

▶ **Practical Campus Network Security - Exploiting Added Value**

Matthew Cook

Senior IT Security Specialist

Security and Compliance Team

▶ Setting the scene

Security and Compliance Team

- ▶ Loughborough University
 - ▶ Cisco house for many years
 - ▶ Originally 3Com based, with a little Lucent, HP...
- ▶ Large network
 - ▶ 658 manageable switches
 - ▶ Excluding Hall Net
- ▶ Investigating additional security features

- ▶ IT Security changes are fast paced
- ▶ Difficult to judge the security of a network
- ▶ Balance between security and freedom
- ▶ Technology use has changed
- ▶ Bandwidth requirements grown
- ▶ Providing Service Level Agreements
- ▶ IT Security does not have an unlimited budget

▶ Exploiting Added Value?

Security and Compliance Team

- ▶ We would like to offer you some 'Added Value'!
- ▶ Very few companies can deliver!

- ▶ Free added value is even better
 - ▶ Features already included
 - ▶ Features enabled by default
 - ▶ Features that provide real world solutions
 - ▶ Just double check, Enhanced software image?

- ▶ Let go back to basics...

▶ What do we want to secure

- ▶ Very good at securing computers
 - ▶ Anti Virus software
 - ▶ Disabling unwanted services
 - ▶ Configuring logging
 - ▶ Host based firewalls
 - ▶ Host based IDS/IPS
 - ▶ Secure protocols
 - ▶ ... and hopefully a secure password!

- ▶ What about the network?

▶ Configuring the basics

Security and Compliance Team

- ▶ The simple things – passwords
- ▶ SSH enabled devices
 - ▶ Router(config)# hostname Lboro
 - ▶ Lboro(config)# ip domain-name lboro.ac.uk
 - ▶ Lboro(config)# crypto key generate rsa
- ▶ AAA – Authentication, Authorisation, Accounting
 - ▶ Having an audit trail
 - ▶ Staff members leaving
 - ▶ TACACS and RADIUS to ACS

▶ Turning things off

- ▶ Only use the CLI or need more flash space
- ▶ Web Server
 - ▶ Lboro(config)# no ip http server
- ▶ ICMP, discuss...
- ▶ Source Routing
 - ▶ Lboro(config)# no ip source route
- ▶ Proxy ARP
 - ▶ Lboro(config-if)# no ip proxy-arp

- ▶ Filter 'untrusted' messages, aka rogue servers
- ▶ Is this a real threat, well...
- ▶ Creates DHCP binding table
- ▶ Trusted and untrusted interfaces
 - ▶ Trusted – DHCP servers or trunks
 - ▶ Untrusted –Client
 - ▶ Default untrusted
 - ▶ Functioning DHCP requires at least one trusted

▶ Implement DHCP Snooping

- ▶ Global:
 - ▶ Lboro# conf t
 - ▶ Lboro(config)# ip dhcp snooping
 - ▶ Lboro(config)# ip dhcp snooping vlan <blah>

- ▶ DHCP Server or Trunk:
 - ▶ Lboro(config-if)# ip dhcp snooping trust

- ▶ Lboro# sh ip dhcp snooping

▶ IP Source Guard

Security and Compliance Team

- ▶ Turn on DHCP Snooping a little while before
- ▶ No DHCP binding table, no access!
- ▶ Interface:
 - ▶ Lboro (config-if)# ip verify source vlan dhcp-snooping

- ▶ CAM/MAC Table overflow
- ▶ One to One contention, no: hubs, switches etc
- ▶ Interface:
 - ▶ Lboro(config-if)# switchport mode access
 - ▶ Lboro(config-if)# switchport port-security
 - ▶ Lboro(config-if)# switchport port-security maximum 1
 - ▶ Lboro(config-if)# switchport port-security mac-address
 - ▶ [<MAC> | Sticky]
 - ▶ Lboro(config-if)# switchport port-security violation
 - ▶ [Protect | Restrict | Shutdown]

▶ Port Blocking (or Isolation)

- ▶ Prevent devices talking to each other
- ▶ No traffic forwarded between protected ports
- ▶ Traffic must flow via Layer 3 device
- ▶ Interface:
 - ▶ Lboro(config-if)# switchport protected
- ▶ Prevent unwanted multicast unicast traffic on ports
- ▶ Interface:
 - ▶ Lboro(config-if)# switchport block [multicast | unicast]

- ▶ Unicast Reverse Path Forwarding
- ▶ Requires Cisco Express Forwarding (CEF)
- ▶ Problems
 - ▶ Asymmetrical routing
 - ▶ Limited logging compared to traditional ACLs
- ▶ Global:
 - ▶ Lboro(config)# ip cef
- ▶ Interface:
 - ▶ Lboro(config-if)# ip verify unicast reverse-path

- ▶ Mitigate Packet Storm traffic saturation
- ▶ Interface:
 - ▶ Lboro(config-if)# storm-control <traffic> level 80 20
 - ▶ [Broadcast | Unicast | Multicast]
- ▶ Default – Filter traffic
- ▶ Interface:
 - ▶ Lboro(config-if)# storm-control action [shutdown | trap]

▶ Cisco Discovery Protocol (CDP)

Security and Compliance Team

- ▶ We like a bit of 'sh cdp neigh'
- ▶ Only on internal networks, trusted networks
- ▶ Enabled by default!
- ▶ Global:
 - ▶ Lboro(config)# no cdp run
- ▶ Interface:
 - ▶ Lboro(config-if)# no cdp enable

- ▶ Along comes an Elec Eng student with a Zebra...
- ▶ Authentication key
- ▶ RIP v2
- ▶ Others: OSPF, EIGRP, BGP
- ▶ Passive interface
 - ▶ Lboro(config-router)# passive-interface fa0/1

- ▶ Configure NTP
 - ▶ Lboro(config)# ntp server 158.125.x.x prefer
 - ▶ Lboro(config)# ntp server 131.231.x.x

- ▶ Peering
 - ▶ Lboro(config)# ntp peer Lboro-gw2
 - ▶ Lboro(config)# ntp peer Lboro-gw3

- ▶ Disable
 - ▶ Lboro(config-if)# ntp disable

- ▶ CS-Mars
- ▶ Netflow
- ▶ Old skool syslog (NG)
 - ▶ Lboro(config)# logging 158.125.x.x
 - ▶ Lboro(config)# service sequence-numbers
 - ▶ Lboro(config)# logging rate-limit all 10

▶ Pulling down the shutters

Security and Compliance Team

- ▶ Pulling the plug is the last resort
- ▶ Intelligent use of existing features
- ▶ Windows based Worm (NetBIOS/SMB/CIFS)
- ▶ Access Group list statements per interface
- ▶ TFTP New lockdown state to router as replacement ACL

► **Questions:**

Matthew Cook

<http://escarpment.net/>