Verbund
- Imported Objects
  - IT-Verbund [Serverscan]
    - IT-Systems: Servers [Serverscan]
      - S- Server [Serverscan]
        - GSM Result [Serverscan]
        - B 3.101 Allgemeiner Server
        - B 3.102 Server unter Unix
        - B 5.4 Webserver
        - B 5.17 Samba

Fig. 22.13: Now the IT Security Baseline components can be selected automatically.


Greenbone Security Manager: Nagios/Centreon Integration
GSM Plugin:
- Pulls newest scan results from GSM
- Download is freely available
- Simple configuration
System Monitoring User Interface
Target-B: http OK
Target-B: GSM Scan CRITICAL
Greenbone Security Manager
Vulnerability Scanning & Vulnerability Management
Nagios®
Centreon
GSM Plugin
System Monitoring
Target-A
Target-B
Target-C
Vulnerability Scan
Service Availability Monitoring

Download the plugin to your monitoring system and make it executable:

```
omd-host :˜# wget -q http://greenbone.net/download/tools/check_omp
omd-host :˜# chmod 755 check_omp
omd-host :˜# ./check_omp --version
Check-OMP Nagios Command Plugin 1.3+ beta3
Copyright (C) 2013 Greenbone Networks GmbH
License GPLv2+: GNU GPL version 2 or later
This is free software : you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

Copy the plugin now to `/opt/omd/sites/`*`site`*`/local/lib/nagios/plugins/`.

22.3.3 Configuring the Plugin

First check if the plugin can reach the GSM through the network, OMP was activated and the user was created properly. In the following command replace the IP address with the IP address of your GSM and provide the user name and password you created.

```
omd-host# /opt/omd/sites/<site>/local/lib/nagios/plugins/check_omp -H 192.168.255.12 \
-u omd -w password -ping
OMP OK: Alive and kicking!
```

Next check if you also have access to the data. The easiest way is to do this via the command line.

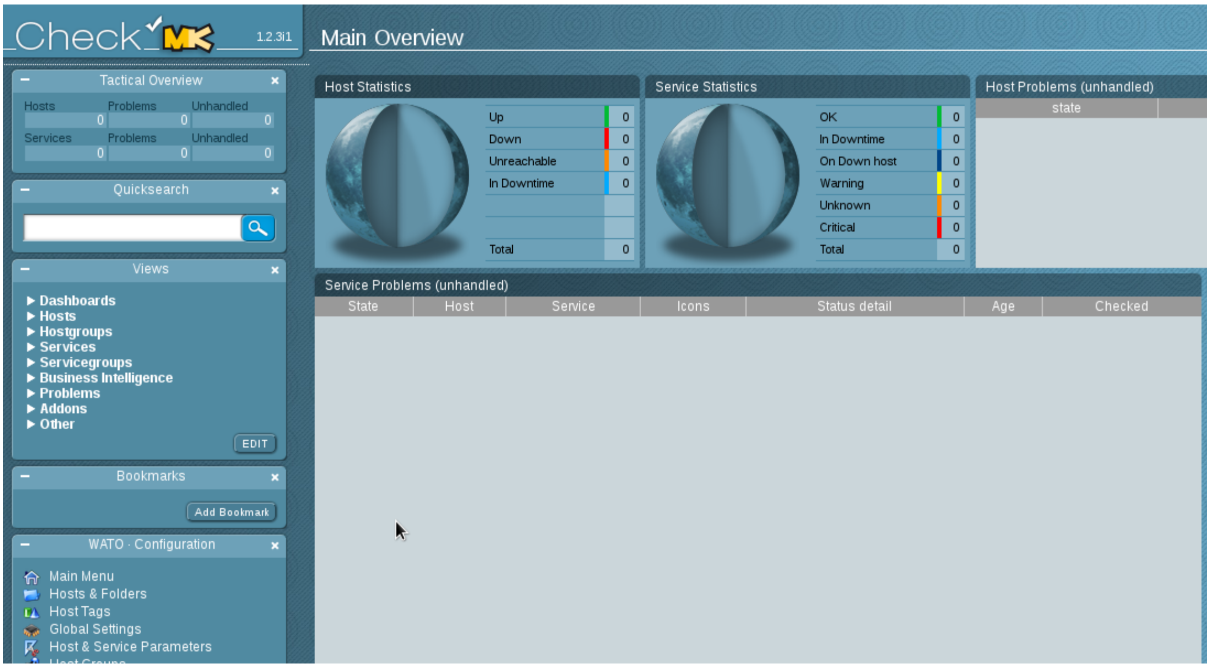
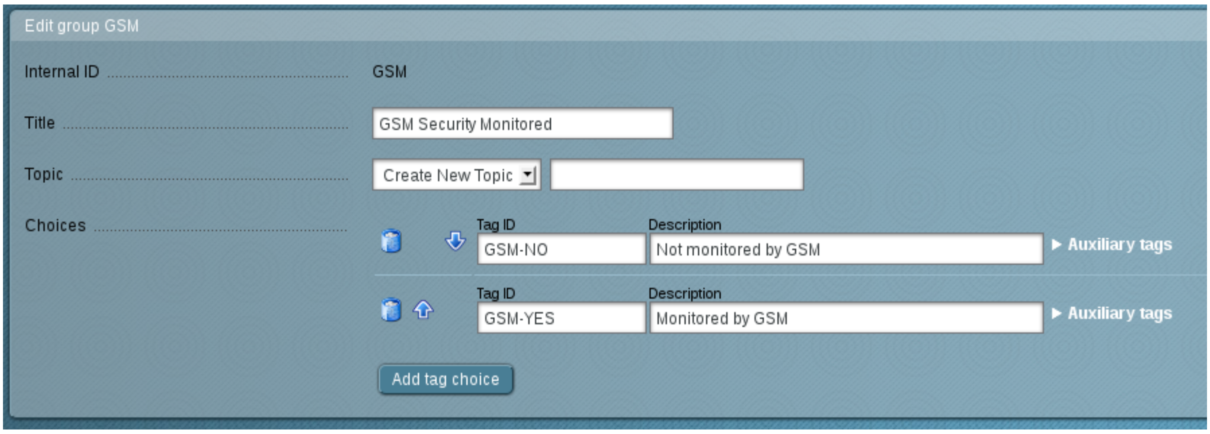


Fig. 22.14: The configuration is done by example on an empty sample site.

```
omd-host# /opt/omd/sites/<site>/local/lib/nagios/plugins/check_omp -H 192.168.255.12 \
-u omd -w password --status -T KVM-Hosts --last-report -F 192.168.255.199
OMP CRITICAL: 4 vulnerabilities found - High : 1 Medium : 1 Low : 2
|High=1 Medium=1 Low=2
```



Edit group GSM

Internal ID: GSM

Title: GSM Security Monitored

Topic: Create New Topic

Choices:

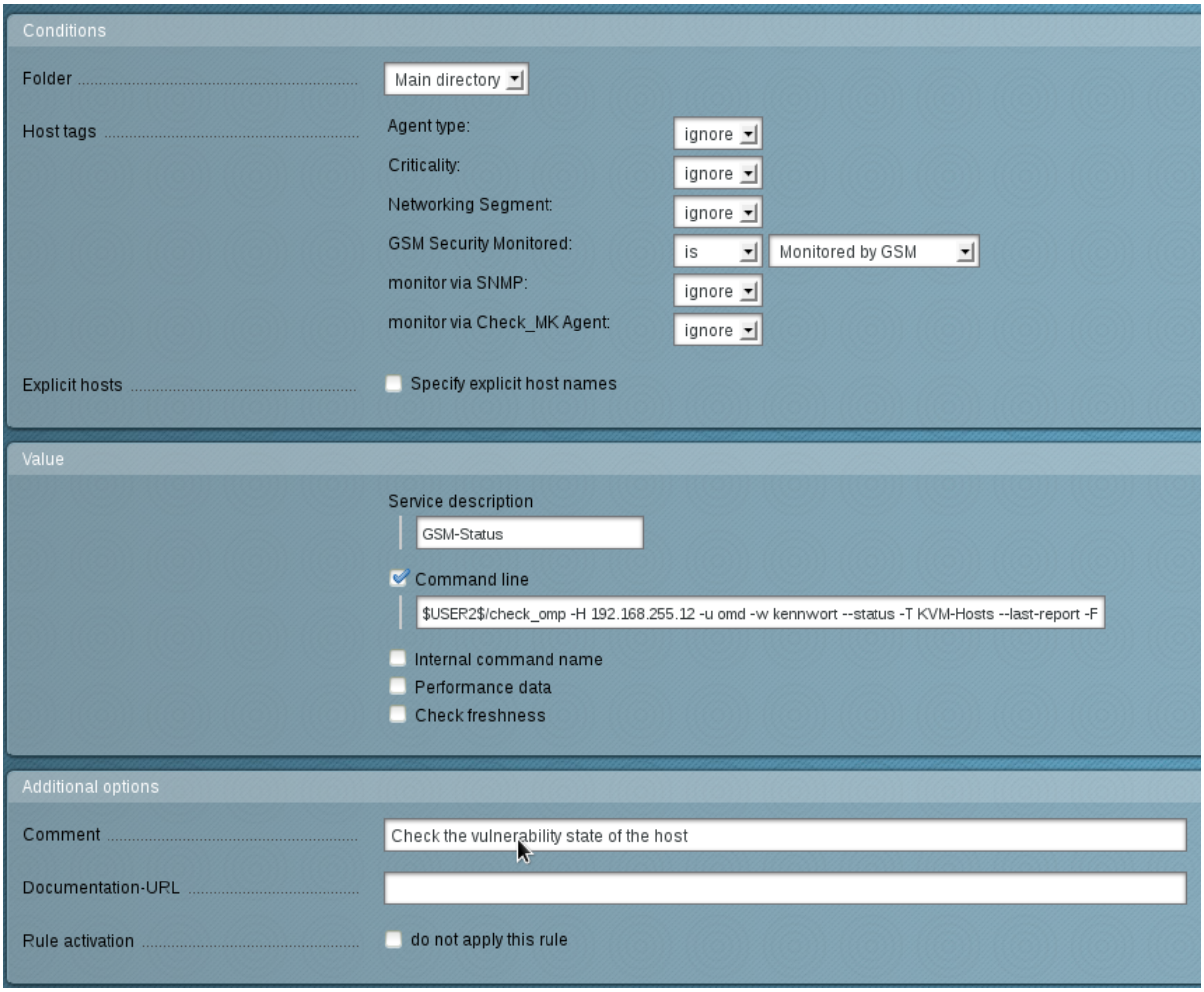
Tag ID	Description
GSM-NO	Not monitored by GSM
GSM-YES	Monitored by GSM

Fig. 22.15: The host tag labels the systems that are being monitored by the GSM.

If the tests were successful the check can be integrated into the web administration frontend WATO. For this switch to the web interface Multisite for your OMD page (see figure *The configuration is done by example on an empty sample site.* (page 216)).

First create the host tag (figure *The host tag labels the systems that are being monitored by the GSM.* (page 216)). It labels the hosts that are also being scanned by the GSM appliance. For this select `Host Tags` in the left menu and here create a new task.

New create a new rule (figure *This rule checks the status in the GSM for every host with the tag Monitored by GSM.* (page 217)), that analyzes the host tag. For this select in the left menu in `Host & Service Parameters` the option `Active Checks`. In the next menu select `Classical Active and Passive Nagios Checks`. Then create a new rule (figure *This rule checks the status in the GSM for every host with the tag Monitored by GSM.* (page 217)) in the current folder (`Create Rule`



Conditions

Folder: Main directory

Host tags:
- Agent type: ignore
- Criticality: ignore
- Networking Segment: ignore
- GSM Security Monitored: is — Monitored by GSM
- monitor via SNMP: ignore
- monitor via Check_MK Agent: ignore

Explicit hosts: □ Specify explicit host names

Value

Service description: GSM-Status

☑ Command line: $USER2$/check_omp -H 192.168.255.12 -u omd -w kennwort --status -T KVM-Hosts --last-report -F

□ Internal command name
□ Performance data
□ Check freshness

Additional options

Comment: Check the vulnerability state of the host

Documentation-URL:

Rule activation: □ do not apply this rule

Fig. 22.16: This rule checks the status in the GSM for every host with the tag `Monitored by GSM`.

`in Folder Main Directory`). Remember to use the following command:

```
$USER2$/check_omp -H <gsm -ip > -u <user > -w < password > -- status -T <report > \
--last -report -F $HOSTADDRESS$
```

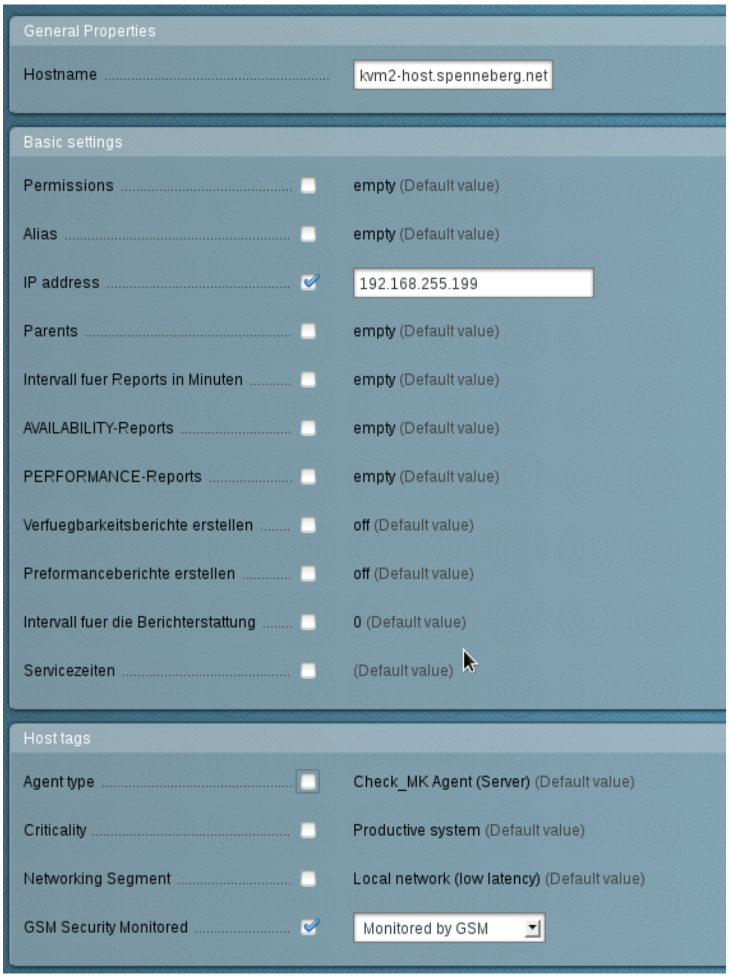
Now the host has to be created or configure in a way that it has the respective host tag (see figure *Every host scanned by the GSM now must have the tag.* (page 218)).

After the changes have been activated in the multisite (`Activate Changes`) the status information is available in the graphical interface.

So that the user name and password are not being displayed in the graphical interface they can be saved as variables to the file `/opt/omd/sites/`*`site`*`/etc/nagios/resource.cfg`:

```
############################################
# OMD settings, please use them to make your config
# portable, but dont change them
$USER1$=/omd/sites/produktiv/lib/nagios/plugins
$USER2$=/omd/sites/produktiv/local/lib/nagios/plugins
$USER3$=produktiv
$USER4$=/omd/sites/produktiv
############################################
# set your own macros here:
$USER5$=omd
$USER6$=kennwort
```

Now the username and the password can be replaced with the variables USER5 and USER6 in WATO.



General Properties

Hostname		kvm2-host.spenneberg.net

Basic settings

Permissions	□	empty (Default value)
Alias	□	empty (Default value)
IP address	☑	192.168.255.199
Parents	□	empty (Default value)
Intervall fuer Reports in Minuten	□	empty (Default value)
AVAILABILITY-Reports	□	empty (Default value)
PERFORMANCE-Reports	□	empty (Default value)
Verfuegbarkeitsberichte erstellen	□	off (Default value)
Preformanceberichte erstellen	□	off (Default value)
Intervall fuer die Berichterstattung	□	0 (Default value)
Servicezeiten	□	(Default value)

Host tags

Agent type	□	Check_MK Agent (Server) (Default value)
Criticality	□	Productive system (Default value)
Networking Segment	□	Local network (low latency) (Default value)
GSM Security Monitored	☑	Monitored by GSM

Fig. 22.17: Every host scanned by the GSM now must have the tag.

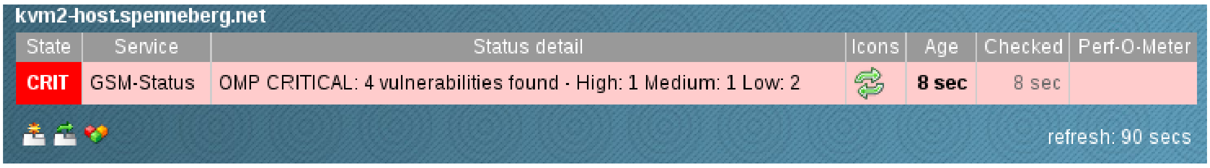
22.4 Sourcefire Defence Center

The Sourcefire Intrusion Prevention System (IPS) is one of the leading solution for intrusion detection and defense in computer networks. As a Network Intrusion Detection System (NIDS) it is being tasked with the discovery, alerting and the defense against attacks on the network.

For the Sourcefire IPS to correctly identify and classify attacks it requires as close as possible information about the systems in the network, the installed applications as well as their possible vulnerabilities. For this purpose the Sourcefire System has its own asset database that can be augmented with information from the GSM. Additionally the Sourcefire system can start an automatic scan if it suspects anything.

The connection methods are available:

1. **Automatic data transfer from the GSM to the NIDS/IDS** If the GSM and NIDS/IDS are configured respectively the data transfer from the GSM to the NIDS/IPS can be utilized easily, like



kvm2-host.spenneberg.net

State	Service	Status detail	Icons	Age	Checked	Perf-O-Meter
CRIT	GSM-Status	OMP CRITICAL: 4 vulnerabilities found - High: 1 Medium: 1 Low: 2		8 sec	8 sec	

refresh: 90 secs

Fig. 22.18: The GSM status is now being displayed in the multisite.

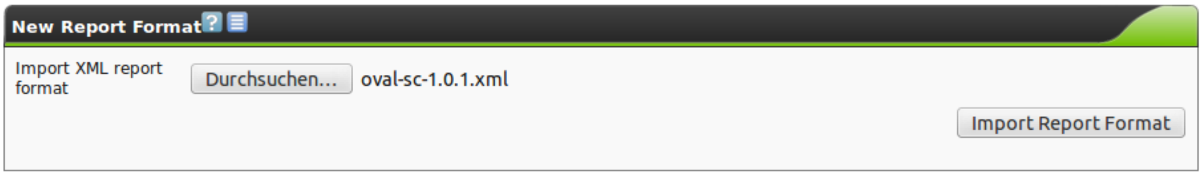
any other alert functionality of the GSM. After completion of the scan it will be forwarded as an alert to the NIDS/IPS in respect to the desired criteria. If the scan task is being run automatically on a weekly basis you get a fully automated alerting and optimization system.

2. **Active control of the GSM by the NIDS/IPS** In the operation of the NIDS/IPS suspected incidents on systems with high risk can occur. In such a case the NIDS/IPS can instruct the GSM to check the system [146].

To use the connection in the options 1 and 2 the GSM as well as the Sourcefire Defense Center must be prepared. In the GSM a report plugin must be installed and on the Defense Center receiving the data must be enabled.

22.4.1 Installation of the Report Plugin

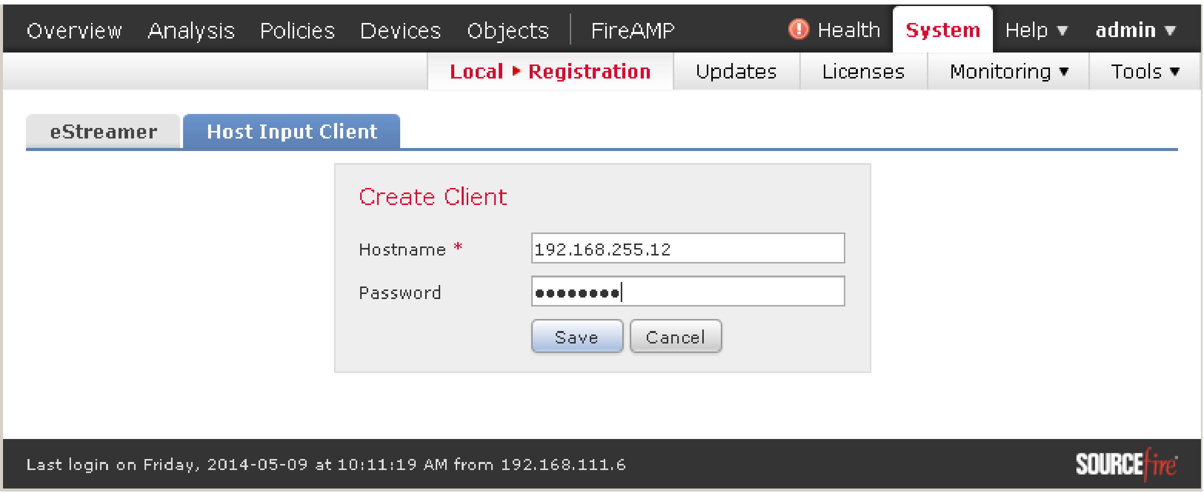
The report plugin can be obtained from the Greenbone web site under http://greenbone.net/technology/report_formats.html. Download the plug in and install it on the GSM. Remember to verify and activate the plugin after importing (see section *Import of additional plugins* (page 91)).



Import XML report format: oval-sc-1.0.1.xml

Fig. 22.19: The report plugin processes the data for Sourcefire.

22.4.2 Configuration of the Host-Input-API clients



Hostname *: 192.168.255.12

Password: ••••••••

Last login on Friday, 2014-05-09 at 10:11:19 AM from 192.168.111.6

Fig. 22.20: The GSM must be set up in the Defense Center.

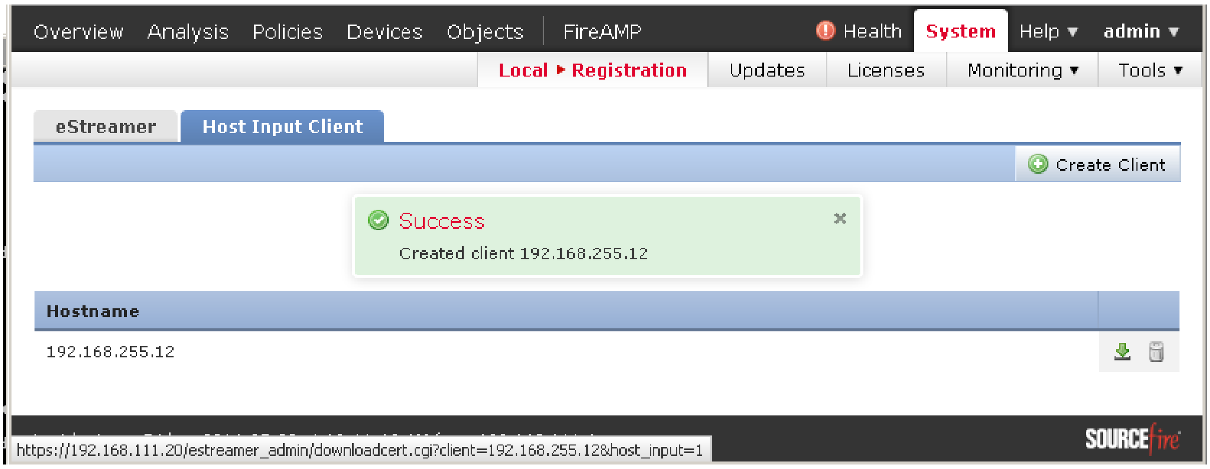
Log into the Sourcefire Defense Center and create a Host-Input-Client. The Host-Input-API is an interface through which the Defense Center accepts data from other applications for its asset database. This option can be found in the web interface under System->Local->Registration. There change into the `Host Input Client` register. Here create the GSM appliance. It is important to enter the IP address of the appliance that the appliance will use to connect to the Defense Center. The connection

[146] This control does not exist as a finalized *Remediation* for the Sourcefire system but it can be implemented via OMP (see chapter OpenVAS Management Protocol (page 179)).

is TLS encrypted. The Defense Center creates a private key and certificate automatically. In the certificate the IP address entered above will be used as Common Name and verified when the client is establishing a connection. If the client uses a different IP address the connection fails.

The created PKCS12 file is optionally secured by a password.

Afterwards the certificate and the key are being created and made available as a download. Download this file.



Success

Created client 192.168.255.12

Hostname
192.168.255.12

https://192.168.111.20/estreamer_admin/downloadcert.cgi?client=192.168.255.12&host_input=1

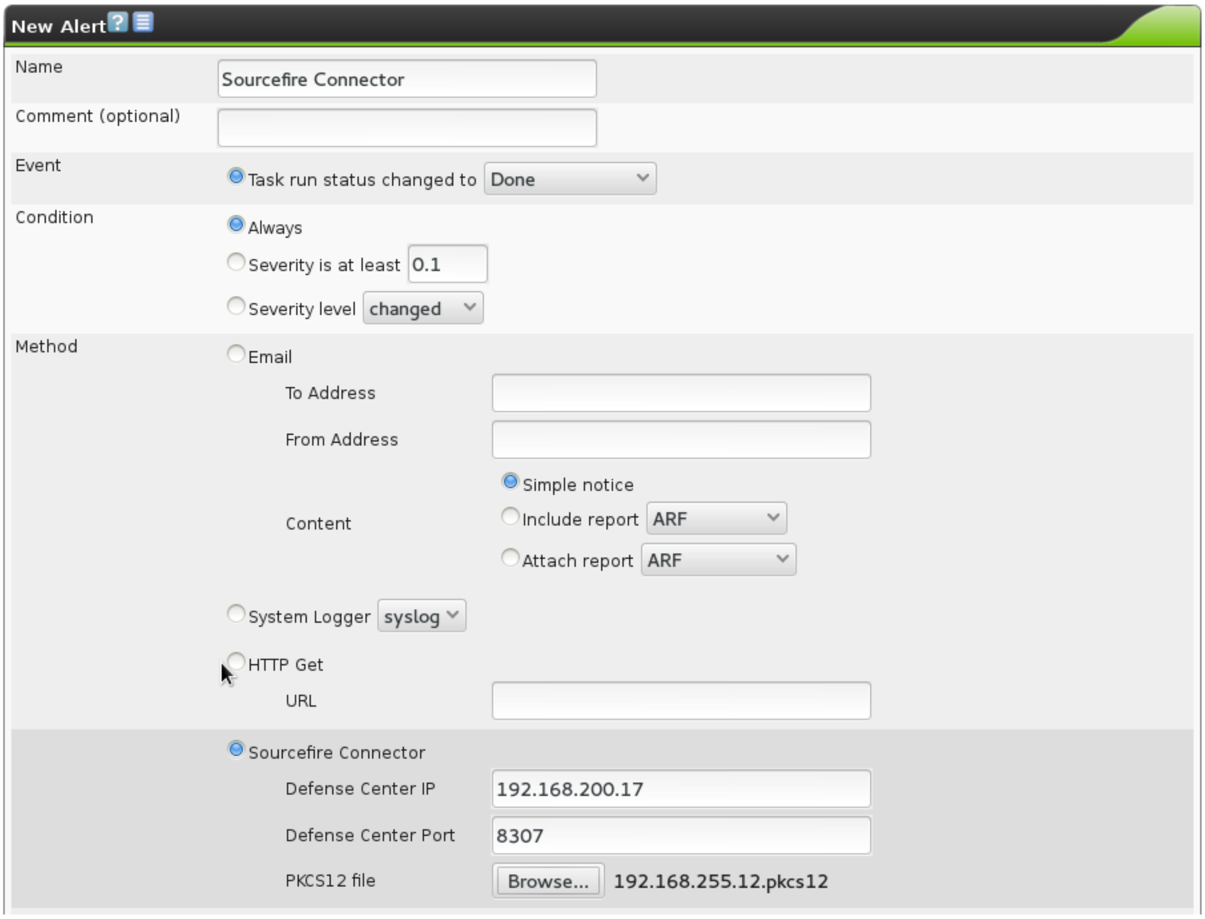
Fig. 22.21: The created PKCS12 file must be downloaded.

22.4.3 Configuration of Alerts on the GSM

Now the respective Alerts must be set up on the GSM. For this switch to *Configuration/Alerts*. Enter the data of the Sourcefire system and the supply the PKCS12 file.

If a password was entered when the client was created the PKCS12 must be decrypted before loading it onto the GSM. For this you can use the following command under Linux:

```
$ openssl pkcs12 -in encrypted.pkcs12 -nodes -out decrypted.pcks12
Enter Import Password : password
MAC verified OK
$
```



New Alert

Name: Sourcefire Connector

Comment (optional):

Event: ● Task run status changed to Done

Condition:
● Always
○ Severity is at least 0.1
○ Severity level changed

Method:
○ Email
To Address:
From Address:
Content: ● Simple notice ○ Include report ARF ○ Attach report ARF
○ System Logger syslog
○ HTTP Get
URL:
● Sourcefire Connector
Defense Center IP: 192.168.200.17
Defense Center Port: 8307
PKCS12 file: Browse... 192.168.255.12.pkcs12

Fig. 22.22: The PKCS12 file is being used by the connector for authentication.

OpenVAS Scanner Protocol

The OpenVAS Scanner Protocol (OSP) is a XML-based stateless request-response API that offers a unified abstraction for vulnerability scanners. The Greenbone Security Manager is able to seamless integrate OSP scanners into the vulnerability management. OSP scanners are all controlled in the same way and the results are stored in the database all in the same structures. An arbitrary number of different or same OSP scanners can be connected.

The term "Vulnerability Scanner" is a to be interpreted pretty far-reaching. It also could be about queries into a patch management system or a plain asset query. As a result of a scanner it is only expected that it is vulnerability details or asset information. The latter could be installed software packages, open ports, running services, TLS certificates or similar.

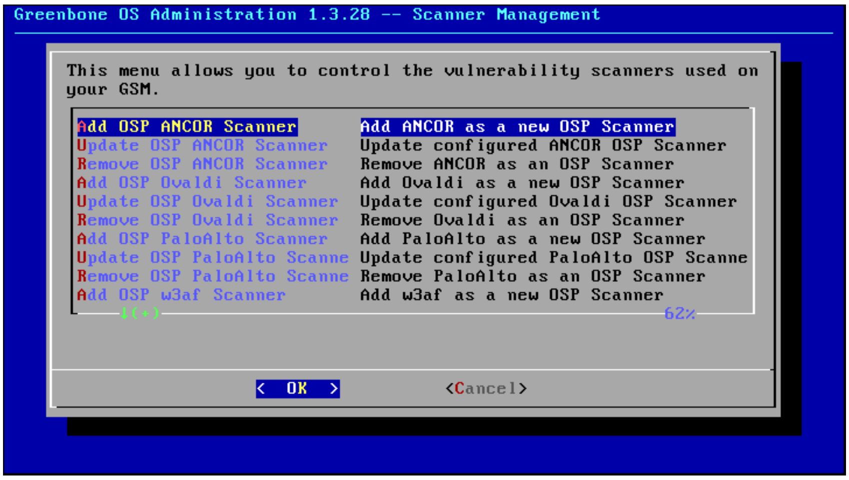
Some OSP scanner are integrated on the GSM appliance and can be enabled via GOS-Admin menu. But it is also possible to add remote OSP scanners.

23.1 Enabling additional OSP Scanners

Additional Scanners may be enabled through the GOS-Admin-Menu. The GSM comes with the OpenVAS scanner configured by default. No other scanner is enabled.

Note: Starting with GOS 3.1.17 pilot users can choose additional scanners. This feature will be available for all users through a later update. To become a pilot user, contact the Greenbone Support.

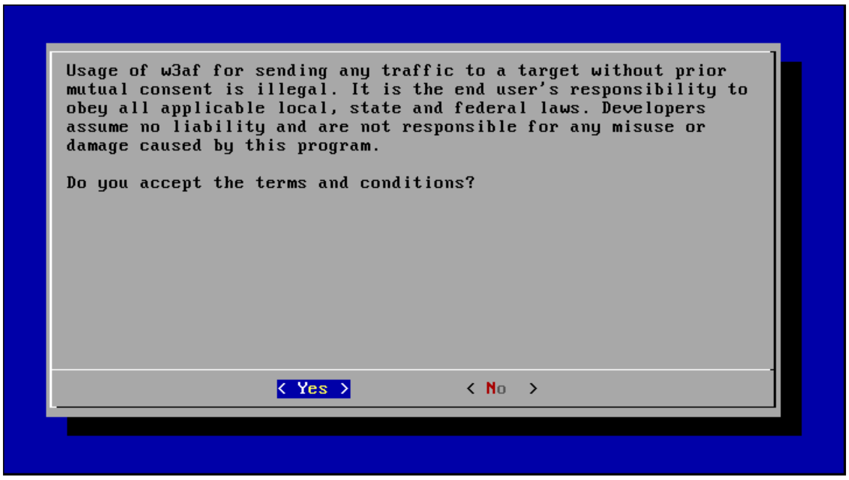
To enable the additional scanners enter the GOS-Admin-Menu and select *Advanced/Scanner Management*. The following menu will be presented:



```
Greenbone OS Administration 1.3.28 -- Scanner Management

This menu allows you to control the vulnerability scanners used on
your GSM.

Add OSP ANCOR Scanner        Add ANCOR as a new OSP Scanner
Update OSP ANCOR Scanner     Update configured ANCOR OSP Scanner
Remove OSP ANCOR Scanner     Remove ANCOR as an OSP Scanner
Add OSP Ovaldi Scanner       Add Ovaldi as a new OSP Scanner
Update OSP Ovaldi Scanner    Update configured Ovaldi OSP Scanner
Remove OSP Ovaldi Scanner    Remove Ovaldi as an OSP Scanner
Add OSP PaloAlto Scanner     Add PaloAlto as a new OSP Scanner
Update OSP PaloAlto Scanne   Update configured PaloAlto OSP Scanne
Remove OSP PaloAlto Scanne   Remove PaloAlto as an OSP Scanner
Add OSP w3af Scanner         Add w3af as a new OSP Scanner
    ↓(+)                                                   62%

              <  OK  >              <Cancel>
```

Fig. 23.1: Enabling additional scanners

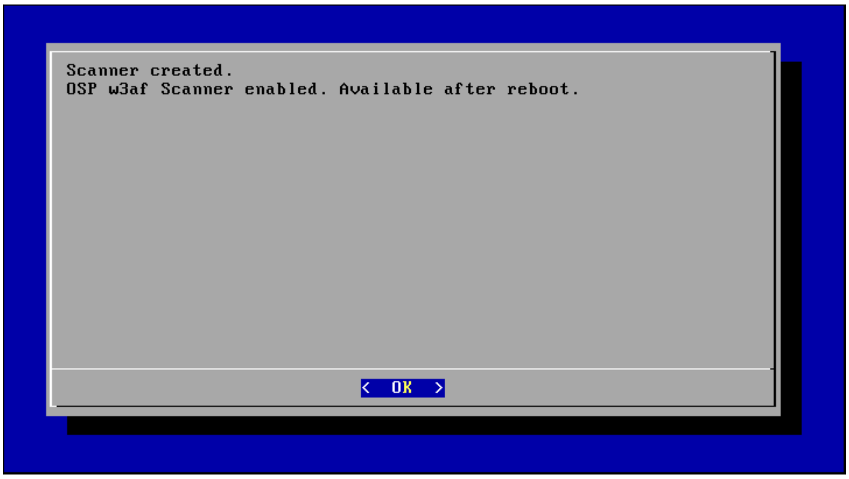
To enable the w3af scanner select *Add OSP w3af Scanner*. Depending on the scanner chosen, some information might be displayed for acceptance:



```
Usage of w3af for sending any traffic to a target without prior
mutual consent is illegal. It is the end user's responsibility to
obey all applicable local, state and federal laws. Developers
assume no liability and are not responsible for any misuse or
damage caused by this program.

Do you accept the terms and conditions?
```

Fig. 23.2: Accept the terms and conditions

Then the scanner is created. The scanner will be available after an additional reboot.



```
Scanner created.
OSP w3af Scanner enabled. Available after reboot.
```

Fig. 23.3: A reboot is required after enabling the scanner

Using the same menu you can update and disable the scanner as well.

23.2 How to write your own OSP wrapper

The OSP protocol documentation is available from the Greenbone website at

http://docs.greenbone.net/API/OSP/osp.html

23.2.1 The challenge: debsecan as OSP scanner

In the following we will work on the challenge to create a OSP wrapper for the tool "debsecan". This tool is available for Debian GNU/Linux systems and can create a list of vulnerabilities the present system is subject to. The tool goes beyond a simple match about which package updates are missing. It rather does an online query to learn about software packages where security problems are identified, but not yet been finally processed to become a security update.

Further details about the tool are available on the debsecan homepage:

http://www.enyo.de/fw/software/debsecan/

For executing debsecan a low privileged user account is sufficient:

```
$ debsecan
CVE-2015-3333 chromium (remotely exploitable, high urgency)
CVE-2015-3334 chromium (remotely exploitable, medium urgency)
CVE-2015-3336 chromium (remotely exploitable, medium urgency)
TEMP-0000000-EA424A libbluray1
CVE-2014-9447 libelf1 (remotely exploitable, medium urgency)
CVE-2014-8354 libmagickcore5
CVE-2014-8355 libmagickcore5
CVE-2014-8562 libmagickcore5
CVE-2014-8716 libmagickcore5
TEMP-0000000-2FC21E libmagickcore5 (low urgency)
TEMP-0000000-7C079F libmagickcore5
TEMP-0000000-EEF23C libmagickcore5 (low urgency)
TEMP-0000000-FDAC72 libmagickcore5
TEMP-0773834-5EB6CF libmagickcore5
CVE-2013-4288 libpolkit-gobject-1-0 (low urgency)
CVE-2002-2439 libstdc++6-4.7-dev (low urgency)
CVE-2014-5044 libstdc++6-4.7-dev
...
```

As you can see, many vulnerabilities are already linked to a CVE. Now we want to make these information available to the Greenbone Security Manager (GSM).

23.2.2 The basis: ospd

After all, OSP is only a specification. So, you could implement an OSP wrapper with an arbitrary programming language.

However, to start immediately with the actual coupling you can use the readily available OpenVAS module "ospd". It is written in Python and offers a base class as well as supporting functions. The entire server functionality including TLS encryption is already done.

You can download the current ospd package from this site:

http://www.openvas.org/install-source-de.html

We will work with version 1.0.0:

https://wald.intevation.org/frs/download.php/1999/ospd-1.0.0.tar.gz

And of course we will check the signature:

https://wald.intevation.org/frs/download.php/1999/ospd-1.0.0.tar.gz.sig

```
$ gpg --verify ospd-1.0.0.tar.gz.sig

$ tar xzf ospd-1.0.0.tar.gz
$ cd ospd-1.0.0/
```

We will now install the package at a temporary place:

```
$ mkdir /tmp/osptest
$ export PYTHONPATH=/tmp/osptest/lib/python2.7/site-packages/
```

Finally ospd is installed into that temporary directory:

```
$ python setup.py install --prefix=/tmp/osptest
```

Of course many roads lead to Rome. You could install the package to arbitrary other places and in other ways. If you are familiar with Python you may choose your preferred way.

23.2.3 The skeleton for the new OSP scanner

As a first step we create a new directory and the central file “wrapper.py”.

One important element is an inheritance of the “OSPDaemon” class with a very simple self information for the time being, which we will call “OSPDdebsecan”. And the other important element is the main routine of the service itself (“main”).

```
$ mkdir -p debsecan/ospd_debsecan
$ cd debsecan/ospd_debsecan
$ gvim wrapper.py
```

```
from ospd.ospd import OSPDaemon
from ospd.misc import main as daemon_main
from ospd_debsecan import __version__

class OSPDdebsecan(OSPDaemon):

    """ Class for ospd-debsecan daemon. """

    def __init__(self, certfile, keyfile, cafile):
        """ Initializes the ospd-debsecan daemon's internal data. """
        super(OSPDdebsecan, self).__init__(certfile=certfile, keyfile=keyfile,
                                            cafile=cafile)
        self.server_version = __version__
        self.scanner_info['name'] = 'debsecan'

    def check(self):
        """ Checks that debsecan command line tool is found and is executable. """
        return True

def main():
    """ OSP debsecan main function. """
    daemon_main('OSPD - debsecan wrapper', OSPDdebsecan)
```

Next we will complete the skeleton to obtain an operational, yet pretty stupid service. For this we create “__init_.py” in the same directory where “wrapper.py” is located:

```
__version__ = '1.0b1'
```

And finally the control module for the package: debsecan/setup.py:

```
from setuptools import setup

from ospd_debsecan import __version__

setup(
    name='ospd-debsecan',
    version=__version__,

    packages=['ospd_debsecan'],

    url='http://www.openvas.org',
    author='OpenVAS Development Team',
    author_email='info@openvas.org',

    license='GPLV2+',
    install_requires=['ospd==1.0.0'],

    entry_points={
        'console_scripts': ['ospd-debsecan=ospd_debsecan.wrapper:main'],
    },
)
```

With this structure the new server can be installed and started:

```
$ python setup.py install --prefix=/tmp/osptest
```

If not yet happened, you might need to adjust the search path for the new server:

```
$ export PATH=$PATH:/tmp/osptest/bin
```

This given, the server can be called directly:

```
$ ospd-debsecan --version
OSP Server for debsecan version 1.0b1
OSP Version: 1.0
Using: OSPd 1.0.0
Copyright (C) 2014, 2015 Greenbone Networks GmbH
License GPLv2+: GNU GPL version 2 or later
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

Lets next test the server functionality and send the server into the background so that it waits for request at port 2346 of our local system:

```
$ ospd-debsecan -b 127.0.0.1 -p 2346 \
  -k /tmp/osptest/var/lib/openvas/private/CA/clientkey.pem \
  -c /tmp/osptest/var/lib/openvas/CA/clientcert.pem \
  --ca-file /tmp/osptest/var/lib/openvas/CA/cacert.pem  &
```

The applied keys and certificates are those which were actually created for the OpenVAS scanner by the tool “openvas-mkcert”. For simplicity here we use use them instead of properly creating our own key pair. If you have installed OpenVAS scanner with a different prefix, then use that one instead of “/tmp/osptest/”.

As you can already suspect, the authentication for our OSP server works via client certificate. An authentication with a username and password is not supported.

With the “omp” command line tool of the “openvas-cli” package we can contact the server:

```
$ omp -h 127.0.0.1 -p 2346 --use-certs -X "<get_version/>"
<get_version_response status_text="OK" status="200"><protocol><version>1.0</versi...
```

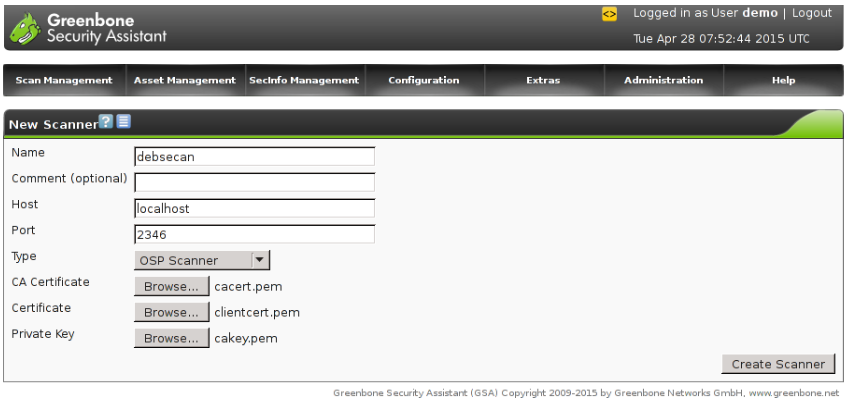
As a default, the “omp” option “–use-certs” will use the standard paths for keys and certificates. Of course it works this way only if executed in the same environment as the server.

The response can be made nicer and easier to read with the additional option “–pretty-print”:

```
$ omp -h 127.0.0.1 -p 2346 --use-certs --pretty-print  -X "<get_version/>"
    <get_version_response status_text="OK" status="200">
      <protocol>
        <version>1.0</version>
        <name>OSP</name>
      </protocol>
      <daemon>
        <version>1.0.0</version>
        <name>OSPd</name>
      </daemon>
      <scanner>
        <version>No version</version>
        <name>debsecan</name>
      </scanner>
    </get_version_response>
```

Lets look at this result in the graphical user interface.

Via menu *Configuration/Scanners* we create a new scanner, see figure *Creating a new OSP scanner* (page 228). The certificates are the same as used for starting the scanner.

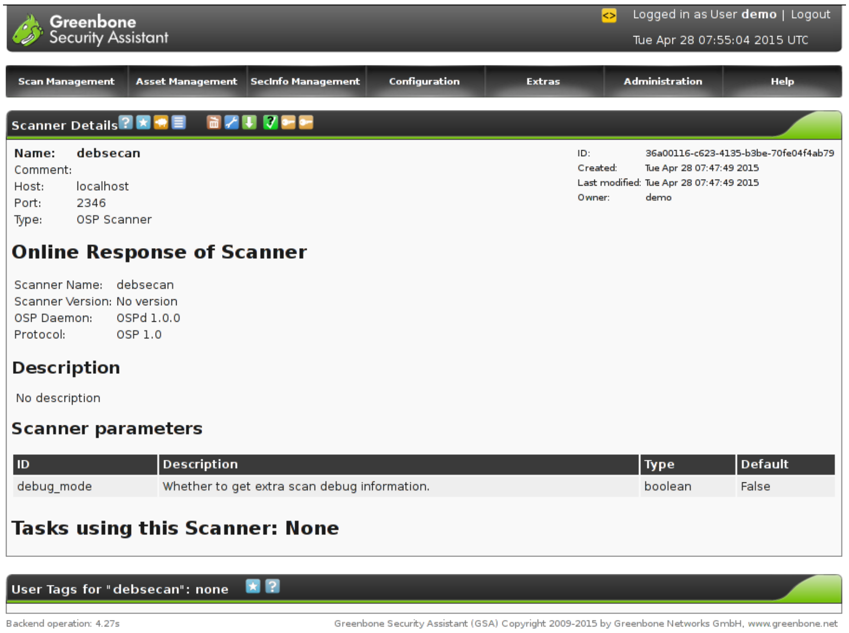

Greenbone
Security Assistant
Logged in as User demo | Logout
Tue Apr 28 07:52:44 2015 UTC
Scan Management
Asset Management
SecInfo Management
Configuration
Extras
Administration
Help
Browse...
Create Scanner
Greenbone Security Assistant (GSA) Copyright 2009-2015 by Greenbone Networks GmbH, www.greenbone.net

New Scanner

Name	debsecan
Comment (optional)	
Host	localhost
Port	2346
Type	OSP Scanner
CA Certificate	cacert.pem
Certificate	clientcert.pem
Private Key	cakey.pem

Fig. 23.4: Creating a new OSP scanner

Directly after the creation of the new scanner, the details about the scanner are displayed, see figure *Online response test for the OSP scanner* (page 228). This “Online Response” shows the same version identification as above plus a parameter: “debug_mode” is a standard parameter of the base class “OSPDaemon”.


Greenbone
Security Assistant
Logged in as User demo | Logout
Tue Apr 28 07:55:04 2015 UTC
Scan Management
Asset Management
SecInfo Management
Configuration
Extras
Administration
Help
User Tags for "debsecan": none
Backend operation: 4.27s
Greenbone Security Assistant (GSA) Copyright 2009-2015 by Greenbone Networks GmbH, www.greenbone.net

Scanner Details

Name:	debsecan	ID:	36a00116-c623-4135-b3be-70fe04f4ab79
Comment:		Created:	Tue Apr 28 07:47:49 2015
Host:	localhost	Last modified:	Tue Apr 28 07:47:49 2015
Port:	2346	Owner:	demo
Type:	OSP Scanner		

Online Response of Scanner

Scanner Name:	debsecan
Scanner Version:	No version
OSP Daemon:	OSPd 1.0.0
Protocol:	OSP 1.0

Description

No description

Scanner parameters

ID	Description	Type	Default
debug_mode	Whether to get extra scan debug information.	boolean	False

Tasks using this Scanner: None

Fig. 23.5: Online response test for the OSP scanner

So far well done: We have a working server. Unfortunately it can't do anything of the actual aim. This will change now.

23.2.4 Establish connection between debsecan and OSP

For this we need to define another class for our OSPDaemon, “exec_scan”:

```
def exec_scan(self, scan_id, target):
    """ Starts the debsecan scanner for scan_id scan. """

    # run the debsecan command
    result = subprocess.check_output(["debsecan"])

    # parse the output of the debsecan command and create
    # respective alarms
    for line in result.split("\n"):
        words = line.split()
        if words.__len__() > 2 and words[0].split("-")[0] == "CVE":
            self.add_scan_alarm(scan_id, host=target, name=words[0],
                                value=line)
```

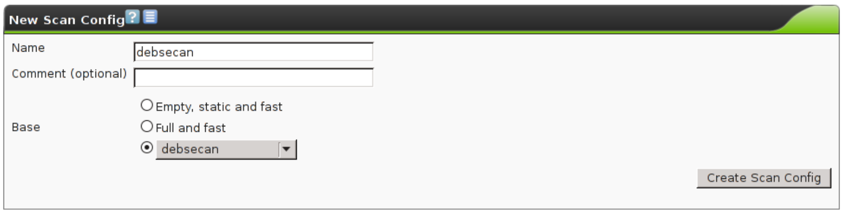
Like before we install and start the new version of the server and test the functionality at command line:

```
$ omp -h 127.0.0.1 -p 2346 --use-certs --pretty-print \
   -X "<start_scan target='localhost'><scanner_params/></start_scan>"

<start_scan_response status_text="OK" status="200">
  <id>8f48d691-c136-488f-8f31-d8761e1c75e1</id>
</start_scan_response>
```

This gives us the ID of our scan. Lets have a look at the scan details:

```
$ omp -h 127.0.0.1 -p 2346 --use-certs --pretty-print \
   -X "<get_scans scan_id='8f48d691-c136-488f-8f31-d8761e1c75e1'/>"

<get_scans_response status_text="OK" status="200">
  <scan id="8f48d691-c136-488f-8f31-d8761e1c75e1" target="localhost"
    end_time="1428004156" progress="100" start_time="1428004156">
    <results>
      <result host="localhost" severity="" test_id="" name="CVE-2015-3333"
       type="Alarm">CVE-2015-3333 chromium (remotely exploitable, high urgency)
      </result>
      <result host="localhost" severity="" test_id="" name="CVE-2015-3334"
       type="Alarm">CVE-2015-3334 chromium (remotely exploitable, medium urgency)
      </result>
      <result host="localhost" severity="" test_id="" name="CVE-2015-3336"
       type="Alarm">CVE-2015-3336 chromium (remotely exploitable, medium urgency)
      </result>
      <result host="localhost" severity="" test_id="" name="CVE-2014-9447"
       type="Alarm">CVE-2014-9447 libelf1 (remotely exploitable, medium urgency)
      </result>
      <result host="localhost" severity="" test_id="" name="CVE-2013-4288"
       type="Alarm">CVE-2013-4288 libpolkit-gobject-1-0 (low urgency)</result>
      <result host="localhost" severity="" test_id="" name="CVE-2002-2439"
       type="Alarm">CVE-2002-2439 libstdc++6-4.7-dev (low urgency)</result>
      <result host="localhost" severity="" test_id="" name="CVE-2013-2074"
       type="Alarm">CVE-2013-2074 kdelibs5-plugins (remotely exploitable, low urgency)
      </result>
    </results>
  </scan>
</get_scans_response>
```

This looks good indeed. Now for a scan via the GUI. For this we need a San Configuration for debsecan, even though it is actually empty. The creation is done via the menu *Configuration/Scan Configs*, see figure *Creating a new Scan Config for OSP scanner debsecan* (page 229).



New Scan Config

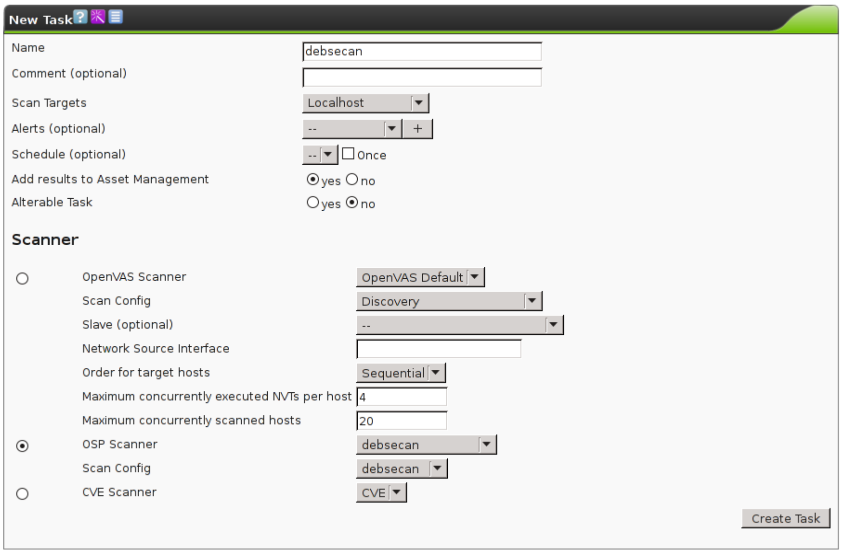
Name: debsecan

Comment (optional):

Base:
○ Empty, static and fast
○ Full and fast
● debsecan

Fig. 23.6: Creating a new Scan Config for OSP scanner debsecan

Next lets create the task as shown in figure *Creating a task for OSP scanner debsecan* (page 230).



New Task

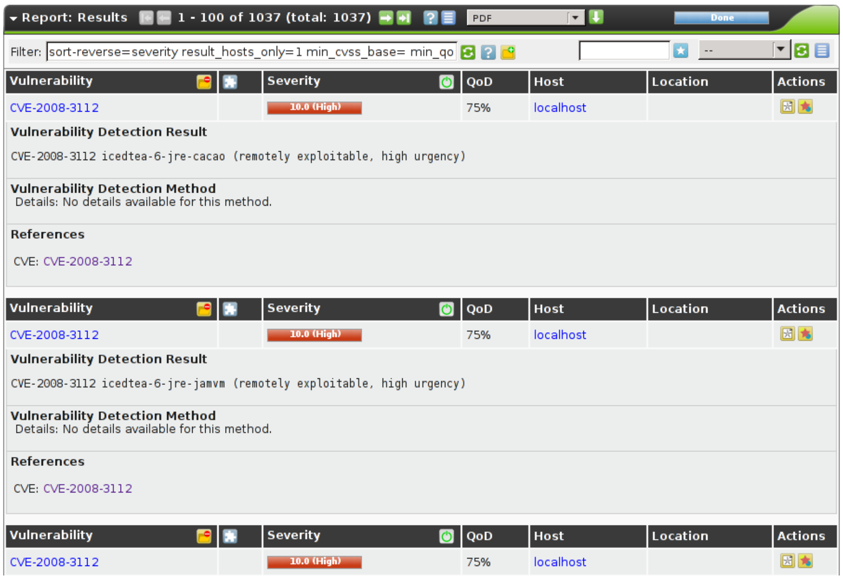
Name	debsecan
Comment (optional)	
Scan Targets	Localhost
Alerts (optional)	--
Schedule (optional)	-- □ Once
Add results to Asset Management	● yes ○ no
Alterable Task	○ yes ● no

Scanner

○	OpenVAS Scanner	OpenVAS Default
	Scan Config	Discovery
	Slave (optional)	--
	Network Source Interface	
	Order for target hosts	Sequential
	Maximum concurrently executed NVTs per host	4
	Maximum concurrently scanned hosts	20
●	OSP Scanner	debsecan
	Scan Config	debsecan
○	CVE Scanner	CVE

Fig. 23.7: Creating a task for OSP scanner debsecan

Finally we start the task in the usual way and get the results illustrated in figure *Scan results of OSP debsecan* (page 230).



Report: Results 1 - 100 of 1037 (total: 1037)

Filter: sort-reverse=severity result_hosts_only=1 min_cvss_base= min_qo

Vulnerability	Severity	QoD	Host	Location	Actions
CVE-2008-3112	10.0 (High)	75%	localhost		

Vulnerability Detection Result

CVE-2008-3112 icedtea-6-jre-cacao (remotely exploitable, high urgency)

Vulnerability Detection Method

Details: No details available for this method.

References

CVE: CVE-2008-3112

Vulnerability	Severity	QoD	Host	Location	Actions
CVE-2008-3112	10.0 (High)	75%	localhost		

Vulnerability Detection Result

CVE-2008-3112 icedtea-6-jre-jamvm (remotely exploitable, high urgency)

Vulnerability Detection Method

Details: No details available for this method.

References

CVE: CVE-2008-3112

Vulnerability	Severity	QoD	Host	Location	Actions
CVE-2008-3112	10.0 (High)	75%	localhost		

Fig. 23.8: Scan results of OSP debsecan

The severity of the results is automatically determined by the GSM based on the internal CVE database.

23.2.5 Result

With 40 lines of Python source code we established a OSP scanner connection that transfers the CVE vulnerability information of the tool debsecan into the Greenbone Security Manager.

When used as a regular task, we can now combine debsecan-based checks with scheduled execution, we can add notes or overrides and actually any other functionality that makes a full vulnerability management.

However, the OSP wrapper for debsecan is still a coarse one. It lacks error handling and by a better processing of the original output of debsecan we could achieve quite more information for the GSM.

Apart from such improvements, there is another desirable goal: The transformation of OSP-debsecan into a remote scanner. So far, the target system is ignored and instead always the local system is checked. With configured credentials on GSM-side, we could extend the OSP wrapper to log into the given target system, execute debsecan on that remote host and process the results in the usual way. This would allow to check entire networks without the need to install ospd-debsecan on each host. The OSP scanner "ospd-ovaldi" is an example for such a remote scanner.

The current state of OSP-debsecan of course is Open Source licensed under GPLv2+ and available here:

https://wald.intevation.org/scm/viewvc.php/trunk/osp-servers/debsecan/?root=openvas

23.2.6 Adding some error handling

OSP offers to send error messages in case some problem occurred during the scan. Such messages will occur in the "Errors" section in the user interface.

The method to be used here is "add_scan_error" and it works analog to the "add_scan_alarm" method. Launching the external tool "debsecan" could fail, for example if it is not installed, so lets handle this in the method "exec_scan":

```
# run the debsecan command
try:
    result = subprocess.check_output(["debsecan"])
except:
    self.add_scan_error(scan_id, host=target,
      value="A problem occurred trying to execute 'debsecan'.")
    return
```

CHAPTER 24

Setup Guides

This chapter provides specific setup guides and trouble shooting for the different GSM appliances:

- *GSM ONE* (page 233)
- *GSM 25V* (page 237)
- *GSM 25* (page 239)
- *GSM 100* (page 241)
- *GSM 500/510/550* (page 243)
- *GSM 400/600/650* (page 245)
- *GSM 5300/6400* (page 247)

The general setup which is the same for all GSM appliance models is described in chapter *Setup* (page 9).

The setup is also explained in a video at http://docs.greenbone.net/Videos/gos-3.1/en/GSM-Setup-GOS-3.1-en-20150629.mp4.

24.1 GSM ONE

This setup guide will show the steps required to put the GSM ONE appliance in to operation. You can use the following checklist to monitor your progress.

Step	Done
VirtualBox 4.3 installed	
Integrity verification (optional)	
Import of the OVA	
Resources: 2 CPUs, 2GB Ram	
Keyboard layout	
IP address configuration	
DNS configuration	
Password change	
Web admin account	
SSL certificate	
Readiness	

24.1.1 Requirements

This section lists the requirements for the successful deployment of the GSM ONE appliance. Please ensure that all requirements are met.

Resources

The virtual appliance requires at least the following resources:

- 2 virtual CPUs
- 2 GB RAM

Supported Hypervisor

While the GSM ONE may be run on different hypervisors, only the following two hypervisors are currently supported:

- Oracle VirtualBox 4.3 on GNU/Linux
- Oracle VirtualBox 4.3 on Microsoft Windows

Verification of Integrity

The integrity of the virtual appliance may be verified. On request the Greenbone support provides an integrity checksum. To request the checksum please contact the Greenbone support via email (emailto:support@greenbone.net). Include your subscription number in the email. The integrity checksum may be provided via phone or via support portal at https://support.greenbone.net. Please specify the preferred channel in the email.

The local verification of the checksum depends on the host operating system.

On Linux systems use the following command to calculate the checksum:

```
sha256sum GSM-ONE-3.1.19-18-gsf201599999.ova
```

On Windows systems you first have to install an appropiate program. You may use rehash which can be found at http://rehash.sourceforge.net. To calculate the checksum, use:

```
rehash.exe -none -sha256 C:\<path>\GSM-ONE-3.1.19-18-gsf201599999.ova
```

If the checksum does not match the checksum provide by the Greenbone support the virtual appliance has been modified and should not be used.

Deployment

Each GSM ONE is activated using a unique subscription key. You may not clone the GSM ONE and use several instances in parallel. This may result in inconsistencies and unwanted side effects.

24.1.2 Importing of the Virtual Appliance

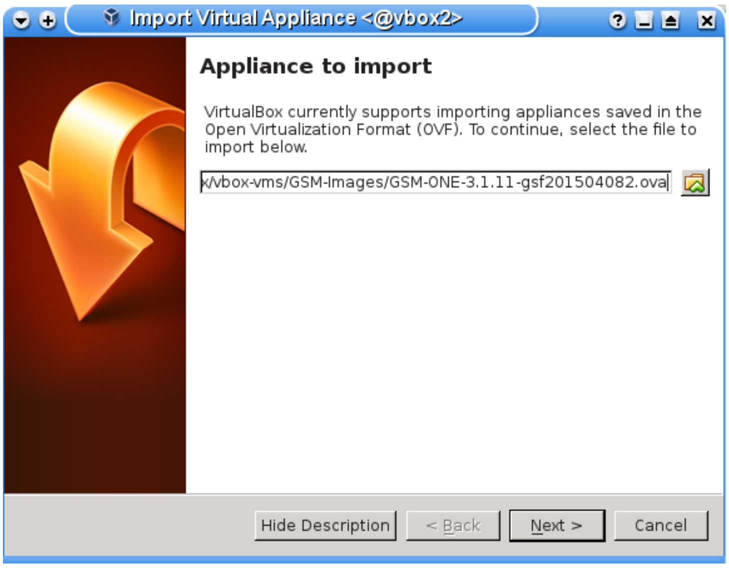
The virtual appliances are being provided by Greenbone in the Open Virtualization Appliance (OVA) format. These files are easily imported into VMWare or VirtualBox. The following scenarios are supported by Greenbone:

- GSM ONE: Oracle VirtualBox 4.3 (Linux and Microsoft Windows)
- GSM 25V: ESXi 5.1

Import into VirtualBox

Install Oracle VirtualBox for your operating system. VirtualBox is often included with Linux distributions. Should this not be the case and for the different versions of Microsoft Windows, VirtualBox is available directly from Oracle http://virtualbox.org/wiki/Downloads.

Once installed, start VirtualBox. Now you can import the OVA-file via *File -> Import Appliance* (see figure *Import of the OVA-Appliance* (page 235))



Appliance to import

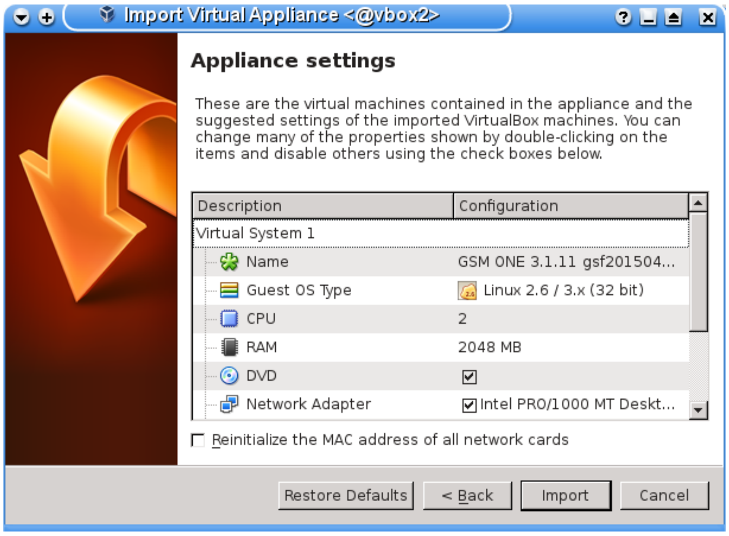
VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

x/vbox-vms/GSM-Images/GSM-ONE-3.1.11-gsf201504082.ova

Fig. 24.1: Import of the OVA-Appliance

Confirm the configuration of the virtual machine in the following window (see figure *Accepting the hardware configuration* (page 235)). If possible, select 4096 MB RAM (memory) for optimal configuration of the virtual appliance. Accept the remaining hardware settings.

The actual import can take up to 10 minutes. Once imported you can start the virtual appliance.



Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Description	Configuration
Virtual System 1	
Name	GSM ONE 3.1.11 gsf201504...
Guest OS Type	Linux 2.6 / 3.x (32 bit)
CPU	2
RAM	2048 MB
DVD	☑
Network Adapter	☑ Intel PRO/1000 MT Deskt...

□ Reinitialize the MAC address of all network cards

Fig. 24.2: Accepting the hardware configuration

General system setup

All GSM appliances share the same way of basic configuration and readiness check.

Please follow the steps described in chapter *Setup* (page 9) and then continue with the next sections for logging in or for troubleshooting.

24.1.3 Login to the Webinterface

The main interface of the GSM is the web gui. To access the web gui use a current web browser and access https://<ip-of-the-gsm>/.

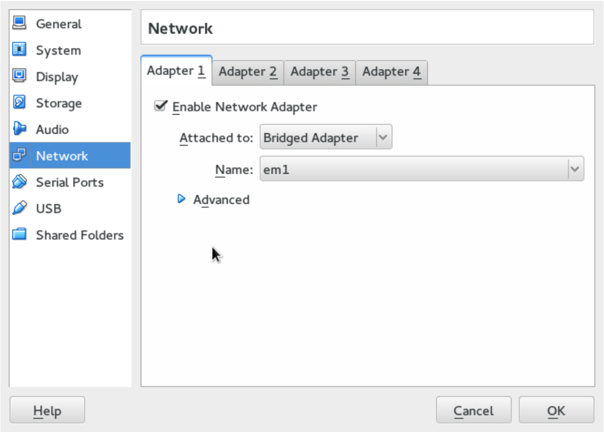
The IP address of the GSM is displayed at the login prompt of the console.

Login using the web admin you created during the setup.

24.1.4 GSM ONE troubleshooting

The following warnings and problems are known and depend on your environment:

- On Linux host systems VirtualBox may warn during the import that the Host-I/O-Cache is activated if the virtual image is stored on a xfs partition. This warning is expected and may be accepted.
- On Linux host systems the warning "Failed to attach the network LUN (VERR_INTNET_FLT_IF_NOT_FOUND)" is displayed if the the virtual machine does not discover any network card. The network card within the VirtualBox hypervisor needs to be configured. Usually the default can be accepted.



Network

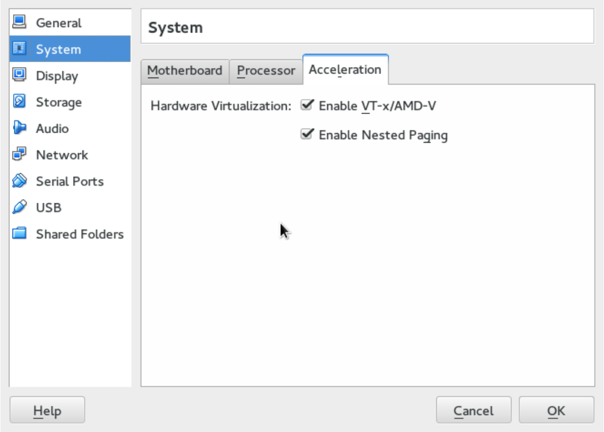
☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: em1

Fig. 24.3: Choose the correct network card in VirtualBox

- If the warning "AMD-V is disabled in the BIOS. (VERR_SVM_DISABLED)." is displayed, you need to enable the option "VT-X/AMD-V" in the BIOS of your host. An alternative solution is disabling of the acceleration in the system configuration of the virtual machine.



System

Hardware Virtualization: ☑ Enable VT-x/AMD-V

☑ Enable Nested Paging

Fig. 24.4: Disabling the hardware acceleration in VirtualBox

24.2 GSM 25V

This setup guide will show the steps required to put the GSM 25V virtual appliance in to operation. You can use the following checklist to monitor your progress.

Step	Done
VMware ESXi 5.1	
Import of the OVA	
Resources: 2 CPUs, 4GB Ram	
Keyboard layout	
IP address configuration	
DNS configuration	
Password change	
Scan user account	
SSL certificate	
Master key download	
Sensor setup on the master	
Readiness	

24.2.1 Requirements

This section lists the requirements for the successful deployment of the GSM 25V appliance. Please ensure that all requirements are met.

Resources

The virtual appliance requires at least the following resources:

- 2 virtual CPUs
- 4 GB RAM

Supported Hypervisor

The GSM 25V is only supported for the following hypervisor:

- VMware ESXi 5.1

Deployment

You will receive the GSM 25V as a VM image in OVA format. Usually the image does not include the latest updates and feeds. You will need to update and synchronize the current feed using the master GSM after deployment.

Each GSM 25V requires a unique subscription key. This key is not pre-installed nad needs to be installed manually before using the GSM 25V. You may not clone the GSM 25V and use several instances in parallel with the same subscription key. This may result in inconsistencies and unwanted side effects.

24.2.2 Importing of the Virtual Appliance

The virtual appliances are being provided by Greenbone in the Open Virtualization Appliance (OVA) format. These files are easily imported into VMWare or VirtualBox. The following scenarios are supported by Greenbone:

- GSM ONE: Oracle VirtualBox 4.3 (Linux and Microsoft Windows)

- GSM 25V: ESXi 5.1

Import into ESXi 5.1

Start the VMware ESXi 5.1 client.

- Now you can import the OVA-file via *File -> Deploy OVF Template* (see figure *Import of the OVA-Appliance* (page 238))

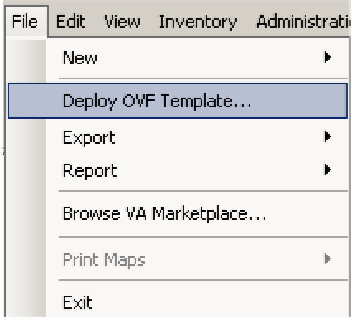
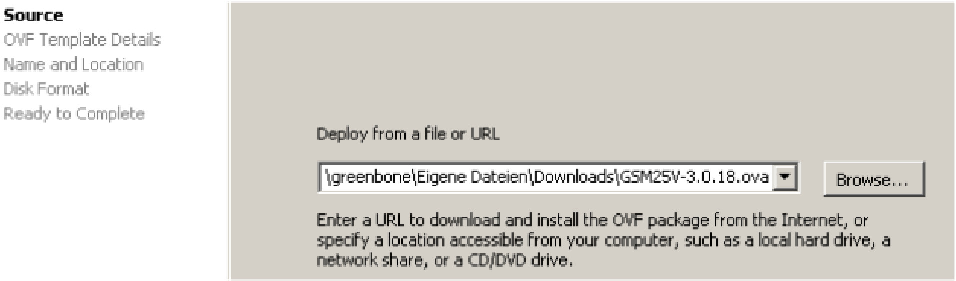


Fig. 24.5: Import of the OVA-Appliance

- Choose the appropiate OVA file (see figure *Specify the OVA file* (page 238)).



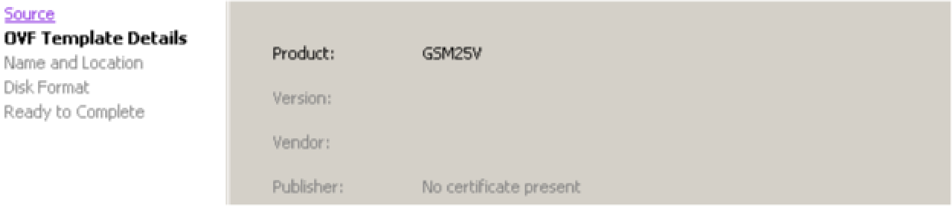
Deploy from a file or URL

\greenbone\Eigene Dateien\Downloads\GSM25V-3.0.18.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

Fig. 24.6: Specify the OVA file

- When displaying the OVF Template Details the product name GSM25V is displayed (see figure *Verify the correct product* (page 238)).



Product: GSM25V

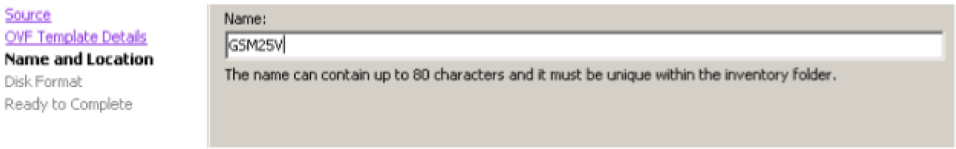
Version:

Vendor:

Publisher: No certificate present

Fig. 24.7: Verify the correct product

- Specify the name and the location of the VM image (see figure *Specify the name and the location of the VM image* (page 239)).
- Choose the disk format "Thin Provision Lazy Zeroed" (see figure *Choose the disk format.* (page 239)).
- Check all import settings and click "Finish" (see figure *Check all import settings.* (page 239)).
- Once the import is finished you may select power on the virtual appliance.

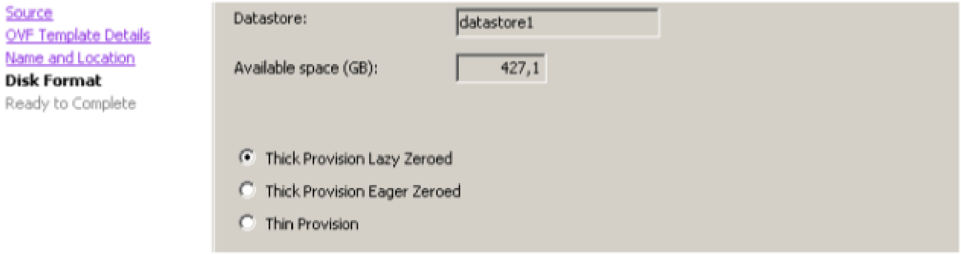


Source
OVF Template Details
Name and Location
Disk Format
Ready to Complete

Name:
GSM25V

The name can contain up to 80 characters and it must be unique within the inventory folder.

Fig. 24.8: Specify the name and the location of the VM image



Source
OVF Template Details
Name and Location
Disk Format
Ready to Complete

Datastore: datastore1

Available space (GB): 427,1

● Thick Provision Lazy Zeroed
○ Thick Provision Eager Zeroed
○ Thin Provision

Fig. 24.9: Choose the disk format.

General system setup

All GSM appliances share the same way of basic configuration and readiness check.

But being a sole sensor the GSM 25V differs in some steps from the other appliances:

- You do not add a web admin but a scan user account.
- You need to exchange the masterkey with the sensor.

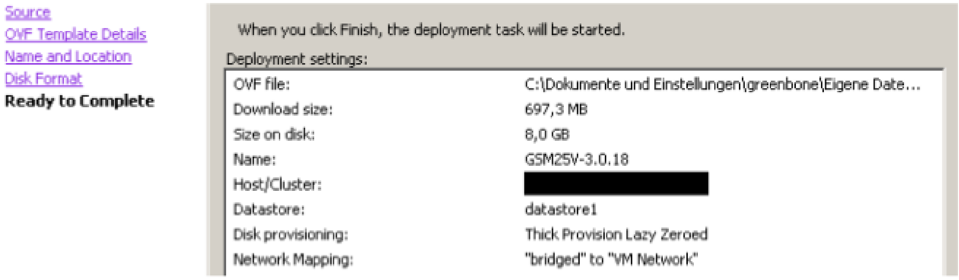
Please follow the steps described in chapter *Setup* (page 9). Please remember to add the scan user account instead of a web admin account and then continue with the section *Sensor* (page 204) to exchange the keys with the master.

The GSM 25V sensor does not offer any web interface. You can login to the sensor using the console and SSH from the master. The sensor is solely managed from the master.

If the communication between the master and the sensor fails, you might need to adjust the rule-set of any internal firewall governing the network connection.

24.3 GSM 25

This setup guide will show the steps required to put a GSM 25 sensor appliance in to operation. You can use the following checklist to monitor your progress.



Source
OVF Template Details
Name and Location
Disk Format
Ready to Complete

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\Dokumente und Einstellungen\greenbone\Eigene Date...
Download size:	697,3 MB
Size on disk:	8,0 GB
Name:	GSM25V-3.0.18
Host/Cluster:	[redacted]
Datastore:	datastore1
Disk provisioning:	Thick Provision Lazy Zeroed
Network Mapping:	"bridged" to "VM Network"

Fig. 24.10: Check all import settings.

Step	Done
Powersupply	
Serial console cable / USB converter	
Putty/Screen setup	
Keyboard layout	
IP address configuration	
DNS configuration	
Password change	
Scan user account	
SSL certificate	
Master key download	
Sensor setup on the master	
Readiness	

24.3.1 Installation

The appliance GSM 25 is 19" mountable and requires 1 rack unit (RU). The optional RACKMOUNT25 kit provides the racking brackets for installation in a 19" rack. For stand-alone operation you will find 4 self-sticking rubber pads to be mounted on the corresponding bottom side embossments.

For cabling the GSM 25 appliance has corresponding connectors at the back:

- **back:**
  - Power supply +12V DC (one), external power supply and suitable cable enclosed
  - Network access (LAN1)
  - RS-232 console port, suitable cable is enclosed
  - Reset button

For the installation you have to use a terminal application and a serial cable to establish a connection.

24.3.2 Serial Port

To utilize the serial port use the enclosed console cable. Alternatively you can use a blue Cisco console cable (rollover-cable).

Should your system not come with a serial port you will require a USB-to-Serial adapter. Ensure the use of a quality adapter. Many cheap adapters can cause errors with the serial protocol. Additionally such adapters might not be compatible with the drivers that come with Microsoft Windows operating systems.

To access the serial port you require a terminal application. The application needs to be configured to a speed of 9600 Bits/s (Baud).

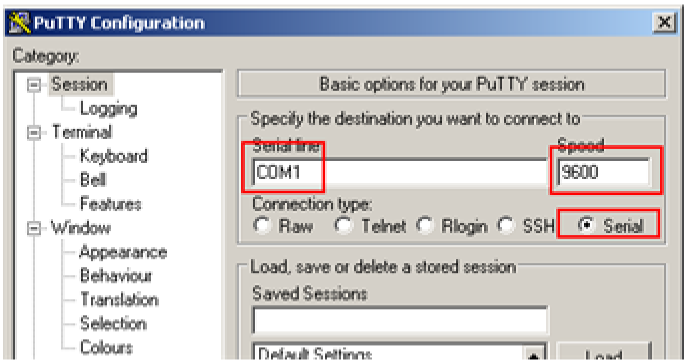
In Linux the command line command **screen** can be used. It is sufficient to run the command providing the serial port.

```
screen /dev/ttyS0   #(for serial port)
screen /dev/ttyUSB0 #(for USB adapter)
```

Sometimes it does not work with the first serial port. You have to experiment with the number (0, 1 or 2). You can quit the command by entering `CTRL-a \`. When starting the command it might be necessary to hit `RETURN` several times to get a command prompt.

In Windows you can use the Putty[147] application. After starting putty you will select the options as per Figure fig:putty-serial. Select the appropriate serial port also.

[147] http://www.chiark.greenend.org.uk/~sgtatham/putty/



Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM1

Speed: 9600

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Load

Fig. 24.11: Setting up the serial port in Putty

24.3.3 Startup

Once the appliance is fully wired and you are connected to the appliance via the console cable and have setup the terminal application (putty, screen or similar) you can power on the appliance. The appliance will boot and depending on the exact model the first messages will be displayed in the terminal application after a short time period.

General system setup

All GSM appliances share the same way of basic configuration and readiness check.

But being a sole sensor the GSM 25 differs in some steps from the other appliances:

- You do not add a web admin but a scan user account.
- You need to exchange the masterkey with the sensor.

Please follow the steps described in chapter *Setup* (page 9). Please remember to add the scan user account instead of a web admin account and then continue with the section *Sensor* (page 204) to exchange the keys with the master.

The GSM 25 sensor does not offer any web interface. You can login to the sensor using the console and SSH from the master. The sensor is solely managed from the master.

If the communication between the master and the sensor fails, you might need to adjust the rule-set of any internal firewall governing the network connection.

24.4 GSM 100

This setup guide will show the steps required to put a GSM 100 appliance in to operation. You can use the following checklist to monitor your progress.

Step	Done
Powersupply	
Serial console cable / USB converter	
Putty/Screen setup	
Keyboard layout	
IP address configuration	
DNS configuration	
Password change	
Web admin account	
SSL certificate	
Readiness	

24.4.1 Installation

The appliance GSM 100 is 19" mountable and requires 1 rack unit (RU). The optional RACKMOUNT100 kit provides the racking brackets for installation in a 19" rack. For stand-alone operation you will find 4 self-sticking rubber pads to be mounted on the corresponding bottom side embossments.

For cabling the GSM 100 appliance has corresponding connectors at the back:

- **back:**
  - Power supply +12V DC (one), external power supply and suitable cable enclosed
  - Network access (LAN1)
  - RS-232 console port, suitable cable is enclosed
  - Reset button

For the installation you have to use a terminal application and a serial cable to establish a connection.

24.4.2 Serial Port

To utilize the serial port use the enclosed console cable. Alternatively you can use a blue Cisco console cable (rollover-cable).

Should your system not come with a serial port you will require a USB-to-Serial adapter. Ensure the use of a quality adapter. Many cheap adapters can cause errors with the serial protocol. Additionally such adapters might not be compatible with the drivers that come with Microsoft Windows operating systems.

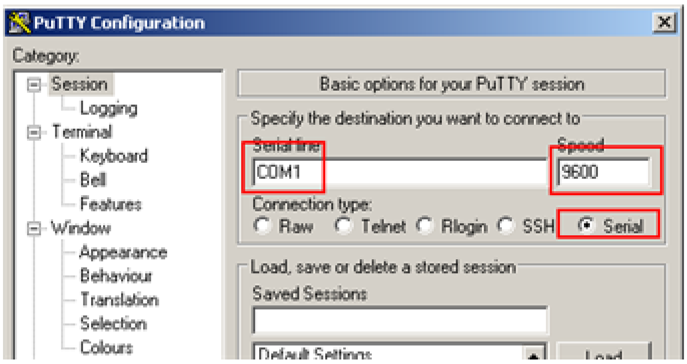
To access the serial port you require a terminal application. The application needs to be configured to a speed of 9600 Bits/s (Baud).

In Linux the command line command **screen** can be used. It is sufficient to run the command providing the serial port.

```
screen /dev/ttyS0   #(for serial port)
screen /dev/ttyUSB0 #(for USB adapter)
```

Sometimes it does not work with the first serial port. You have to experiment with the number (0, 1 or 2). You can quit the command by entering `CTRL-a \`. When starting the command it might be necessary to hit `RETURN` several times to get a command prompt.

In Windows you can use the Putty[148] application. After starting putty you will select the options as per Figure fig:putty-serial. Select the appropriate serial port also.



Serial line: COM1

Speed: 9600

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Saved Sessions

Default Settings

Fig. 24.12: Setting up the serial port in Putty

[148] http://www.chiark.greenend.org.uk/~sgtatham/putty/

24.4.3 Startup

Once the appliance is fully wired and you are connected to the appliance via the console cable and have setup the terminal application (putty, screen or similar) you can power on the appliance. The appliance will boot and depending on the exact model the first messages will be displayed in the terminal application after a short time period.

General system setup

All GSM appliances share the same way of basic configuration and readiness check.

Please follow the steps described in chapter *Setup* (page 9) and then continue with the next sections for logging in.

24.4.4 Login to the Webinterface

The main interface of the GSM is the web gui. To access the web gui use a current web browser and access https://<ip-of-the-gsm>/.

The IP address of the GSM is displayed at the login prompt of the console.

Login using the web admin you created during the setup.

24.5 GSM 500/510/550

This setup guide will show the steps required to put a GSM 500, 510 or 550 appliance in to operation. You can use the following checklist to monitor your progress.

Step	Done
Powersupply	
Serial console cable / USB converter	
Putty/Screen setup	
Firmware check (>= 2.0)	
Keyboard layout	
IP address configuration	
DNS configuration	
Password change	
Web admin account	
SSL certificate	
Readiness	

24.5.1 Installation

The appliances GSM 500, GSM 510 and GSM 550 are 19" mountable and require 1 rack unit (RU). For installation in a 19" this equipment comes with the respective racking brackets.

For cabling GSM 500, GSM 510 and GSM 550 appliances have corresponding connectors at the front and back:

- **back:**
    - Power supply (one)
    - VGA-monitor
    - Keyboard via USB
    - Serial Console

- **front**
  - Keyboard via USB
  - Network port eth0
  - RS-232 console port (|0|0|0), Cisco compatible, suitable cable is enclosed

For the installation you have to use a terminal application and a console cable to establish a connection.

24.5.2 Serial Port

To utilize the serial port use the enclosed console cable. Alternatively you can use a blue Cisco console cable (rollover-cable).

Should your system not come with a serial port you will require a USB-to-Serial adapter. Ensure the use of a quality adapter. Many cheap adapters can cause errors with the serial protocol. Additionally such adapters might not be compatible with the drivers that come with Microsoft Windows operating systems.

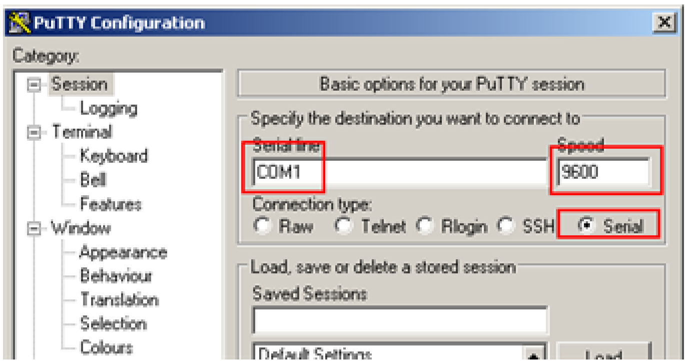
To access the serial port you require a terminal application. The application needs to be configured to a speed of 9600 Bits/s (Baud).

In Linux the command line command **screen** can be used. It is sufficient to run the command providing the serial port.

```
screen /dev/ttyS0   #(for serial port)
screen /dev/ttyUSB0 #(for USB adapter)
```

Sometimes it does not work with the first serial port. You have to experiment with the number (0, 1 or 2). You can quit the command by entering `CTRL-a \`. When starting the command it might be necessary to hit `RETURN` several times to get a command prompt.

In Windows you can use the Putty[149] application. After starting putty you will select the options as per Figure fig:putty-serial. Select the appropriate serial port also.



Serial line: COM1

Speed: 9600

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Fig. 24.13: Setting up the serial port in Putty

24.5.3 Startup

Once the appliance is fully wired and you are connected to the appliance via the console cable and have setup the terminal application (putty, screen or similar) you can power on the appliance. The appliance will boot and depending on the exact model the first messages will be displayed in the terminal application after a short time period.

[149] http://www.chiark.greenend.org.uk/~sgtatham/putty/

Firmware Notice

The appliances GSM 500, GSM 510 and GSM 550 are first generation devices. These devices were shipped with older firmware images which needs to be upgraded before the appliances are put into production. If the displayed flash version is < 2.0 please contact the Greenbone support (mailto:support@greenbone.net[150]) before continuing!

General system setup

All GSM appliances share the same way of basic configuration and readiness check.

Please follow the steps described in chapter *Setup* (page 9) and then continue with the next sections for logging in.

24.5.4 Login to the Webinterface

The main interface of the GSM is the web gui. To access the web gui use a current web browser and access https://<ip-of-the-gsm>/.

The IP address of the GSM is displayed at the login prompt of the console.

Login using the web admin you created during the setup.

24.6 GSM 400/600/650

This setup guide will show the steps required to put a GSM 400, 600 or 650 appliance in to operation. You can use the following checklist to monitor your progress.

Step	Done
Powersupply	
Serial console cable / USB converter	
Putty/Screen setup	
Keyboard layout	
IP address configuration	
DNS configuration	
Password change	
Web admin account	
SSL certificate	
Readiness	

24.6.1 Installation

The appliances GSM 400, GSM 600 and GSM 650 are 19" mountable and require 1 rack unit (RU). For installation in a 19" this equipment comes with the respective racking brackets.

For cabling GSM 400, GSM 600 and GSM 650 appliances have corresponding connectors at the front and back:

- **back:**
  - Power supply (one)
  - VGA-monitor
  - Keyboard via USB
  - Serial Console

[150] support@greenbone.net

- **front**
  - Keyboard via USB
  - Network port eth0
  - RS-232 console port (|O|O|O), Cisco compatible, suitable cable is enclosed

For the installation you have to use a terminal application and a console cable to establish a connection.

24.6.2 Serial Port

To utilize the serial port use the enclosed console cable. Alternatively you can use a blue Cisco console cable (rollover-cable).

Should your system not come with a serial port you will require a USB-to-Serial adapter. Ensure the use of a quality adapter. Many cheap adapters can cause errors with the serial protocol. Additionally such adapters might not be compatible with the drivers that come with Microsoft Windows operating systems.

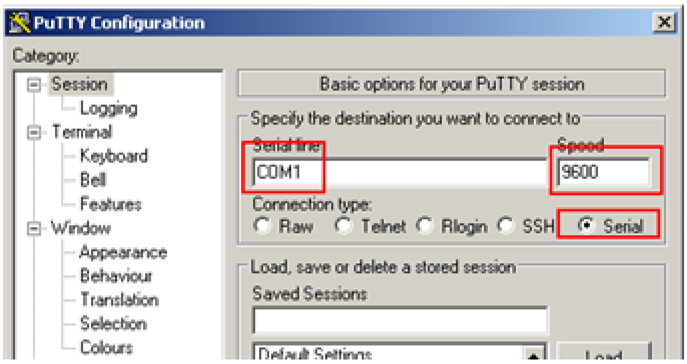
To access the serial port you require a terminal application. The application needs to be configured to a speed of 9600 Bits/s (Baud).

In Linux the command line command **screen** can be used. It is sufficient to run the command providing the serial port.

```
screen /dev/ttyS0   #(for serial port)
screen /dev/ttyUSB0 #(for USB adapter)
```

Sometimes it does not work with the first serial port. You have to experiment with the number (0, 1 or 2). You can quit the command by entering `CTRL-a \`. When starting the command it might be necessary to hit `RETURN` several times to get a command prompt.

In Windows you can use the Putty[151] application. After starting putty you will select the options as per Figure fig:putty-serial. Select the appropriate serial port also.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM1

Speed: 9600

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Fig. 24.14: Setting up the serial port in Putty

24.6.3 Startup

Once the appliance is fully wired and you are connected to the appliance via the console cable and have setup the terminal application (putty, screen or similar) you can power on the appliance. The appliance will boot and depending on the exact model the first messages will be displayed in the terminal application after a short time period.

[151] http://www.chiark.greenend.org.uk/~sgtatham/putty/

General system setup

All GSM appliances share the same way of basic configuration and readiness check.

Please follow the steps described in chapter *Setup* (page 9) and then continue with the next sections for logging in.

24.6.4 Login to the Webinterface

The main interface of the GSM is the web gui. To access the web gui use a current web browser and access https://<ip-of-the-gsm>/.

The IP address of the GSM is displayed at the login prompt of the console.

Login using the web admin you created during the setup.

24.7 GSM 5300/6400

This setup guide will show the steps required to put a GSM 5300 or 6400 appliance in to operation. You can use the following checklist to monitor your progress.

Step	Done
Powersupply (2 connectors)	
Serial console cable / USB converter	
Putty/Screen setup	
Keyboard layout	
IP address configuration	
DNS configuration	
Password change	
Web admin account	
SSL certificate	
Readiness	

24.7.1 Installation

The appliances GSM 5300 and GSM 6400 are 19" mountable and require 2 rack units (RU). For installation in a 19" this equipment comes with the respective racking brackets.

For cabling GSM 5300 and GSM 6400 appliances have corresponding connectors at the front and back:

- **back:**
  - Power supply (two)
  - VGA-monitor
- **front**
  - Keyboard via USB
  - Network port labeled “MGMT” (eth0)
  - RS-232 console port (|O|O|O), Cisco compatible, suitable cable is enclosed

For the installation you have to use a terminal application and a console cable to establish a connection.

24.7.2 Serial Port

To utilize the serial port use the enclosed console cable. Alternatively you can use a blue Cisco console cable (rollover-cable).

Should your system not come with a serial port you will require a USB-to-Serial adapter. Ensure the use of a quality adapter. Many cheap adapters can cause errors with the serial protocol. Additionally such adapters might not be compatible with the drivers that come with Microsoft Windows operating systems.

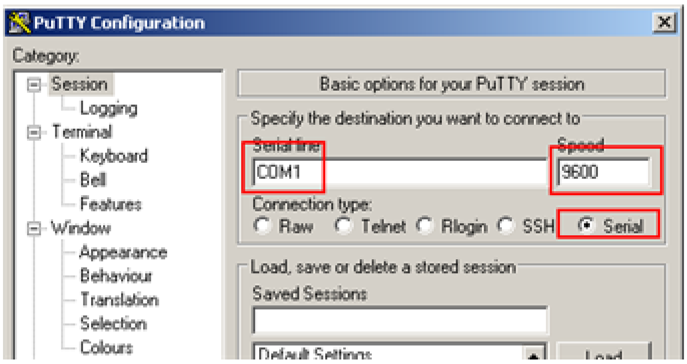
To access the serial port you require a terminal application. The application needs to be configured to a speed of 9600 Bits/s (Baud).

In Linux the command line command **screen** can be used. It is sufficient to run the command providing the serial port.

```
screen /dev/ttyS0   #(for serial port)
screen /dev/ttyUSB0 #(for USB adapter)
```

Sometimes it does not work with the first serial port. You have to experiment with the number (0, 1 or 2). You can quit the command by entering `CTRL-a \`. When starting the command it might be necessary to hit `RETURN` several times to get a command prompt.

In Windows you can use the Putty[152] application. After starting putty you will select the options as per Figure fig:putty-serial. Select the appropriate serial port also.



Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM1

Speed: 9600

Connection type:
○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Fig. 24.15: Setting up the serial port in Putty

24.7.3 Startup

Once the appliance is fully wired and you are connected to the appliance via the console cable and have setup the terminal application (putty, screen or similar) you can power on the appliance. The appliance will boot and depending on the exact model the first messages will be displayed in the terminal application after a short time period.

General system setup

All GSM appliances share the same way of basic configuration and readiness check.

Please follow the steps described in chapter *Setup* (page 9) and then continue with the next sections for logging in.

[152] http://www.chiark.greenend.org.uk/~sgtatham/putty/

24.7.4 Login to the Webinterface

The main interface of the GSM is the web gui. To access the web gui use a current web browser and access https://<ip-of-the-gsm>/.

The IP address of the GSM is displayed at the login prompt of the console.

Login using the web admin you created during the setup.

CHAPTER 25

CLI Command Reference

This chapter lists all the commands in alphabetical order. For each command there is a short description and reference to sections where the command is discussed in more detail.

addadmin With this command a web/scan administrator can be created. The command expects a user name and a password separated by a colon (see section *Creating a web administrator (scan administrator)* (page 19)).

certdownload With this command a key and a CA signed certificate can be copied to the GSM (see section *Certificate by an external certificate authority* (page 21)).

commit Not yet activated changes can be confirmed (see section *Configuring settings* (page 17)).

ethtool The command `ethtool` displays the current status of the network adapters including link status (see section *Monitoring and debugging of network functions* (page 33)).

exit Log out of the command line.

feedstartsync Starts the feedsynchronization from the command line (see section *Feed Synchronization* (page 31)).

feedsyncstatus This controls whether at this moment a synchronization is performed (see section *Feed Synchronization* (page 31)).

feedversion This command displays the current version. It shows the date and time, i.e. 201502090646 is 6:46 am on February 9th, 2015 (see section *Feed Synchronization* (page 31)).

gbfw This is a frontend for the local Greenbone firewall and only meant for experts.

getip This command displays the current IP configuration (see section *Monitoring and debugging of network functions* (page 33)).

getroute This command displays the current IP routing configuration (see section *Monitoring and debugging of network functions* (page 33)).

getusers This command displays the currently in the command line logged in users.

gos-admin-menu This command starts the GOS-Admin-Menu (see section *Base configuration* (page 10)).

gsmuser This is an alternate command for the user management.

ip This command displays various information about the network configuration (see section *Monitoring and debugging of network functions* (page 33)).

ldapcacertdownload This command allows to save the certificate of the LDAP server on the GSM (see section *LDAP with SSL/TLS* (page 176)).

masterkeydownload Saves the master key on a slave (see chapter *Master and Slave Setup* (page 203)).

ntpq This command displays the time synchronization of the system with external sources (see section *Network Time Protocol* (page 24)).

passwd This allows a user to change their password from the command line (see section *Admin password change* (page 18)).

ps Displays the currently running processes. To see all processes use **ps ef**.

reboot Initiate the reboot of the appliance from the command line (see section *Reboot and shutdown of the appliance* (page 22)).

rollback Discard the changes before a commit (see section *Configuring settings* (page 17)).

shell After logging in as admin you will work in a restricted shell. With this command you can run a complete UNIX shell from the command line.

show This command displays individual files or a schedule (see section *Activation key* (page 14)).

shutdown Initiate the shutdown of the appliance from the command line (see section *Reboot and shutdown of the appliance* (page 22)).

softwarestartsync Start of the synchronization of system upgrades (see section *Upgrade* (page 39)).

softwaresyncstatus Check the status of the synchronization of system upgrades (see section *Upgrade* (page 39)).

softwareversion Display the current software version (see section *Upgrade* (page 39)).

sslcatkey This command displays the certificate signing request for a certificate to be signed (see section *Certificate by an external certificate authority* (page 21)).

sslcatreq This command, like `sslcatkey`, displays the certificate signing request for a certificate to be signed (see section *Certificate by an external certificate authority* (page 21)).

sslcatself This command displays the self-signed certificate created by the GSM (see section *Self-signed certificates* (page 20)).

sslcheck This command checks the certificate chain of certificates which were issued by a trust center (see section *Certificate by an external certificate authority* (page 21)).

ssldownload With this command the CA signed certificate resulting from a certificate signing request can be copied to the GSM (see section *Certificate by an external certificate authority* (page 21) and `sslreq`).

sslreq Initiate the creation of a certificate signing request (see section *Certificate by an external certificate authority* (page 21)).

sslselfsign Initiate the creation of a self-signed certificate by the GSM (see section *Self-signed certificates* (page 20)).

subscriptiondownload Download the activation key to the GSM (see section *Activation key* (page 14)).

systembackup Start a backup of the system (see section *Backup and Restore* (page 43)).

systembackupstatus Display the status of a backup of the system (see section *Backup and Restore* (page 43)).

systemfeedbackup Start the backup of the feed (see section *Backup and Restore* (page 43)).

systemfeedbackupstatus Display the status of a backup of the feed (see section *Backup and Restore* (page 43)).

systemrecoverybackup Perform a restore (see section *Backup and Restore* (page 43)).

systemrecoverybackupstatus Display the status of a restore (see section *Backup and Restore* (page 43)).

systemrecoverysnapshot Perform a restore of a snapshot (see section *Snapshot of the System* (page 44)).

systemrecoverysnapshotstatus Display the status of a restore of a snapshot (see section *Snapshot of the System* (page 44)).

`systemsnapshot` Create a system snapshot (see section *Snapshot of the System* (page 44)).

`systemsnapshotstatus` Display the status of a system snapshot (see section *Snapshot of the System* (page 44)).

`systemupgrade` Start an upgrade (see section *Upgrade* (page 39)).

`systemupgradestatus` Display the status of an upgrade (see section *Upgrade* (page 39)).

`systemuserdatabackup` Perform the backup of user data (see section *Backup of User Data via USB-Stick* (page 45)).

`systemuserdatabackupstatus` Display the status of the backup of user data (see section *Backup of User Data via USB-Stick* (page 45)).

CHAPTER 26

CLI Configuration Reference

This chapter lists all settings in alphabetical order. For each setting there is a short description and reference to sections where the setting is discussed in more detail.

address_ethX_ipv4 IPv4 address of the network adapter Ehernet-X with netmask. Alternatively the value dhcp could be set. Depending on the appliance X can have a value between 0 and 19. See section *IP Addresses* (page 24). Entering an IPv4 address for network adapter Ethernet-0 in mandatory all other IP addresses are optional.

address_ethX_ipv6 This is the IPv6 address for adapter Ethernet-X. See section *IP Addresses* (page 24). The setting is optional.

airgap Default: `disabled` This is the role in a airgap synchronization scenario. Possible Values are: `disabled`, `master` or `slave`. See section *Airgap Update* (page 48).

airgap_ftp_location Default: not set This is the address of the ftp server for the airgap synchronization. Hereby a directory can be included as well (for example: your.ftp.server/subdirectory). See section *Airgap Update* (page 48).

airgap_ftp_password Default: not set This is the password that is being used when logging into the ftp server for the airgap functionality. See section *Airgap Update* (page 48).

airgap_ftp_user Default: not set This is the user that is being used when logging into the ftp server for the airgap functionality. See section *Airgap Update* (page 48).

airgap_type Default: `usb` This is the airgap method. Possible values are `ftp` and `usb`. See section *Airgap Update* (page 48).

autoslavesync Default: `disabled` This variable decides if slaves are being supplied with the NVT feeds from the master automatically using the push method. See chapter *Master and Slave Setup* (page 203).

default_route_ipv4 Default: not set This is the default route for IPv4. By default the system is configured via DHCP. Then the default route is also being set via DHCP. See section *Default Gateway* (page 24). This setting is optional.

dns1 Default: `8.8.8.8` This is the first namserver that is being used by the GSM. If this namserver is not available the second one will be used. Only an IPV4 address is allowed for this value. IPv6 nameservers are not yet supported. The default value is a Google server. See section *DNS server* (page 23).

dns2 Default: `8.8.4.4` This is the second namserver that is being used by the GSM. This setting is optional. If this namserver is not available the third one will be used. Only an IPV4 address is allowed for this value. IPv6 nameservers are not yet supported. The default value is a Google server. See section *DNS server* (page 23).

dns3 Default: not set This is the third namserver that is being used by the GSM. This setting is optional. If this namserver is not available a name resolution is not possible. Only an IPV4 address is allowed for this value. IPv6 nameservers are not yet supported. See section *DNS server* (page 23).

domainname Default: `Greenbone.net` This is the domain of the appliance. By prepending the hostname you get the fully qualified name of the appliance. See section *domainname* (page 23).

fancontrol Default: `enabled` This controls the fan behaviour. If this functionality is enabled the fan will only be activated on demand. Possible values are `enabled` and `disabled`. See section *domainname* (page 23).

feedfrommaster Default: `disabled` This variable defines if the slave expects and accepts feeds from the master. Possible values are `enabled` and `disabled`. See chapter *Master and Slave Setup* (page 203).

feedsync Default: `enabled` This variable defines if synchronization with the Greenbone Security Feed should occur. Possible values are `enabled` and `disabled`. See section *Feed Synchronization* (page 31).

guest_login Default: `disabled` This variable enables or disables the guest access for the web interface. Possible values are `enabled` and `disabled`. See section *Guest Log in* (page 168).

guest_password Default: not set This variable defines the password for the guest access. See section *Guest Log in* (page 168).

guest_user Default: not set This variable defines the user name for the guest access. See section *Guest Log in* (page 168).

hostname Default: `gsm` This is the host name of the appliance. By appending the domain name you get the fully qualified name of the appliance. See section *hostname* (page 23).

ifadm Default: `all` This is the network adapter through which the web interface and SSH interface are allowed to be accessed. Possible values are *all* or the specific network adapter (i.e. *eth0*). See section *Management Adapter* (page 12).

ipv6support Default: `enabled` With this variable IPv6 support can be enabled and disabled. If IPv6 support is enabled the GSM creates Link-Local IPV6 addresses. Possible values are `enabled` and `disabled`. See section *IP Addresses* (page 24).

keyboard_layout Default: `DE` This configures the keyboard layout for the CLI interface. Possible values are `DE`, `ES`, `FR`, `IT`, `PL`, `SE`, `UK` and `US`. See section *Keyboard layout* (page 10).

mailhub Default: `mail.example.com` The GSM can send emails with reports for example. For this the mailserver specified in this variable is used. The value should be a fully qualified DNS name. See section *Mail Server* (page 25).

netmode Default: `default` Selects the network configuration mode. Possible values are *enabled* and *expert*. See section *Expert Network Configuration* (page 27).

ntp_server1 This is the first NTPv5 time server. As a value an IPv4 address is expected. See section *Network Time Protocol* (page 24).

ntp_server2 This is the second NTPv5 time server. This setting is optional See section *Network Time Protocol* (page 24).

omp_ciphers Default:

`SECURE128:-AES-128-CBC:-CAMELLIA-128-CBC:-VERS-SSL3.0:-VERS-TLS1.0` Selects the TLS cipher supported by OMP. The syntax of this cipher priority string is the one of "GNUTLS" and documented here: http://gnutls.org/manual/html_node/Priority-Strings.html . See section *OpenVAS Management Protocol (OMP)* (page 30).

proxy_credentials Default: not set The GSM can receive its feeds through an http proxy. If the proxy expects an authentication then with this variable the username and password can be stored (username:password). See section *Proxy configuration* (page 31).

proxy_feed Default: not set The GSM can receive its GOS updates and feeds through an http proxy. Here the proxy for receiving the updates and feeds can be set. See section *Proxy configuration* (page 31).

public_omp Default: `disabled` Enables or disables OMP access to port 9390. Here the proxy for receiving the updates can be set. See section *OpenVAS Management Protocol (OMP)* (page 30).

selfsigssl Default: `disabled` This setting allows for the creation and use of self-signed certificates for the authentication of the GSM. See section *Self-signed certificates* (page 20).

sensors Default: not set This is a list of the sensors managed by the GSM. The list is separated by spaces. See section *Sensor* (page 204).

snmp Default: `disabled` This setting allows remote access via SNMPv3. See section *SNMP* (page 26).

snmp_contact Default: `Greenbone_Unspecified_contact` This is the contact specified in the SNMP output. See section *SNMP* (page 26).

snmp_key Default: not set The privacy password for SNMPv3 requests. The password must be at least 8 characters See section *SNMP* (page 26).

snmp_location Default: `Hildesheim` This is specified in the SNMP output place. See section *SNMP* (page 26).

snmp_password Default: not set This is the authentication password for SNMPv3 requests. The password must be at least 8 characters long. See section *SNMP* (page 26).

snmp_trap Default: `disabled` With this setting sending of SNMP traps can be activated. See section *SNMP* (page 26).

snmp_trapcommunity Default: `public` This defines the community string for SNMP traps. See section *SNMP* (page 26).

snmp_trapreceiver Default: `192.168.0.1` This defines the receiver for SNMP traps. See section *SNMP* (page 26).

snmp_user Default: not set This is the user name for SNMPv3 requests. See section *SNMP* (page 26).

ssh Default: `disabled` This is the status of the SSH server. Possible values are *enabled* and *disabled*. See section *SSH Access* (page 30).

superuser Default: `disabled` This activates the superuser access via SSH for debugging purposes. Possible values are `enabled` and `disabled`. See section *Superuser* (page 19).

superuserpassword Default: `disabled` When the superuser was activated the password can be set with this variable. Possible values are `disabled` or an 8 character long password. See section *Superuser* (page 19).

syncport Default: `24` This is the port for the synchronization with the Greenbone Security Feed. Possible values are `24` or `443`. See section *Feed Synchronization* (page 31).

synctime Default: `06:25` This is the time for the daily synchronization with the Greenbone Security Feed. The format is entered in HH:MM in the UTC time zone. The synchronization is not possible between 10:00 (10 am) and 13:00 (1pm). See section *Feed Synchronization* (page 31).

syslog_server1 Default: not set This is the first syslog server. See section *Central Logging Server* (page 25).

syslog_server2 Default: not set This is the second syslog server. See section *Central Logging Server* (page 25).

web_ciphers Default:

`SECURE128:-AES-128-CBC:-CAMELLIA-128-CBC:-VERS-SSL3.0:-VERS-TLS1.0` Select the supported SSL/TLS cipher. See section *Central Logging Server* (page 25).

web_interface Default: `classic` This is the default web interface. See chapter Alternate User Interfaces (page 161).

webtimeout Default: `15` This is the default timeout for HTTPS browser sessions in minutes. See section *HTTPS Timeout* (page 30).

CHAPTER 27

Frequently Asked Questions

This section collects frequently asked questions with answers.

27.1 What is the difference between a scan sensor and a scan slave?

A scan slave is controlled by a scan master for doing vulnerability scans. Scans for scan slaves are configure on the scan master by each user as needed and permitted. GSM's from midrange upward can act as a master and control one or many scan slaves. Any GSM can act as a scan slave. Any scan slave has to take care on its own to update the feed and release.

A scan sensor is a GSM that solely works as scan slave but is also fully managed by the master unit. This management includes automatic feed and release updates. Essentially, a sensor does not require any other connection than to its master and, once installed, does not require any administrative works.

27.2 Scan process very slow

The performance of a scan depends on various aspects.

- Several port scanners were activated concurrently.

  If your are using a individual Scan Config please take care to select only a single port scanner in the family "Port Scanner". Of course "Ping Host" can still be activated.

- Unused IP addresses are scanned very time-consuming.

  In a first phase for each IP address it is detected whether a active system is present. In case it is not, this IP will not be scanned. Firewalls and other systems can prevent a successful detection. The NVT "Ping Host" (1.3.6.1.4.1.25623.1.0.100315) offers to fine-tune detection.

27.3 Scan triggers alarm at other security tools

For many vulnerability tests the behaviour of real attacks is applied. Even though a real attack does not happen, some security tools will issue an alarm.

Known examples are:

- Symantec reports attack regarding CVE-2009-3103 if the NVT "Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution Vulnerability" (1.3.6.1.4.1.25623.1.0.100283) is executed. This NVT is only executed if "safe checks" is explicitly disabled in the Scan Configuration because it can affect the target system.

27.4 On scanned target systems appears a VNC dialog

When testing port 5900 or configured VNC port, a window appears on scanned target system that asks the user whether to allow the connection. This was observed for UltraVNC Version 1.0.2.

Solution: Exclude port 5900 or other configured VNC port from target specification. Alternatively upgrade to a newer version of UltraVNC would help (UltraVNC 1.0.9.6.1 only uses balloons to inform users).

27.5 After Factory Reset neither Feed-Update nor System-Upgrade works

(This is not relevant for virtual appliances where no factory reset is integrated anyway)

A Factory Reset deletes the whole system including the subscription key. The key is mandatory for Feed-Update and System-Upgrade.

1. Reactivate subscription key:

   A backup key is delivered with each GSM appliance, usually stored on a USB Stick and labelled with the key ID. Use this key to reactivate the GSM. The activation is described in the SetUp Guide of the respective GSM type.

2. Update system to current version:

   Depending on the age of the factors emergency system you now need to execute the respective upgrade procedure.

CHAPTER 28

Glossary

This section defines relevant terminology which is consistently used across the entire system.

28.1 Host

A Host is a single system that is connected to a computer network and that may be scanned. One or many hosts form the basis of a scan target.

A host is also an asset type. Any scanned or discovered host can be recorded in the asset database.

Hosts in scan targets and in scan reports are identified by their network address, either an IP address or a hostname.

28.2 Quality of Detection (QoD)

The Quality of Detection (QoD) is a value between 0% and 100% describing the reliability of the executed vulnerability detection or product detection.

This concept also solves the challenge of potential vulnerabilities. Such are always recorded and kept in the results database but are only visible on demand.

While the QoD range allows to express the quality quite fine-grained, in fact most of the test routines use a standard methodology. Therefore QoD Types are associate with a QoD value. The current list of types might be extended over time.

QoD	QoD Type	Description
100%	exploit	The detection happened via an exploit and therefore is fully verified.
99%	remote_vul	Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerability.
98%	remote_app	Remote active checks (code execution, traversal attack, sql injection etc.) where the response clearly shows the presence of the vulnerable application.
97%	package	Authenticated package-based checks for Linux(oid) systems.
97%	registry	Authenticated registry-based checks for Windows systems.
95%	remote_active	Remote active checks (code execution, traversal attack, sql injection etc.) where the response shows the likely presence of the vulnerable application or of the vulnerability. "Likely" means that only rare circumstances are possible where the detection would be wrong.
80%	remote_banner	Remote banner check of applications that offer patch level in version. Many proprietary products do so.
80%	executable_version	Authenticated executable version checks for Linux(oid) or Windows systems where applications offer patch level in version.
75%		This value was assigned to any pre-qod results during system migration. However, some NVTs eventually might own this value for some reason.
70%	remote_analysis	Remote checks that do some analysis but which are not always fully reliable.
50%	remote_probe	Remote checks where intermediate systems such as firewalls might pretend correct detection so that it is actually not clear whether the application itself answered. This can happen for example for non-TLS connections.
30%	remote_banner_unreliable	Remote banner checks of applications that don't offer patch level in version identification. For example, this is the case for many Open Source products due to backport patches.
30%	executable_version_unreliable	Authenticated executable version checks for Linux(oid) systems where applications don't offer patch level in version identification.
1%	general_note	General note on potential vulnerability without finding any present application.

The value of 70% is the default minimum used for the default filtering to display the results in the reports.

28.3 Severity

The Severity is a value between 0.0 (no severity) and 10.0 (highest severity) and expresses also a Severity Class (None, Low, Medium or High).

This concept is based on CVSS but is applied also where no full CVSS Base Vector is available. For example, arbitrary values in that range are applied for Overrides and used by OSP scanners even without a vector definition.

Comparison, weighting, priorisation is possible of any scan results or NVTs because the severity concept is strictly applied across the entire system. Not a single severity is just expressed as "High" for example. Any new NVT is assigned with a full CVSS vector even if CVE does not offer one and any results of OSP scanners is assigned a adequate severity value even if the respective scanner uses a different severity scheme.

The severity classes None, Low, Medium and High are defined by sub-ranges of the main range 0.0-10.0. Users can select to use different classifications. The default is the NVD classification which is the most commonly used one.

Scan results are assigned a severity while achieved. The severity of the related NVT may change over time though. Users can select Dynamic Severity to let the system always use the most current severity of NVTs for the results.

28.4 Solution Type

This information shows possible solutions for the remediation of the vulnerability. Currently three different variants are available:

- Workaround: Information is available about a configuration or specific deployment scenario that can be used to avoid exposure to the vulnerability. There may be none, one, or more workarounds available. This is typically the "first line of defense" against a new vulnerability before a mitigation or vendor fix has been issued or even discovered.
- Mitigation: Information is available about a configuration or deployment scenario that helps to reduce the risk of the vulnerability but that does not resolve the vulnerability on the affected product. Mitigations may include using devices or access controls external to the affected product. Mitigations may or may not be issued by the original author of the affected product, and they may or may not be officially sanctioned by the document producer.
- Vendor-Fix: Information is available about an official fix that is issued by the original author of the affected product. Unless otherwise noted, it is assumed that this fix fully resolves the vulnerability.
- None-Available: Currently there is no fix available. Information should contain details about why there is no fix.
- WillNotFix: There is no fix for the vulnerability and there never will be one. This is often the case when a product has been orphaned, end-of-lifed, or otherwise deprecated. Information should contain details about why there will be no fix issued.