black hat EUROPE 2013

MARCH 12-15, 2013
GRAND HOTEL KRASNAPOLSKY
AMSTERDAM, NETHERLANDS

# Hacking Appliances:
# Ironic exploits in security products

**Ben Williams**

# Proposition

- There is a temptation to think of Security Appliances as impregnable fortresses, this is definitely a mistake.

- Security Appliance *(noun)* - Poorly configured and maintained Linux system with insecure web-app (and other applications)

# Which kind of appliances exactly?

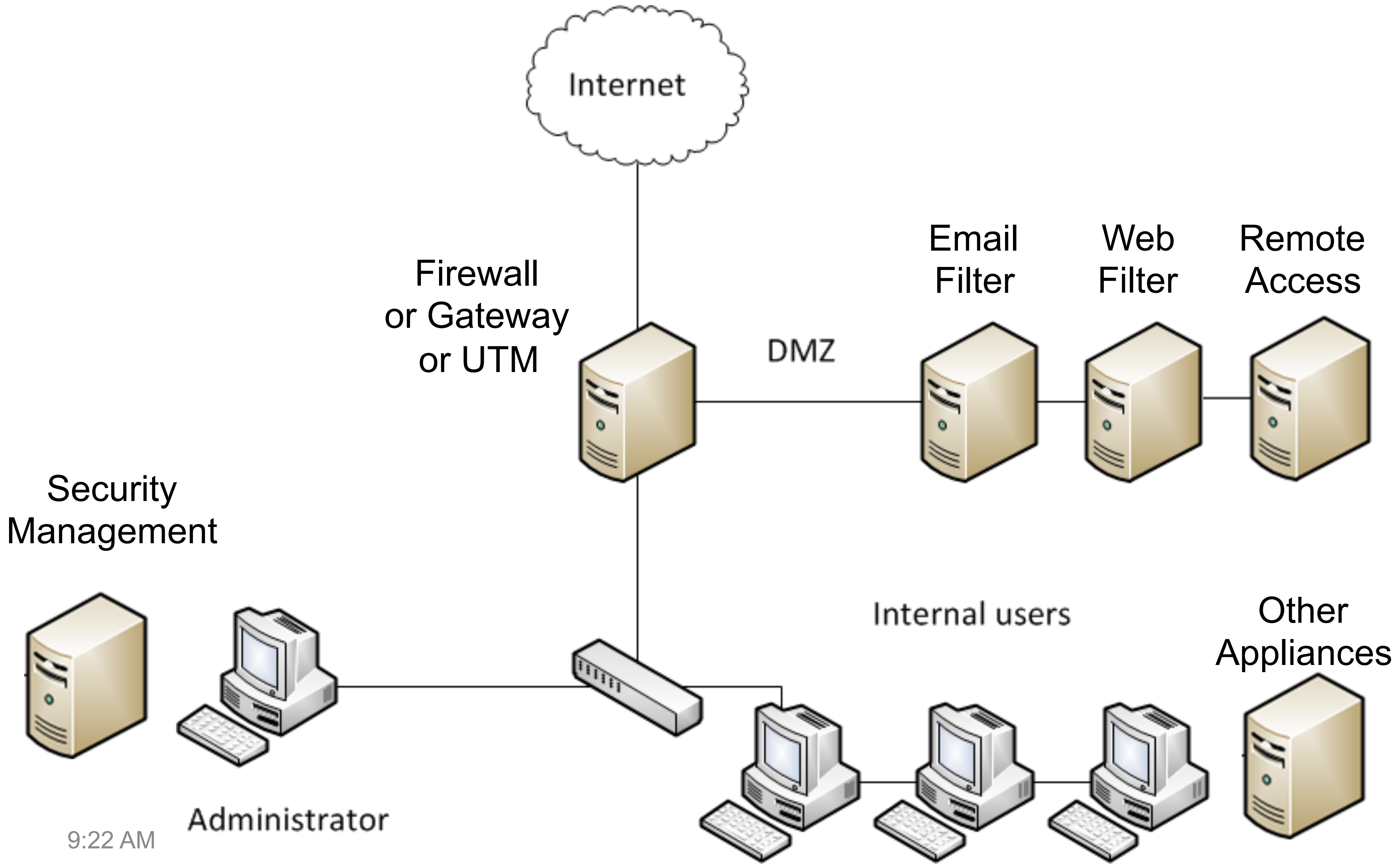
- Email filtering
  - Proofpoint (F-secure among others), Baracuda, Symantec, Trend Micro, Sophos, McAfee
- Firewall, Gateway, Remote Access
  - McAfee, Pfsense, Untangle, ClearOS, Citrix, Barracuda
- Others
  - Single sign-on, communications, file-storage etc

# Are these product well-used and trusted?

2013 SC Magazine US Awards Finalists - Reader Trust Awards - “Best Email Security Solution”

- Barracuda Email Security
- McAfee Email Protection
- Proofpoint Enterprise Protection
- Symantec Messaging Gateway
- Websense Email Security Gateway Anywhere

# How are they deployed?



Firewall
or Gateway
or UTM

Email
Filter

Web
Filter

Remote
Access

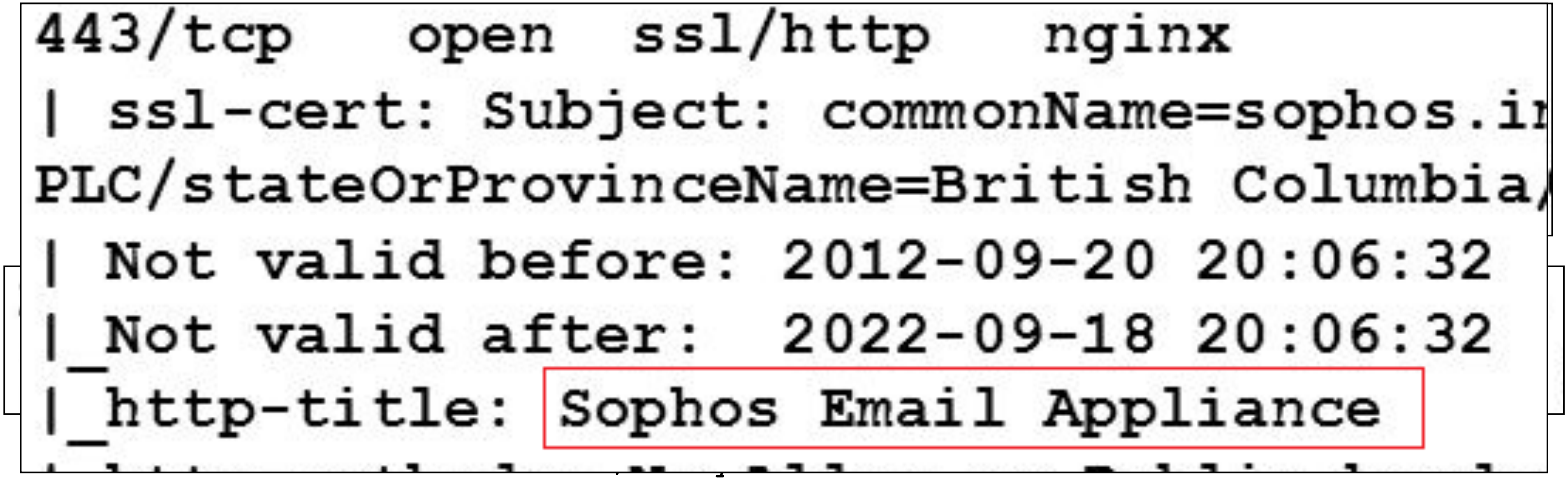
Security
Management

Other
Appliances

# Sophos Email Appliance (v3.7.4.0)

- Easy password attacks
- Command-injection
- Privilege escalation
- Post exploitation

http://designermandan.com/project/crisis-charity/



```
443/tcp   open  ssl/http   nginx
| ssl-cert: Subject: commonName=sophos.i
PLC/stateOrProvinceName=British Columbia/
| Not valid before: 2012-09-20 20:06:32
|_Not valid after:  2022-09-18 20:06:32
|_http-title: Sophos Email Appliance
```

```
| Not valid before: 2012-09-20 20:06:32
|_Not valid after:  2022-09-18 20:06:32
|_http-title: Sophos Email Appliance
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
5432/tcp  open  postgresql PostgreSQL DB 8.0.15 - 8.0.21
18080/tcp open  http       nginx
|_http-methods: No Allow or Public header in OPTIONS response (status code 302)
| http-title: 302 Found
|_Did not follow redirect to https://sophos.insidetrust.com:18080:18080/
```

# Large demo video removed

# Easy targeted password-attacks… because

- Known username (default, often fixed)
- Linux platform with a scalable and responsive webserver
- No account lockout, or brute-force protection
- Minimal password complexity
- Administrators choose passwords
- Few had logging/alerting

- Over an extended period, an attacker stands a very good chance of gaining administrative access

# Really obvious vulnerabilities

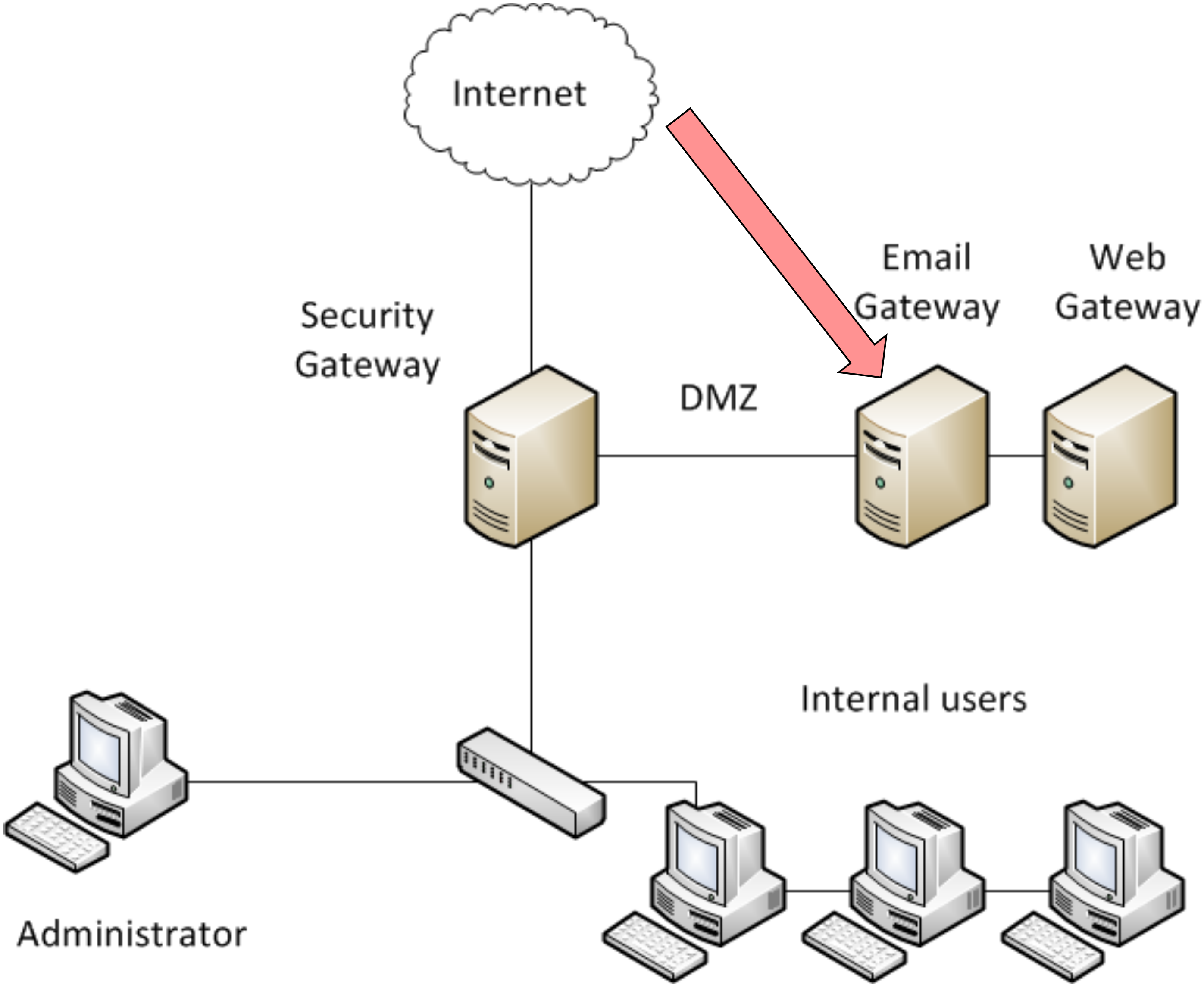
- Loads of issues
- XSS with session hijacking, CSRF, poor cookie and password security, OS command injection…
- So… I got an evaluation…

Large demo video removed

# Command-injection (and root shell)

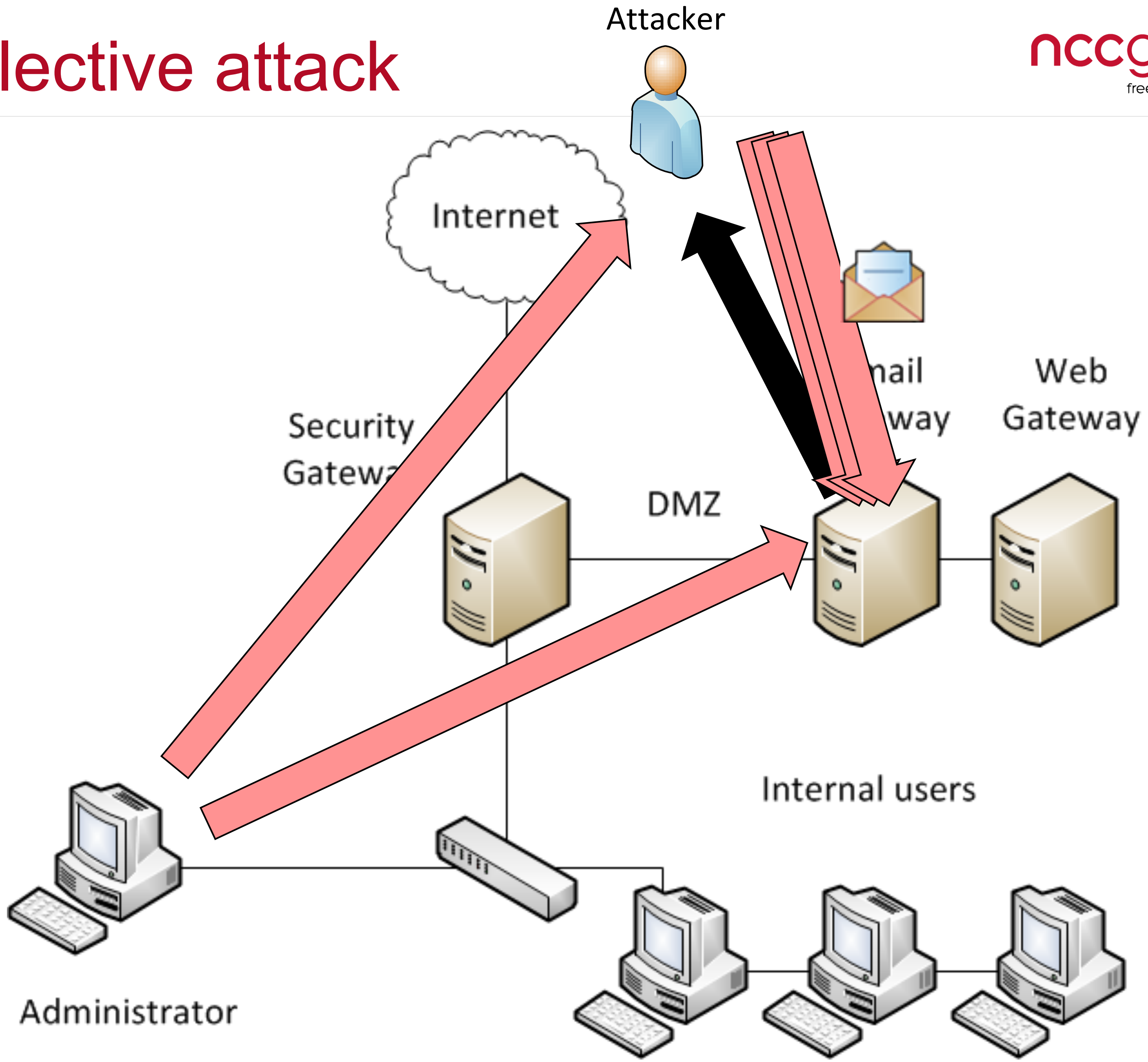
- Why do we want a root shell?
- Reflective attacks (with reverse shells)
- Admins can’t view all email, but an attacker can
- Foothold on internal network

# Direct attack



# Large demo video removed

# Reflective attack



# Large demo video removed

# What do you get on the OS?

- Old kernel
- Old packages
- Unnecessary packages
- Poor configurations
- Insecure proprietary apps

# Appliances are not "Hardened Linux"

- It's common for useful tools to be already installed
  - Compilier/debugger (gcc,gdb), Scripting languages (Perl, Python, Ruby), Application managers (yum, apt-get), Network sniffers (tcpdump), Other tools (Nmap, Netcat)
- File-system frequently not "hardened" either
  - No SELinux. AppArmour or integrity checking
  - Rare to see no-write/no-exec file systems

# Meanwhile… Post exploitation

9:22 AM

# Large demo video removed

# Stealing passwords

- Plain-text passwords on box
- Steal credentials from end-users
  - Just decrypt HTTPS traffic with Wireshark
  - Using the SSL private key for self-signed cert

# Large demo video removed

nccgroup
freedom from doubt

# Sophos fix info: Leave auto-update enabled

- Reported Oct 2012
- Vendor responsive and helpful (though limited info released)
- Fix scheduled for Jan 14th 2013

# The ironic thing about Security Appliances

- Most Security Appliances suffer from similar security vulnerabilities
- Some significantly worse

# Common exploit categories

- Almost all Security Appliance products had
  - Easy password attacks
  - XSS with session-hijacking, or password theft
  - Non-hardened Linux OS – (though vendors claim otherwise)
  - Unauthenticated information disclosure (exact version)
- The majority had
  - CSRF of admin functions
  - OS Command-injection
  - Privilege escalation (either UI and OS)

# Common exploit categories

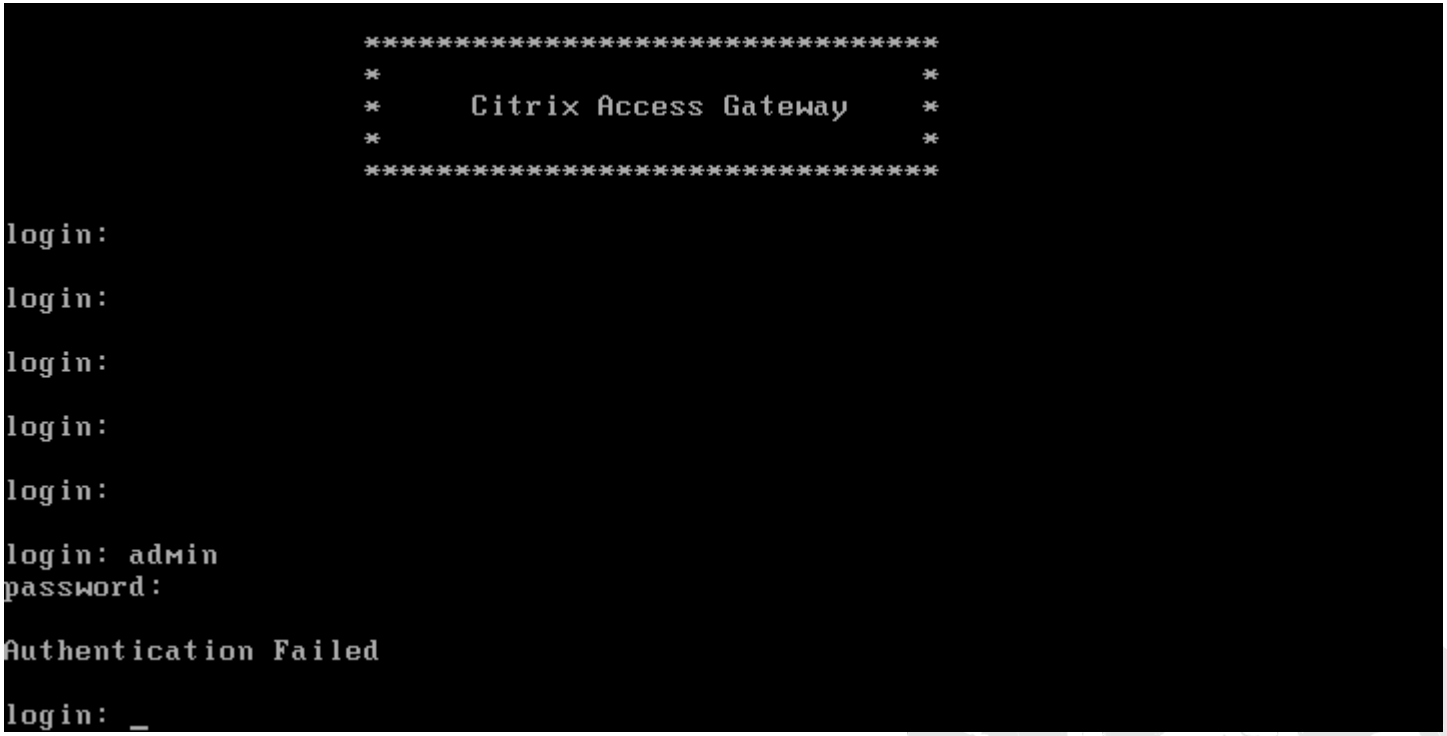
- Several had
  - Stored out-of-band XSS and OSRF (for example in email)
  - Direct authentication-bypass
- A few had
  - Denial-of-Service
  - SSH misconfiguration
- There were a wide variety of more obscure issues

# Citrix Access Gateway (5.0.4)

- Multiple issues
- Potential unrestricted access to the internal network

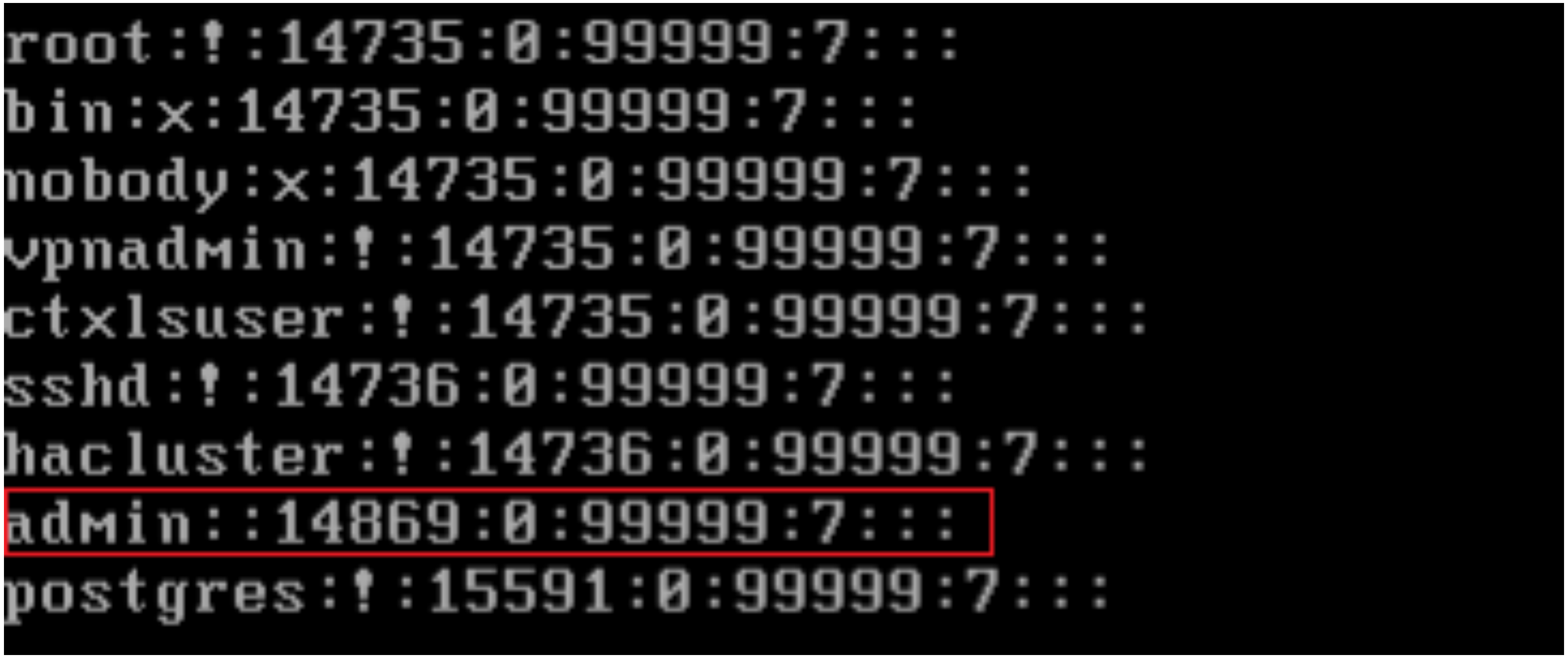
# Erm… That's a bit odd…

ssh admin@192.168.233.55



```
                    *********************************
                    *                               *
                    *     Citrix Access Gateway     *
                    *                               *
                    *********************************

login:

login:

login:

login:

login:

login: admin
password:

Authentication Failed

login: _
```

# Where's my hashes to crack?



```
root:!:14735:0:99999:7:::
bin:x:14735:0:99999:7:::
nobody:x:14735:0:99999:7:::
vpnadmin:!:14735:0:99999:7:::
ctxlsuser:!:14735:0:99999:7:::
sshd:!:14736:0:99999:7:::
hacluster:!:14736:0:99999:7:::
admin::14869:0:99999:7:::
postgres:!:15591:0:99999:7:::
```

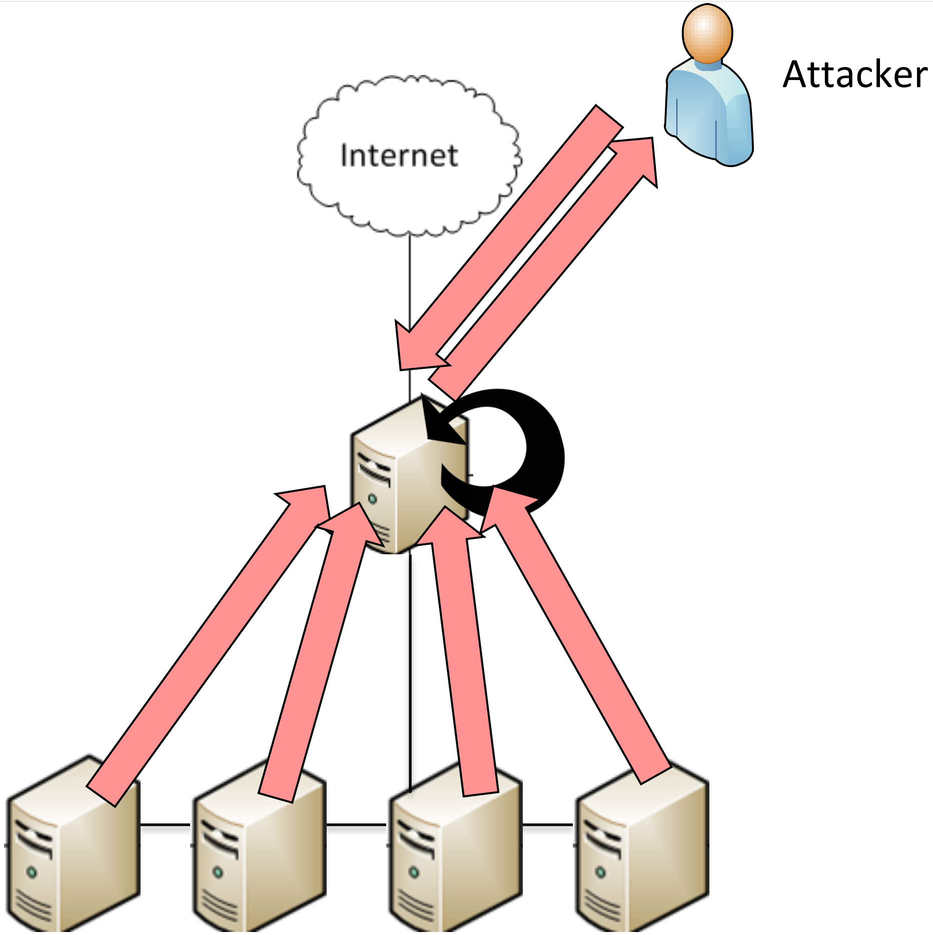
# Port-forwarding (no password)

When SSH is enabled on the CAG - port-forwarding is allowed

```
ssh admin@192.168.1.55
ssh admin@192.168.1.55 -L xxxx:127.0.0.1:xxxx
```

Large demo video removed

# Potential access to internal systems!



# Large demo video removed

# Rather ironic: Remote Access Gateway

- Unauthenticated access to the internal network?
- Auth-bypass and root-shell

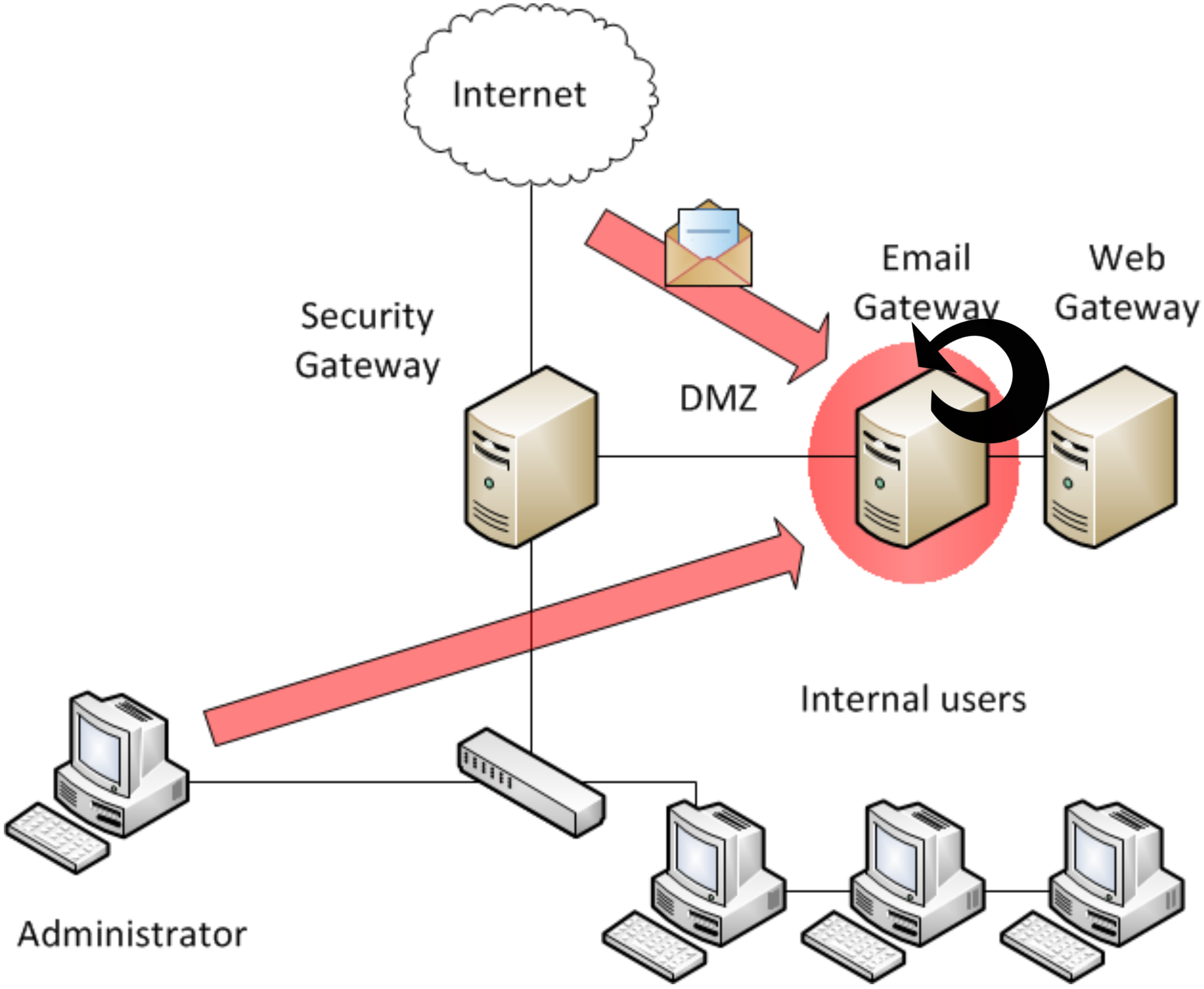
# Citrix fix info: Affects CAG 5.0.x

- Reported Oct 2012
- Fixed released last week (6th March 2013)
- CVE-2013-2263 Unauthorized Access to Network Resources
- http://support.citrix.com/article/ctx136623

# Combination attacks

- Combining multiple common issues

# Proofpoint: ownage by Email (last year)



# Out-of-band XSS and OSRF

- I found 4 products with this issue
  - Three of which were Anti-spam products where you could attack users/administrators via a specially-crafted spam email
- Out-of-Band XSS and OSRF has a massive advantage over CSRF attacks
  - Easy to distribute attack payloads
  - XSS cannot be detected and blocked by the admins browser
  - Minimal social-engineering or reconnaissance

# Backup-restore flaws - revisited via CSRF

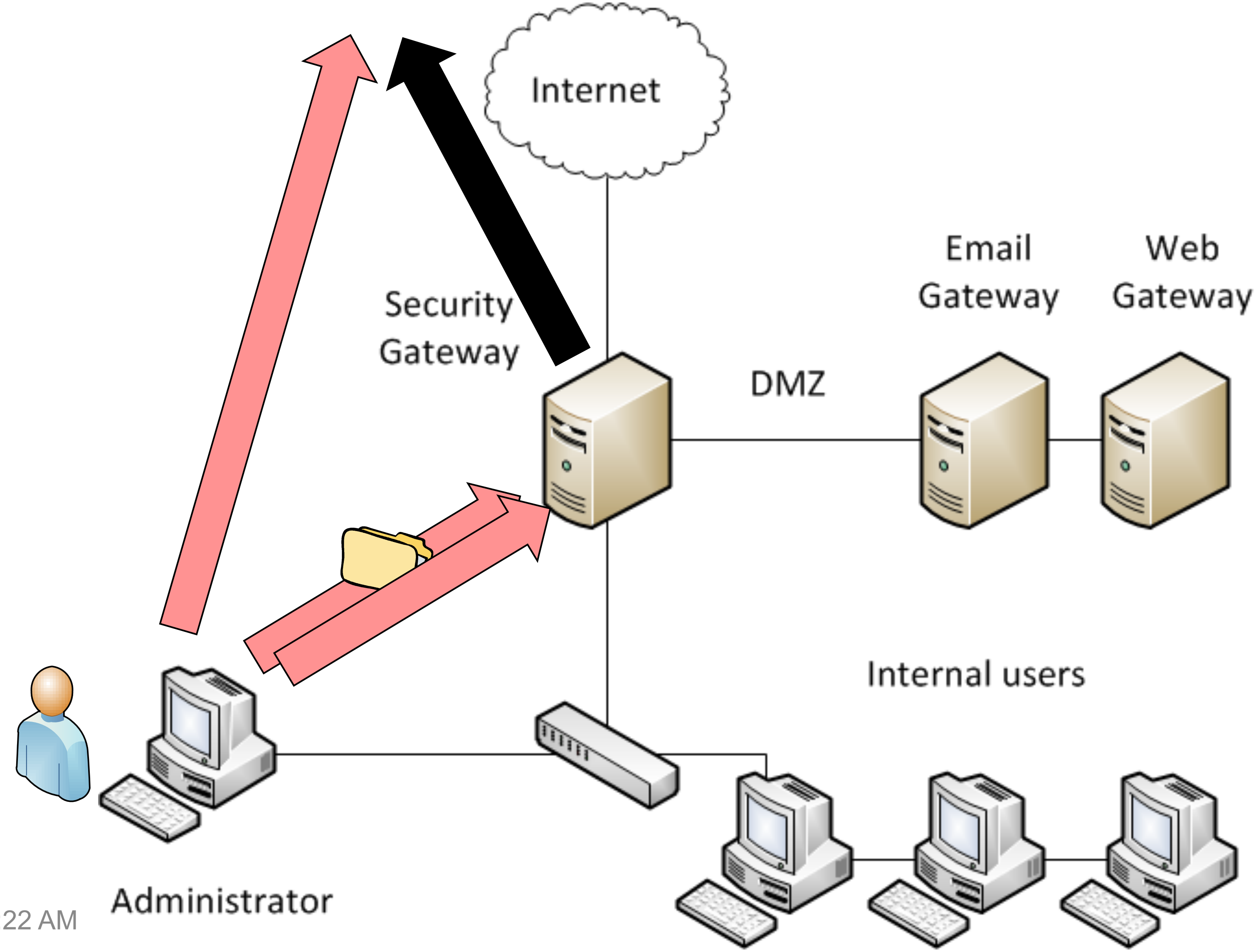
- Vendors deciding not to fix the backup/restore tar.gz issue
- But… common feature, and high-privilege

- Use CSRF to restore the attacker’s backup!
  - Spoof a file-upload and “apply policy”
  - Which results in a reverse-shell as root

# Large demo video removed

# CSRF backup/restore attack

nccgroup
freedom from doubt



# Symantec Email Appliance (9.5.x)

| Description | NCC Rating |
|---|---|
| Out-of-band stored-XSS - delivered by email | Critical |
| XSS (both reflective and stored) with session-hijacking | High |
| Easy CSRF to add a backdoor-administrator (for example) | High |
| SSH with backdoor user account + privilege escalation to root | High |
| Ability for an authenticated attacker to modify the Web-application | High |
| Arbitrary file download was possible with a crafted URL | Medium |
| Unauthenticated detailed version disclosure | Low |

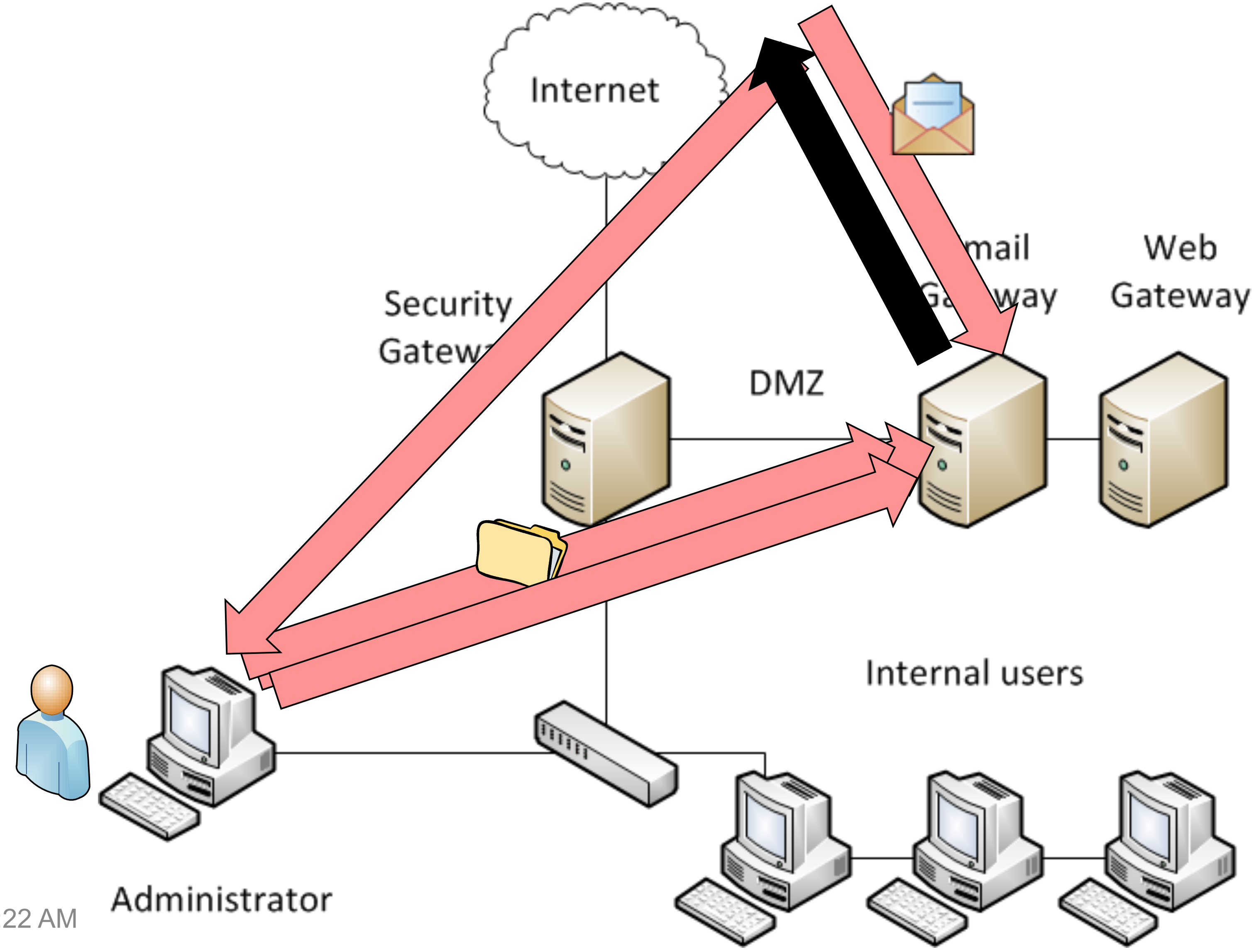
# Out-of-band XSS and OSRF

- Chain together issues in various ways
  - XSS in spam Email subject line, to attack the administrator
  - Use faulty “backup/restore” feature (with OSRF) to add arbitrary JSP to the admin UI, and a SUID binary
  - XSS - Executes new function to send a reverse-shell back to the attacker

# Large demo video removed

9:22 AM

# XSS Email to reverse-shell as root



9:22 AM

# Rather ironic

- Root-shell via malicious email message
- In an email filtering appliance?

# Symantec fix info: Upgrade to 10.x

- Reported April 2012 – Fixed Aug 2012
  - CVE-2012-0307 XSS issues
  - CVE-2012-0308 Cross-site Request Forgery CSRF
  - CVE-2012-3579 SSH account with fixed password
  - CVE-2012-3580 Web App modification as root
  - CVE-2012-4347 Directory traversal (file download)
  - CVE-2012-3581 Information disclosure

http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=2012&suid=20120827_00

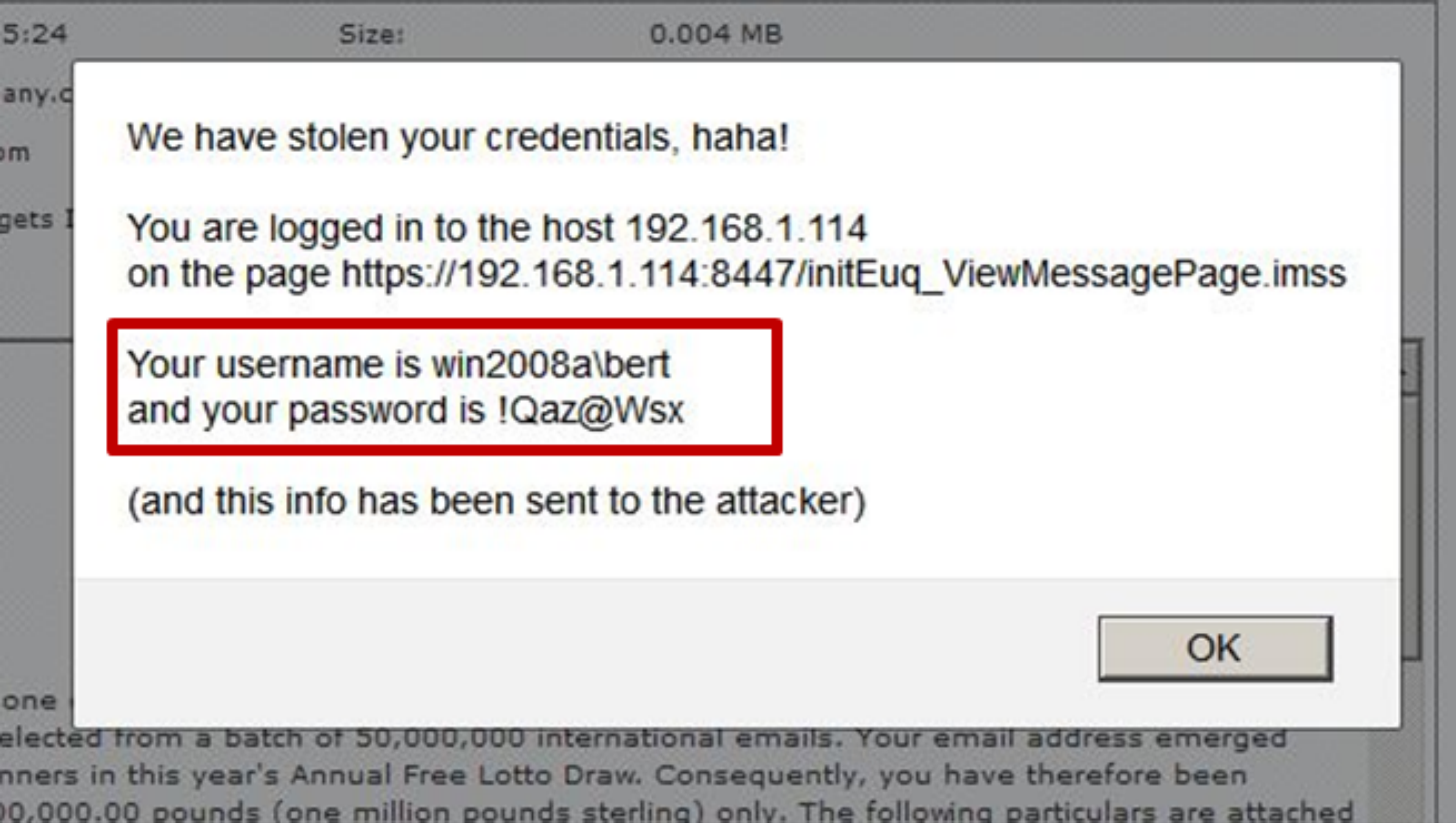
# TrendMicro Email Appliance

# Trend Email Appliance (8.2.0.x)

- Multiple issues

| Description | NCC Rating |
|---|---|
| **Out-of-band stored-XSS in user-portal - delivered via email** | Critical |
| **XSS (both reflective and stored) with session-hijacking** | High |
| **Easy CSRF to add a backdoor-administrator (for example)** | High |
| **Root shell via patch-upload feature (authenticated)** | High |
| **Blind LDAP-injection in user-portal login-screen** | High |
| **Directory traversal (authenticated)** | Medium |
| **Unauthenticated access to AdminUI logs** | Low |
| **Unauthenticated version disclosure** | Low |

Large demo video removed



5:24 Size: 0.004 MB

any.c

om

gets I

We have stolen your credentials, haha!

You are logged in to the host 192.168.1.114
on the page https://192.168.1.114:8447/initEuq_ViewMessagePage.imss

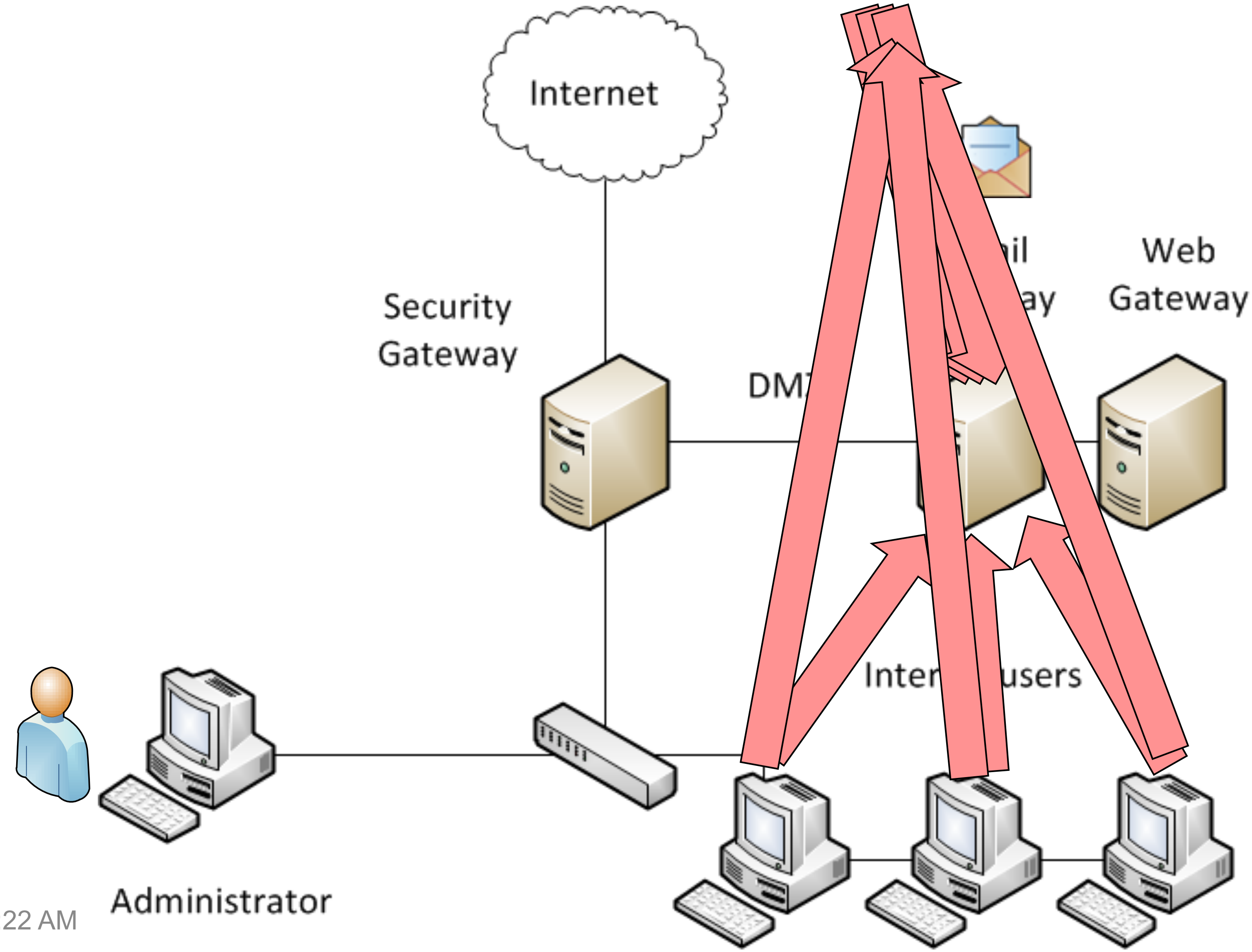
Your username is win2008a\bert
and your password is !Qaz@Wsx

(and this info has been sent to the attacker)

one

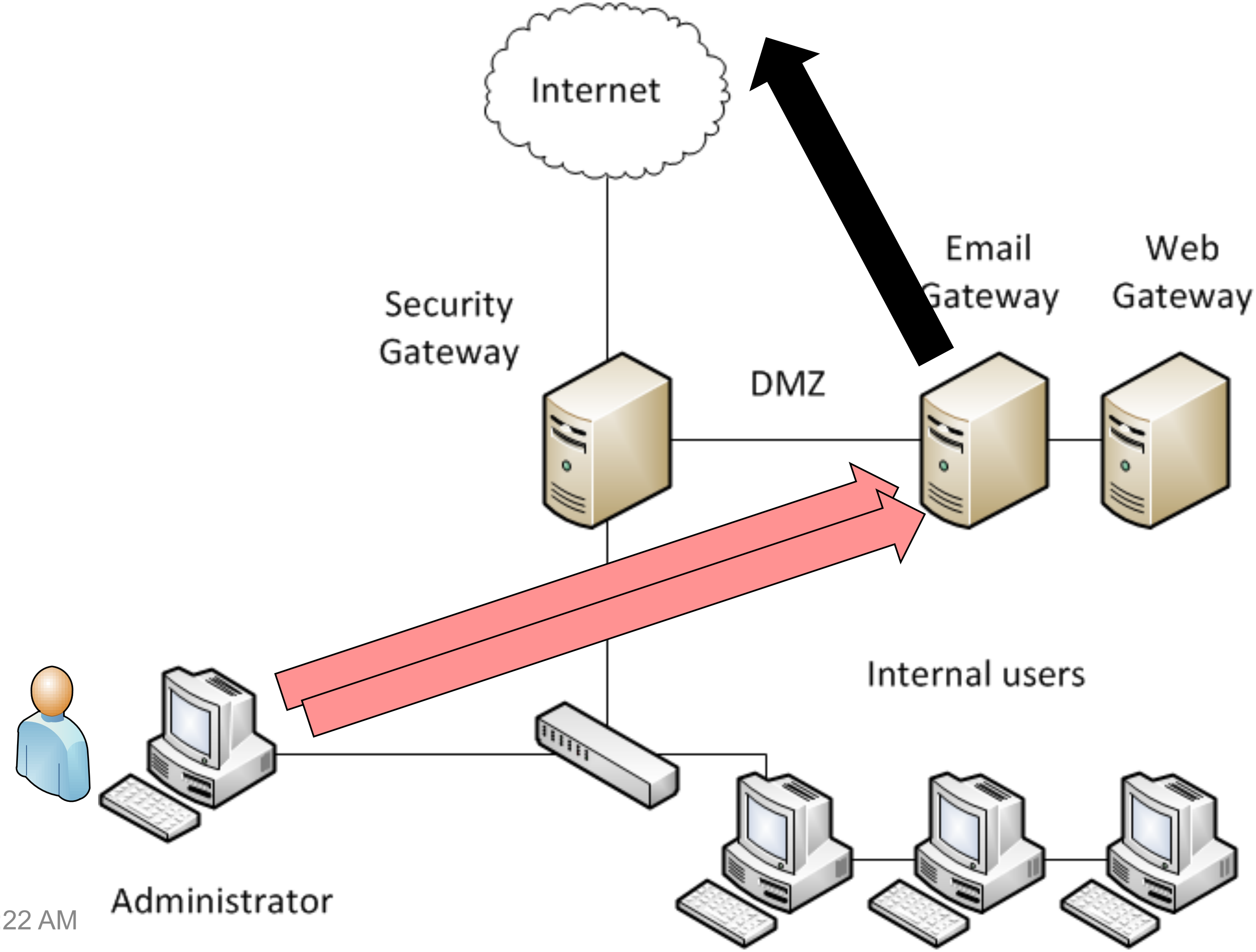
elected from a batch of 50,000,000 international emails. Your email address emerged
nners in this year's Annual Free Lotto Draw. Consequently, you have therefore been
00,000.00 pounds (one million pounds sterling) only. The following particulars are attached

# End-user Email XSS ownage



# Large demo video removed

# Admin Email XSS ownage



# Trend Fix info: Use workarounds

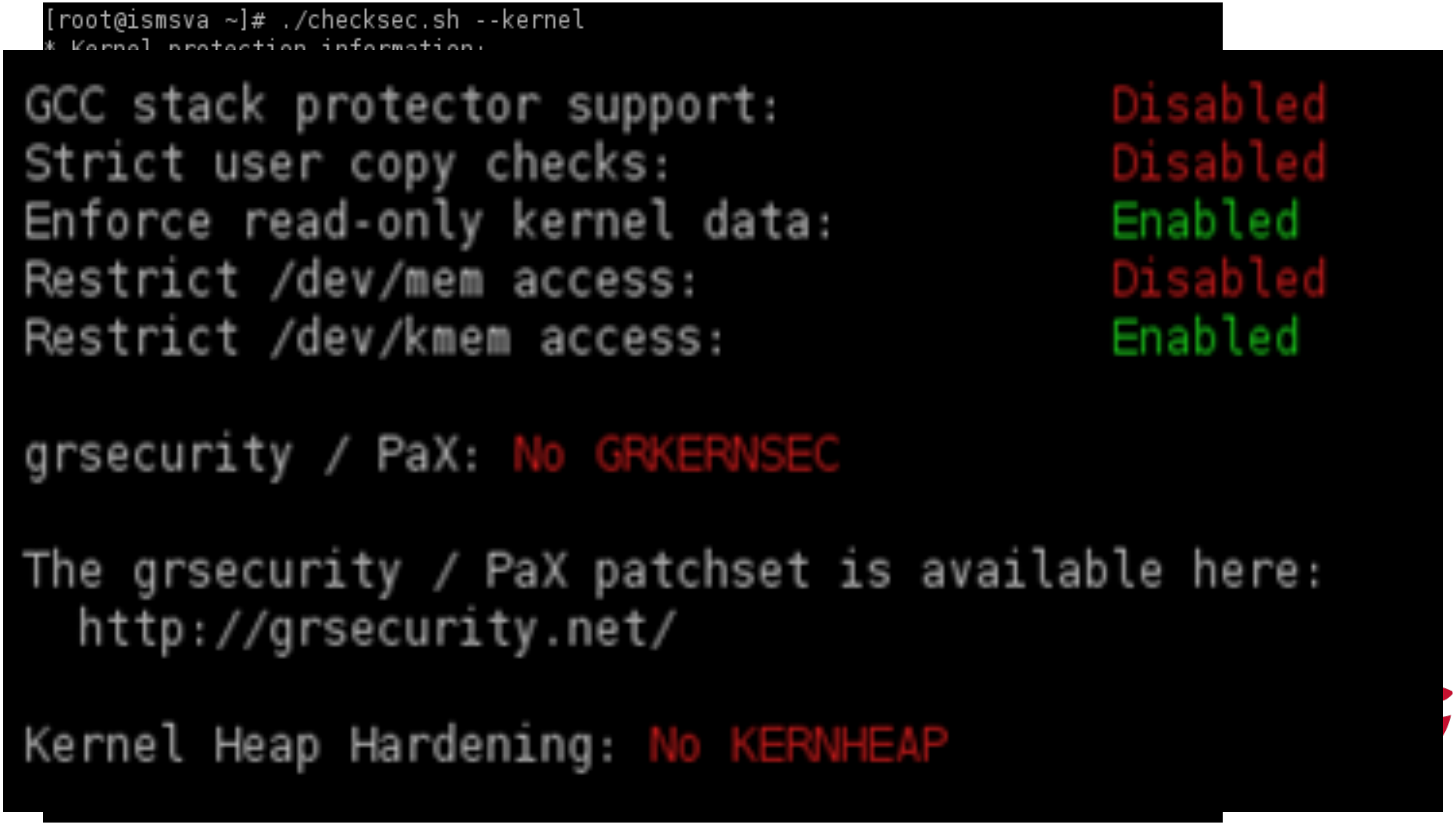
- Reported April 2012
- No fixes released or scheduled AFAIK

# Other Research

- Poking about with binaries
  - Investigation of memory corruption issues
  - Processing of messages etc

9:22 AM

# Kernel protections

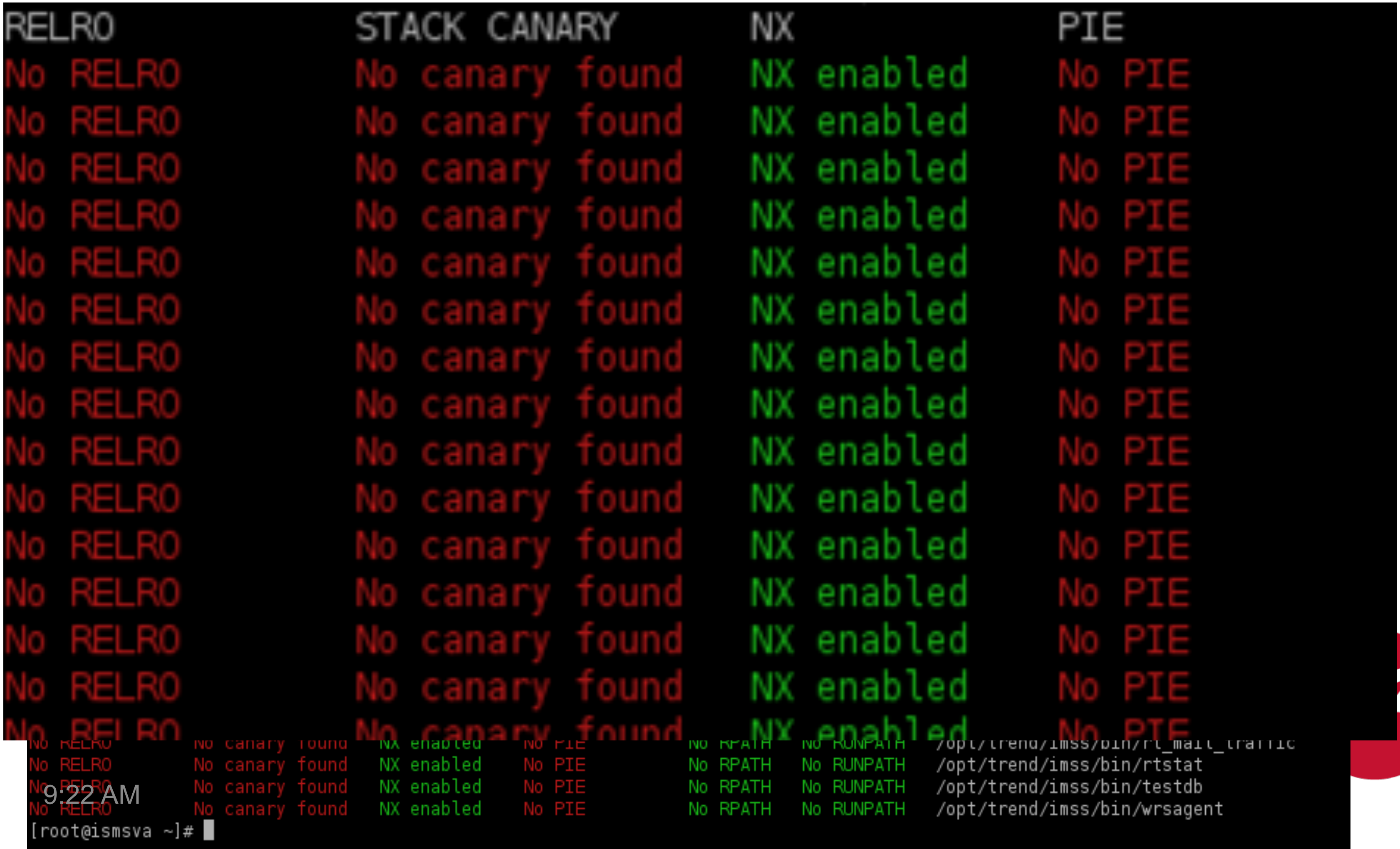


```
[root@ismsva ~]# ./checksec.sh --kernel
* Kernel protection information:
GCC stack protector support:            Disabled
Strict user copy checks:                Disabled
Enforce read-only kernel data:          Enabled
Restrict /dev/mem access:               Disabled
Restrict /dev/kmem access:              Enabled

grsecurity / PaX: No GRKERNSEC

The grsecurity / PaX patchset is available here:
  http://grsecurity.net/

Kernel Heap Hardening: No KERNHEAP
```

9:22 AM

nccgroup
freedom from doubt

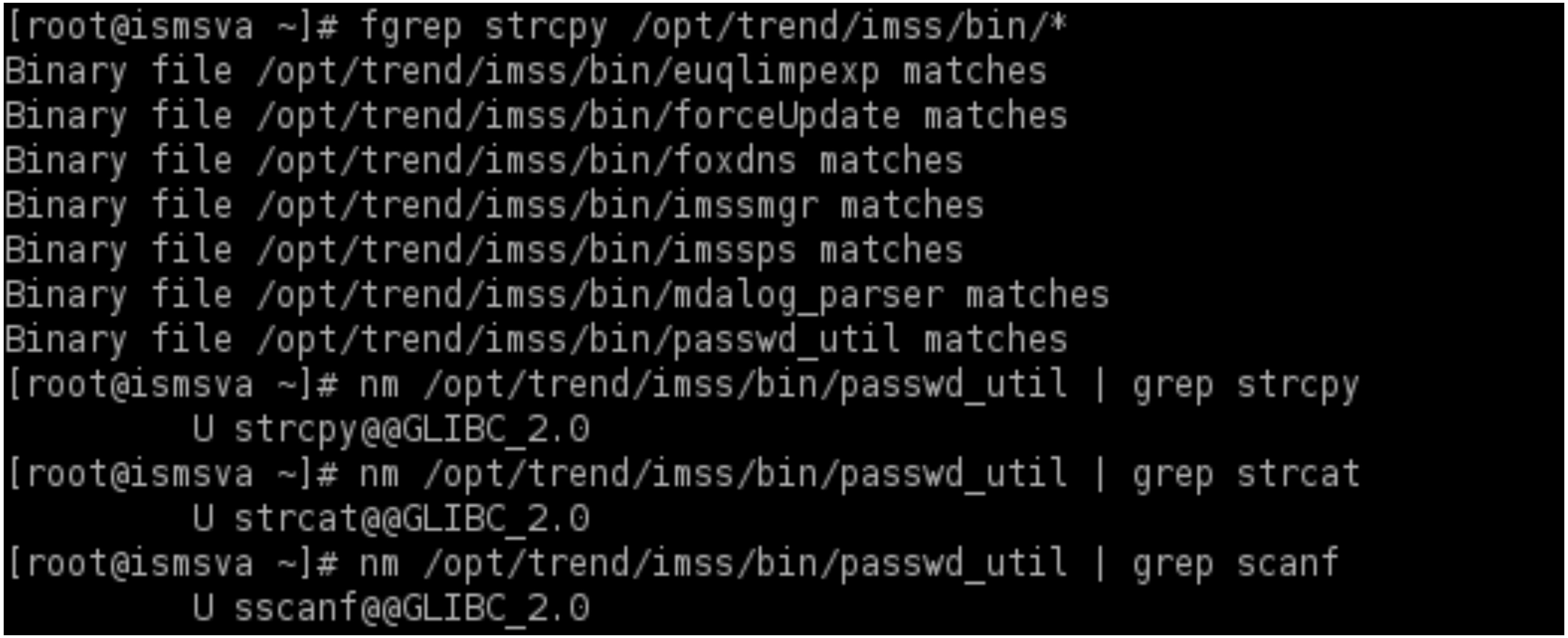
# Compiled Binaries



```
RELRO           STACK CANARY      NX            PIE
No RELRO        No canary found   NX enabled    No PIE
No RELRO        No canary found   NX enabled    No PIE
No RELRO        No canary found   NX enabled    No PIE
No RELRO        No canary found   NX enabled    No PIE
No RELRO        No canary found   NX enabled    No PIE
No RELRO        No canary found   NX enabled    No PIE
No RELRO        No canary found   NX enabled    No PIE
No RELRO        No canary found   NX enabled    No PIE
No RELRO        No canary found   NX enabled    No PIE
No RELRO        No canary found   NX enabled    No PIE
No RELRO        No canary found   NX enabled    No PIE
No RELRO        No canary found   NX enabled    No PIE
No RELRO        No canary found   NX enabled    No PIE
No RELRO        No canary found   NX enabled    No PIE
No RELRO        No canary found   NX enabled    No PIE
```

```
No RELRO        No canary found   NX enabled    No PIE          No RPATH   No RUNPATH   /opt/trend/imss/bin/rt_mail_traffic
No RELRO        No canary found   NX enabled    No PIE          No RPATH   No RUNPATH   /opt/trend/imss/bin/rtstat
No RELRO        No canary found   NX enabled    No PIE          No RPATH   No RUNPATH   /opt/trend/imss/bin/testdb
No RELRO        No canary found   NX enabled    No PIE          No RPATH   No RUNPATH   /opt/trend/imss/bin/wrsagent
[root@ismsva ~]#
```

# “Banned” (insecure) functions in use



```
[root@ismsva ~]# fgrep strcpy /opt/trend/imss/bin/*
Binary file /opt/trend/imss/bin/euqlimpexp matches
Binary file /opt/trend/imss/bin/forceUpdate matches
Binary file /opt/trend/imss/bin/foxdns matches
Binary file /opt/trend/imss/bin/imssmgr matches
Binary file /opt/trend/imss/bin/imssps matches
Binary file /opt/trend/imss/bin/mdalog_parser matches
Binary file /opt/trend/imss/bin/passwd_util matches
[root@ismsva ~]# nm /opt/trend/imss/bin/passwd_util | grep strcpy
         U strcpy@@GLIBC_2.0
[root@ismsva ~]# nm /opt/trend/imss/bin/passwd_util | grep strcat
         U strcat@@GLIBC_2.0
[root@ismsva ~]# nm /opt/trend/imss/bin/passwd_util | grep scanf
         U sscanf@@GLIBC_2.0
```

# Conclusions

- The majority of Security Appliances tested were insecure
  - Interesting state of play in 2012 - 2013
- Variable responses from vendors
  - Some fixed within 3 months, some not
- Evolution
  - Software > Appliances > Virtual Appliances > Cloud Services
- Huawei

# Solutions

- Regular software maintenance
- Secure Development Lifecycle (SDL)
- Product security testing
- Penetration testing

9:22 AM

# Questions?

## UK Offices

Manchester - Head Office

Cheltenham

Edinburgh

Leatherhead

London

Thame

## European Offices

Amsterdam - Netherlands

Munich – Germany

Zurich - Switzerland

## North American Offices

San Francisco

Atlanta

New York

Seattle

## Australian Offices

Sydney

# Large demo video removed