Tenable Tools for Security Compliance – The Antivirus Challenge

January 20, 2005
(Updated February 7, 2007)

Nicolas Pouvesle / John Lampe

Table of Contents

Introduction

Worms and viruses, devastating in the 90's, have gained momentum in the last few years and are arguably the largest risk to many companies. As such, antivirus products are a staple part of any Corporate Security policy. The antivirus client has become as common on the desktop as the web browser; however, the story does not end there. What does a company do after the antivirus deployment is complete? How does a company ensure that the antivirus client is actually running and protecting as advertised? When is the right time to update? Where are updates coming from? How does a company protect its network from roving computers, remote access connections? Etc. This paper will address some of the flaws with current antivirus management policies and show how these flaws can be addressed with Tenable's products: Security Center, Nessus Vulnerability Scanner and Passive Vulnerability Scanner.

What's Wrong with my Current Architecture?

Antivirus is typically deployed in a layered architecture. That is, a typical company will scan for viruses at:

- The edge of the network (SMTP server, Proxy, etc.)
- The Core of the network (internal servers)
- The desktop

In addition, the typical antivirus "Enterprise" solution will utilize central servers which maintain the latest antivirus signatures. In the typical setup, the clients come on line and locate their Enterprise antivirus server. The client will check for updates and, if required, install updates and possibly reboot. The Security Administrators can monitor these central servers for statistics and reports. In most instances, the Central Enterprise server can also remotely administer and install software on the remote clients.

Problems

- Rogue clients. A rogue client is one that is either not running antivirus software, running non-standard antivirus software, or is not enrolled with the central antivirus servers. Such rogue clients introduce a risk to the computing environment. Any large network will have rogue clients. Some common rogue clients are:
    - Visitors.
    - Servers. Sadly, many administrators still view Antivirus technologies as immature and do not want to risk performance degradation on critical servers. In addition, many administrators think that they are risk-free if they are not browsing the web or receiving email on the server. Of course, with more sophisticated viruses and multiple attack vectors, these critical servers often fall prone to malcode attacks.
    - Remote access Users. These users dial or VPN into the corporate network. If they were previously infected with a virus, suddenly they are propagating the virus inside the corporate network.
- Single points of failure. Many architectures rely on a central antivirus server managing many clients. If the architecture does not allow for multiple points of graceful fail over (i.e.: If the client cannot reach server "A", there should be a

contingency plan for server “B” and “C”, etc.), then a server failure results in a client that must survive without updates for some period of time.

- Version control anomalies. It is a risk if the antivirus software is not running with the most recent signatures. An antivirus product is only as good as the latest signature release.
- Network Blind Spots. As networks are acquired, merged, re-allocated, etc. it is a reality that certain network segments may become invisible to the central Antivirus servers. As this occurs, these networks and clients become High Risk. Often, companies do not realize these “blind spots” until there is an outbreak which impacts the Enterprise.
- Multiple Console Apathy. In a layered environment it is not uncommon for a company to be running with many different antivirus solutions and/or versions. Differing versions of antivirus will have separate consoles. As the number of consoles grows the ability of the security staff to adequately monitor each of the consoles decreases. Furthermore, without a comprehensive console to check all clients, it becomes quite complex merging console reports to determine where coverage may be lacking. In large and complex computing environments, there is a diffusion of responsibility regarding antivirus coverage (i.e.: Administrator X is not monitoring Server Y but assumes that some other antivirus product or administrator is covering it). Typically, these cracks in the antivirus architecture do not become known until an outbreak occurs.

Using Tenable’s Products to Ensure Antivirus Compliance

Tenable Network Security, Inc. is the author and manager of the Nessus Security Scanner which is available from http://www.nessus.org/. In addition to constantly improving the Nessus engine, Tenable is in charge of writing most of the plugins available to the scanner. Nessus is available for Unix, Windows and OS X operation systems. The Passive Vulnerability Scanner, also offered by Tenable Network Security, Inc., is a scanner which detects vulnerabilities without having to actively generate any network traffic.

The Nessus Vulnerability Scanner performs many security checks for the hosts it tests and these checks are written predominantly in a language named NASL. This stands for the Nessus Attack Scripting Language. The checks are often referred to as “plugins” or Nessus modules. Security Center is a central console for the Nessus Vulnerability Scanner and the Passive Vulnerability Scanner which handles plugin updates, event storage, correlation, and much more.

How do Tenable’s Security Center, Nessus Vulnerability Scanner and Passive Vulnerability Scanner deal with these problems?

- Rogue clients. Tenable’s Nessus Vulnerability Scanner can be configured to automatically scan ranges or network segments. Critical networks (Extranets, DMZ, etc.) can be scheduled for routine Policy scans. A policy scan can be defined within the Security Center and typically only includes a small subset of the 5,000+ Tenable Plugins. For example, a company may wish to scan all critical servers on a daily basis in order to ensure that the latest antivirus signatures are being run. In 2004, Jeff Adams contributed two Nessus plugins which check for the existence and version of McAfee and Norton antivirus. Since then, Tenable has rewritten and expanded upon these checks. Specifically, the latest edition of Tenable’s Nessus Vulnerability Scanner includes a check for Trend Micro antivirus as well as a generic check to determine if any antivirus is running on the remote client. With these checks and the existing Nessus architecture, security administrators can now look through domains and ranges for rogue hosts. Deploying the Passive Vulnerability Scanner on critical network junctions ensures that you maintain an up-to-date map of your network. With the Passive Vulnerability Scanner, new hosts or networks can be discovered in real time. These new hosts or networks can then be passed to the Nessus Vulnerability Scanner for an Antivirus compliance check. **Note: See the example below for a more detailed case study.**

- Single points of failure. As mentioned above, Tenable's Nessus Vulnerability Scanner discovers machines on a network and then scans those machines for antivirus. If an Antivirus Server goes offline and the clients are not running the latest signatures, the Nessus Vulnerability Scanner can be used to find these machines. In addition, the Nessus Vulnerability Scanner checks can be easily extended to check for machines which are running antivirus but are not communicating with a central Antivirus Server. **See the example below for a more detailed case study.**

- Version control anomalies. Tenable's Security Center can be configured to automatically download new Nessus Plugins. Tenable Network Security, Inc. maintains a list of the most recent signature files for the major Antivirus vendors. As new antivirus updates are made available, Tenable releases a modified Nessus plugin which checks for the most recent version.

- Network Blind Spot. Deploying the Passive Vulnerability Scanner on critical network junctions ensures that you maintain an up-to-date map of your network. With the Passive Vulnerability Scanner, new hosts or networks can be discovered in real time. These new hosts or networks can then be passed to the Nessus Vulnerability Scanner for an Antivirus compliance check.

- Multiple Console Apathy. Tenable's Nessus Vulnerability Scanner ships with a generic Antivirus check which looks for some of the top Antivirus solutions. In addition, a company can easily extend the checks to include any antivirus solution. **See the example below for a more detailed example.**

Existing Antivirus Plugins

Each of the following plugins is dedicated to finding and reporting on Antivirus configuration on remote systems. A plugin denoted as "GPL" means that it is available to the general public. A plugin denoted as "non-GPL" means that the plugin is not available to the general public.

- nav_installed.nasl. Originally written by Jeff Adams and later rewritten by Tenable Network Security, Inc., this plugin checks for installation, versions, and run-status of Symantec's Norton Antivirus (GPL).
- mcafee_installed.nasl. Originally written by Jeff Adams and later rewritten by Tenable Network Security, Inc., this plugin checks for installation, versions, and status of McAfee's Antivirus (GPL).
- trendmicro_installed.nasl. Written by Tenable Network Security, Inc., this plugin checks for installation, versions, and run-status of Trend Micro's antivirus (non-GPL).
- antivirus_installed.nasl. Written by Tenable Network Security, Inc., this plugin checks the Nessus Knowledge Base (KB) to see if any of the common antivirus products have been installed (non-GPL).

Each of these plugins stores data within the Nessus KB. Given this, a company can easily extend the functionality of the Antivirus checks.

Example:
To conduct a Nessus scan for an Antivirus compliance scan, perform the following steps:

- Perform an update of the Nessus plugins to make sure you have the latest version of the plugins denoted above.
- Configure a new scan by selecting all plugins denoted above.
- Enable a port scan for ports 139 and 445.
- Make sure that “Enable Dependencies at Runtime” is ENABLED. (***)
- Ensure that you have given the Nessus Vulnerability Scanner credentials in order to read the registry on the remote system.
- Run the scan.

For those who are using the Security Center to manage their scans, you would simply create a “Template” scan with the settings from above. This scan would then be available to authorized users.

*** **CAVEAT:** Nessus version 2.2.3/2.4 includes a feature called “silent dependencies”. Versions of Nessus **prior** to 2.2.3 will report on all the enabled dependencies. With newer versions of the Nessus Vulnerability Scanner, this verbosity can be turned off. That is, enabling a closed group of X plugins will only result in, at most, X report items.

Extending the Nessus Vulnerability Scanner

While Tenable’s Nessus Vulnerability Scanner ships with the four plugins above, an organization may wish to extend this functionality for some other Antivirus products or to check for permutations of the existing checks. With NASL this is trivial. Because of the Nessus KB, companies can write custom plugins which only query the KB during a scan.

For example, if a company wanted to only check a certain domain for a certain Antivirus product, the check would be as simple as:

- Check the KB to see if the host resides in domain X
- Check the KB to see if Antivirus Y is installed
- Check the KB to see the version of Antivirus Y
- Report on hosts which are within the domain and are either not running antivirus or running an older version of antivirus signatures

A more detailed example:
Company ABC would like to include a custom check which ensures that all desktop antivirus clients, “ABCVirus”, are configured to report to a central Enterprise Manager “ABCV-Manager”. In order to do this, they have written a NASL script which they will upload to their Nessus Vulnerability Scanner. The code to complete this check would look something like:

```
if(description)
{
script_id();
script_version("$Revision:$");
name["english"] = "ABCVirus Client/Console check";
script_name(english:name["english"]);
desc["english"] = "
This plugin checks that the remote host has the ABCVirus client.

In addition, the check ensures that the client is configured to report to an
ABC's central ABCV-Manager Console.

Solution : Contact Jim Smith, Enterprise Information Security,
for ABC's Policy regarding ABCVirus.
Jim@abc.com
(555) 555-5555 extension 555

Risk factor: High";

script_description(english:desc["english"]);
summary["english"] = "Checks that the remote host has the ABCVirus Agent
installed.";
script_summary(english:summary["english"]);
script_category(ACT_GATHER_INFO);
script_copyright(english:"This script is Copyright (C) 2004 ABC Inc.");
family["english"] = "Windows";
script_family(english:family["english"]);
script_dependencies("netbios_name_get.nasl", "smb_login.nasl",
"smb_registry_full_access.nasl", "smb_enum_services.nasl",
"abcvirus_installed.nasl");
script_require_keys("SMB/name", "SMB/login", "SMB/password",
"SMB/registry_full_access","SMB/transport","Antivirus/ABCVirus/installed");
script_require_ports(139, 445);
exit(0);
}

include("smb_nt.inc");

port = kb_smb_transport();
if(!port)
      port = 139;

abc = get_kb_item ("Antivirus/ABCVirus/installed");
abcm = get_kb_item ("Antivirus/ABCVirus/ABCV-Manager");

if (! abc)
      security_hole(port);

if (abc && ! abcm)
{
  report = "The remote host has ABCVirus Antivirus installed. However the
client is not configured to forward alerts to the ABCV-Manager console.
Contact
Jim@abc.com
(555) 555-5555 extension 555
As soon as possible

Solution : Make sure ABCV-Manager is installed.

Risk factor : High";
security_hole (port);
}
```

NOTE: the script above would actually require another component (abcvirus_installed.nasl) to populate the KB.

The plugin above simply queries the KB for two values. First, the script looks to ensure that the antivirus client is installed. If it is not installed, the script generates a report. If the antivirus client **is** installed, the check goes on to check for the existence of the antivirus manager software. If the antivirus manager software is not present, the script generates a report.

By customizing their own plugin, ABC Company is able to very quickly scan, report and begin remediation on Enterprise systems which are not running their corporate policy for antivirus.

About Tenable Network Security

Tenable, headquartered in Columbia, Md., USA, is the world leader in Unified Security Monitoring. Tenable provides agent-less solutions for continuous monitoring of vulnerabilities, configurations, data leakage, log analysis and compromise detection. For more information, please visit us at http://www.tenablesecurity.com.

TENABLE Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
TEL: 410-872-0555
http://www.tenablesecurity.com