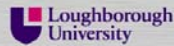


▶ **Microsoft Vista Security and Networking**

Matthew Cook
Senior IT Security Specialist
Security and Compliance Team



▶ **Introduction**

Security and Compliance Team

- ▶ Pressure for Microsoft Vista Implementation
- ▶ Many things have changed
 - ▶ Visible Changes
 - ▶ Beneath the surface
- ▶ Avoid duplication of technical resource



2

▶ **Under the hood**

Security and Compliance Team

- ▶ Enhanced Buffer Overflow Protection
 - ▶ NX bit in hardware
 - ▶ Address Space Layout Randomisation
- ▶ Services
 - ▶ More services by default
 - ▶ Restricted Services
 - ▶ Per service ACLs
- ▶ Signed drivers
- ▶ Kernel Patch Protection (x64)




3

Logon

Security and Compliance Team

- ▶ GINA
- ▶ User Account Control
 - ▶ Standard User or Administrator
 - ▶ Administrator Approval Mode
 - ▶ File system and registry virtualisation

4




Group Policy

Security and Compliance Team

- ▶ Grown exponentially
- ▶ NT 4 tattoos
- ▶ Number frequently increase
- ▶ Vista and Longhorn has approx 2,500
- ▶ Allows for a very tailored configuration

5




Internet Explorer 7

Security and Compliance Team

- ▶ New architecture
- ▶ Phishing Filter
- ▶ SSL Certificate Warning
- ▶ Protected mode (in Vista)
 - ▶ Default, except in trusted zone
 - ▶ Uses new layering technology
 - ▶ User Account Control
 - ▶ Integrity of Applications
 - ▶ Process Privilege protections
 - ▶ Restrict Access
- ▶ Fix My Settings

6



▶ Microsoft Security Centre

Security and Compliance Team

- ▶ Firewall
 - ▶ Monitors egress traffic
 - ▶ Location aware improvements
- ▶ Windows Defender
 - ▶ Software explorer
- ▶ Monitoring Improvements
 - ▶ Anti Virus
 - ▶ Anti Spyware
 - ▶ Firewall
 - ▶ Microsoft Update
 - ▶ Internet Explorer Settings
 - ▶ User Account Control

7

▶ Filing System Protection

Security and Compliance Team

- ▶ BitLocker Drive Protection
 - ▶ Accidental data disposal
 - ▶ TPM
 - ▶ Encryption keys and RIPA Part 3
- ▶ Enhancements to traditional EFS
- ▶ Connection of USB devices
 - ▶ USB Sticks
 - ▶ USB hard discs
 - ▶ iPods etc

8

▶ Networking Changes

Security and Compliance Team

- ▶ Network Access Protection (NAP)
 - ▶ Posture checking
 - ▶ Isolation
- ▶ Network Awareness
 - ▶ Connectivity
 - ▶ Connections
 - ▶ Location
- ▶ Network diagnostics framework
- ▶ Wireless improvements
- ▶ TCP Offloading support
- ▶ SMB 2.0

9

Network Posture

Security and Compliance Team

Windows XP IPv4

```
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open taskscheduler
```

Windows Vista IPv4/6

```
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
5357/tcp open wininit.exe
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open lsass.exe
49157/tcp open services.exe
```

10

Network Services

Security and Compliance Team

```
49152/tcp open - wininit.exe Windows Startup Application
49153/tcp open - svchost.exe Audiosrv, Dhcp, Eventlog,
lmhosts, wscsv
49154/tcp open - svchost.exe EventSystem, FDResPub,
LanmanWorkstation,netprofm, nsi, SSDPSRV, upnphost,
W32Time, WebClient
49155/tcp open - svchost.exe AeLookupSvc, Appinfo,
AppMgmt, BITS, Browser, CertPropSvc, EapHost, gpsvc,
IKEEXT, iphlpsvc, LanmanServer, MMCSS, ProfSvc,
RasMan, Schedule, seclogon, SENS, SessionEnv,
ShellHWDetection, Themes, Winmgmt, wuauaserv
49156/tcp open - lsass.exe KeyIso, Netlogon,
ProtectedStorage, SamSs
```

11

Network Attack Surface

Security and Compliance Team

- ▶ Network Attack Surface for Vista has changed:
- ▶ Many tools no longer work
 - ▶ Fport
 - ▶ Sys Internals TCP View
- ▶ PortQry 2.0
 - ▶ <http://support.microsoft.com/kb/832919>
- ▶ Reference Material
 - http://www.symantec.com/avcenter/reference/Vista_Network_Attack_Surface_RTM.pdf
 - <http://www.symantec.com/avcenter/reference/ATR-VistaAttackSurface.pdf>
 - <http://www.microsoft.com/technet/technetmag/issues/2007/02/VistaKernel/>

12

▶ Web Services for Devices

Security and Compliance Team

Web Services for Devices

<http://msdn2.microsoft.com/en-us/library/aa386284.aspx>

<http://msdn2.microsoft.com/en-us/library/aa385800.aspx>

```
wsdapi    5357/tcp    Web Services for Devices
wsdapi    5357/udp    Web Services for Devices
wsdapi-s  5358/tcp    WS for Devices Secured
wsdapi-s  5358/udp    WS for Devices Secured
```

13

▶ IPv6

Security and Compliance Team

- ▶ Redesigned IPv6 network stack
- ▶ Enabled by default
- ▶ Conversations on local subnet
- ▶ AAAA DNS Lookups
- ▶ IPSec support
- ▶ Teredo NAT Tunneling

14

▶ Image X

Security and Compliance Team

- ▶ Imaging machines creates lots of network traffic
- ▶ WAIK CDImage Download WinPE2
- ▶ `ImageX /compress /capture <drive> <path>`
- ▶ `/compress <none|fast|high>`
- ▶ `ImageX /apply <path> 1 <drive>`
- ▶ .wim File based, not sector based
- ▶ Multiple images per .wim file
- ▶ RIS -> WDS Windows Deployment Services
- ▶ Multicast not supported until Server 2008

15

▶ Recommendations

Security and Compliance Team

- ▶ Don't forget basic security principals:
 - ▶ Passwords
 - ▶ Anti Virus
 - ▶ Patching
 - ▶ Securing the Install
 - ▶ Protecting the LAN
 - ▶ Educating Users

16

▶ Resources

Security and Compliance Team

- ▶ Administering Windows Vista Security The Big Surprises
 - ▶ Mark Minasi
 - ▶ ISBN 0-470-10832-0
- ▶ Microsoft Windows Vista Resource Kit
 - ▶ Microsoft
 - ▶ ISBN 0-735-62283-3
- ▶ JISCmail Lists <http://www.jiscmail.ac.uk/>
 - ▶ windows-uk
 - ▶ uk-security

17

▶ JANET Training

Security and Compliance Team

- ▶ Portfolio of network based training
- ▶ Over 10 different courses
- ▶ Training venues in many locations
- ▶ Comprehensive course workbook + CD

- ▶ Firewalls: Planning and Implementation
 - ▶ Leicester University – 20th June 2007
 - ▶ <http://www.ja.net/services/training/>

18

► **Questions:**

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

