


ESISS



**Playing Detective
DISC Guest Talk 2009**

9th December 2009

Matthew Cook

- ▶ Network and Security Manager for Loughborough University
- ▶ Managing ESISS initiative
- ▶ JANET Contracted Trainer
- ▶ Author of multiple Technical Guides/courses
- ▶ Invited speaker over 50 events in 10 years
- ▶ Personally discovered vulnerabilities in: HP Insight Manager, ExLibris Aleph/MetaLib and Cisco AnyConnect VPN/ASA platform



Agenda

- ▶ Why are we playing detective?
- ▶ What are we seeing?
- ▶ How to playing detective.
- ▶ Tools and examples.
- ▶ Network Based Anomaly Detection.
- ▶ Reputational monitoring.
- ▶ Futures.

▶ <http://escarpment.net/> and <http://esiss.ac.uk/>

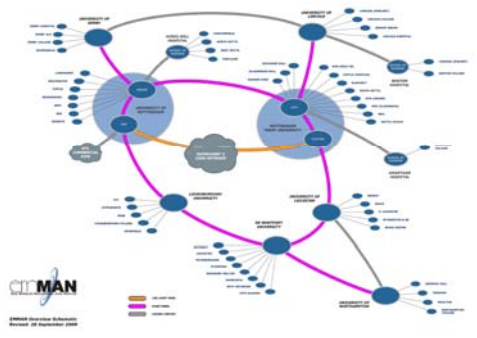
A bit more about Loughborough

- A 437 acre campus University
- 3,000 Staff and 15,000 Students
- 5,500 Study Bedrooms

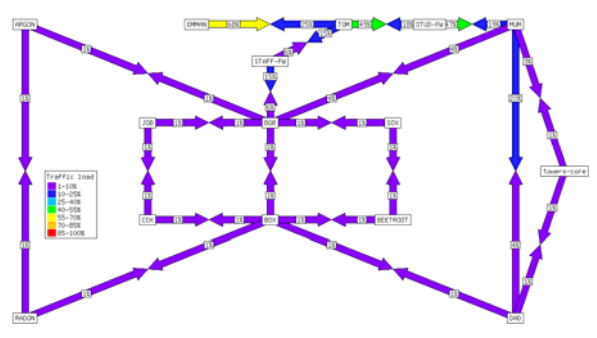
- 1,200 network switches/routers
- 24,000 network connections
- 650 wireless access points

- IT Service with 110 FTEs, 13 Network & Security

East Midlands Region



Network at a Glance



Why we are playing detective?

- Investigating Peer to Peer Usage
- Breach in internal AUP Policy
- Forensics Required
- Assistance required by government agency
 - Police Force, CEOP, MI5, HMRC etc
 - RIPA Act - Section 22(4)
 - Data Protection Act - Section 29
- For reasons to keep the network available
 - A person with a right to control the system
 - Has the express or implied consent, AUP Policy

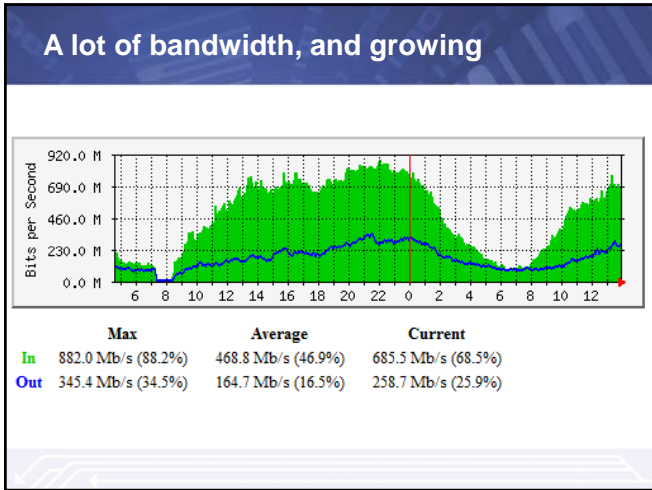
What are we seeing?

- A lot of peer to peer traffic
- External abuse attempts
- Mis-configured internal devices, printers etc
- Internal worm outbreaks
- SPAM bots
- Internal enquires regarding AUP breach
- Enquires from government bodies

- Playing detective on a bigger scale

Dealing with Incidents

- Important to have a policy to follow
- Incidents dealt with in a uniform manner
- Appropriate people managing the process
- Minimum information tracked in Service Desk
- Verify the requestor
- Encrypted storage of data
 - Important when sharing data
- Internally all data gathered from incidents provided to HR or Student Services



- ### Tools
- › Experienced Professionals
 - › Registration systems
 - › NetDISCO
 - › Aggregated Logfiles
 - › Netflow
 - › IDS, replacing Snort
 - › Lancope Stealthwatch
 - › Orion NPM

NetDISCO

MAC	Vendor	Match	Device or Node	First Seen	Last Seen
00:25:90:00:00:00		IP -> MAC	131.231.0.0 (blackhole)	Jun 3 19 54 2009	Dec 9 14 04 2009
		Switch Port	131.231.0.0 FastEthernet0/1 (cisco-2960-48t-e-105-rcv27-1)	May 27 19 19 2009	Dec 9 15 15 2009
		MAC -> IP	131.231.0.0 (88a-43-50)	May 27 09 02 2009	Oct 21 14 16 2009

Matched 1 nodes

Node Search

MAC, hostname, IP, netBIOS

Time Stamps: On / Off

Archived Data: On / Off

Show Vendor: On / Off

Advanced Node Search

[+] Search on Vendor or OUI

Specific Searches

- Search for possible Wireless Access Points (WAP)
- These aren't guaranteed to be wireless access points, they just have MACs that fall into the right range. Also remember people can hide them under fake MAC addresses as well.
- Search for nodes with multiple active IP addresses


* Advanced Searches can be slow to load

IDS Systems

06/16-05:17:26.101855 [**] [1:2181:1] P2P
 BitTorrent transfer [**] [Classification: Potential
 Corporate Privacy Violation] [Priority: 1] {TCP}
 131.231.*.*:1559 -> 65.6.195.243:6883

06/16-12:22:19.935235 [**] [1:1432:4] P2P
 GNUTella GET [**] [Classification: Potential
 Corporate Privacy Violation] [Priority: 1] {TCP}
 158.125.*.*:4229 -> 210.24.249.191:6346

Wireless Access Points



The screenshot shows a map of a campus area with numerous red and green markers representing wireless access points. A search bar is visible at the top right, and a list of AP details is shown on the right side of the map. The details include fields for AP Type, AP Name, AP Address, AP Data, AP Location, and AP Link.

Wireless Access Points

- Some are legitimate: SMEs or Sporting Bodies in Innovation Centres, Students Personal Access Points, Vending Machines, Rogue Access Points and Houses surrounding campus.
- RADAR
- Unauthenticated Access

```
[root@box huntkill]# ./trackme 158.125.*.*
Leave IP2MAC with MAC of '00:00:00:00:00:00'
Seen 00:00:00:00:00:00 on sox interface Po2 going to box
Seen 00:00:00:00:00:00 on box interface Gi1/2 going to beetroot
Seen 00:00:00:00:00:00 on beetroot interface Gi0/6 going to cisco-35-
ZZ
Seen 00:00:00:00:00:00 on cisco-35-** interface FastEthernet0/15
(seen19 on port)
```

Logs, Logs and more Logs

- Logging is key, trivial to set up, difficult to use...
- WMF vulnerability in January 2006
- Aggregation to a central location:
 - DHCP Servers
 - Authentication Servers
 - Email Servers
 - Web Servers (VLE, Intranet, VPN)
 - Network Devices
 - Firewalls
 - IDS
 - Servers: AIDE, Tripwire, Snare, HIDS

Examples

- Physical theft of computer RAM
- Physical theft of whole Computer
- Malicious email: x-originating-ip: [123.121.x.x]
- Hijacked accounts (someone in the room)
- Research Server
- Projects Server
- Photocopier
- Appliance Devices, things you can't patch!

The Beauty of Trend Analysis

- If it happens to you, it will happen to...
- Looking at trends within the sector
- Looking at trends across the global

- SSH Scans
- BotNet Controllers
- Credential dictionary attacks – Email
- Email Spam bots

What can we monitor?

- ▶ Twitter
- ▶ Google Search
- ▶ Facebook
- ▶ BeBo
- ▶ Blogosphere
- ▶ New Sites
- ▶ Wikipedia
- ▶ TheStudentRoom.co.uk
- ▶ WhatUni.com
- ▶ RateMyProfessor.com
- ▶ YouTube
- ▶ Graduate Jobs Forum
- ▶ Web Server Directory List
- ▶ Default Installs/files
- ▶ Web Stats Pages
- ▶ RBL Checks
- ▶ Open SMTP Relay
- ▶ Recursive DNS Check
- ▶ Web Forgery
- ▶ Bug-Me-Not
- ▶ PHP versions
- ▶ Safebrowsing Alerts
- ▶ IRC/IRQ Chat
- ▶ Much, much more

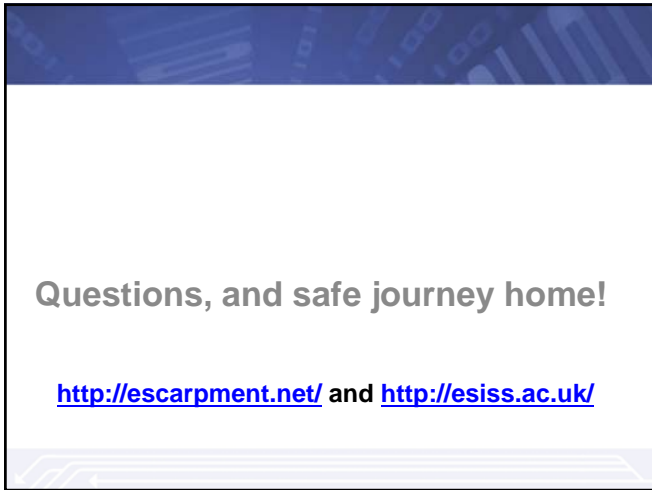
Reputational Monitoring from ESISS

Organization: Loughborough University
 Test Results: Admin
 Overall Health Indicator: ██████████

Test Mechanism	Description	Weight	Most Recent Score	Last Update
Home Page Search	Checking the name "Loughborough University" appears on the home page URL.	0.5	1,000	2009-12-09 10:24:03
Welcome Poster	Network visitor welcome.	0.5	1,000	2009-12-09 18:15:12
Open Proxy Services	Open Proxy Testing.	0.5	1,000	2009-12-09 22:12:02
JMWET RBL presence	Check Lists feeds for RBL entries.	0.2	1,000	2009-12-09 20:49:02
Check for banned words	Look for banned words in Loughborough University.	0.5	0.538	2009-12-09 14:23:01
Vulnerable Wordpress Versions	Checks for buggy versions of Wordpress.	0.2	1,000	2009-12-09 18:18:06
Vulnerable Gallery Versions	Check for obsolete versions of the Gallery photo album software.	0.5	1,000	2009-12-09 19:03:03
Vulnerable PHPMyAdmin versions	Look for buggy PHPMyAdmin MySQL database front ends.	0.3	1,000	2009-12-09 13:19:02
Bruteforce	Bruteforce username and password exposure.	0.7	1,000	2009-12-09 12:28:04
WhatUni.com	Check reviews in whatuni.com.	1.0	1,000	2009-12-09 18:54:05

Futures

- ▶ Increasing bandwidth
- ▶ 802.1X and NAC
- ▶ Site Visitors
- ▶ VPN Portal Abuse
- ▶ IPv6
- ▶ SSL Proliferation
- ▶ Encryption
- ▶ Appliances, things you cannot patch!
- ▶ Cloud Computing: SaaS and IaaS
- ▶ Emerging ISO Standards



Questions, and safe journey home!

<http://escarpment.net/> and <http://esiss.ac.uk/>
