Cleaning Blocked Machines

Guide to getting router blocks lifted

The OxCERT team

Primary objective: protect the integrity of the University network (backbone).

- Dedicated to security and incident response
- security@oucs.ox.ac.uk
- Members
  - Robin Stevens
  - Jonathan Ashton
  - David Ford

Incident Handling

- What is a notification? Who receives it?
- https://networks.oucs.ox.ac.uk/webauth/blocks
- Location
- ID (MAC/IP Address)
- Date
- Reason

Incident Handling

Hi,

I have just put in a router block for the following MAC address,

[hostname]
129.67.XXX.XXX
00:0c:76:8d:6d:22

As it was found to be running a 'warez' server on port 2020

Could you have a look at the machine and check that everything is ok? Let us know when you want the block removed.

Jonathan
Oxford University Computing Services
Network Security Team - OxCERT

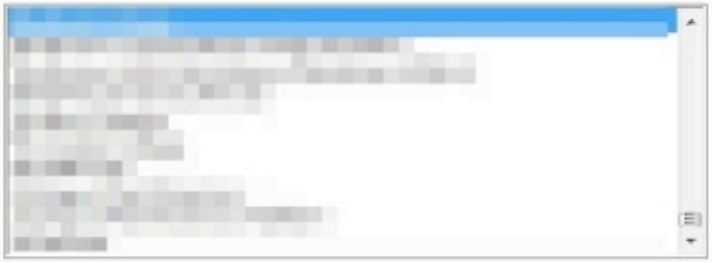
- Date
- Reason

Incident Handling

- What is a notification? Who receives it?
- https://networks.oucs.ox.ac.uk/webauth/blocks
- Location
- ID (MAC/IP Address)
- Date
- Reason

Reasons

- Scan 445
- botnet:18067
- warez 3223

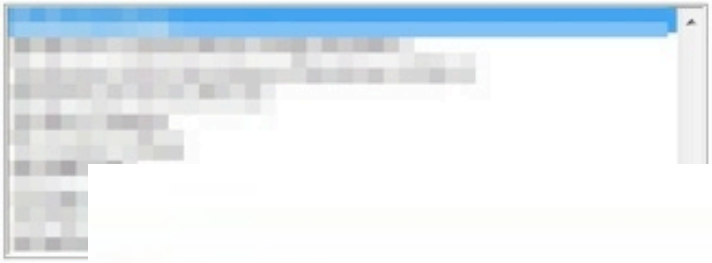


Password: Submit

network connection	block	imposed	reason
[redacted]	00:0c:76:8d:6d:22	Sat May 03 10:47:37 2008	warez: tcp 2020
[redacted]	00:0d:60:75:d5:2b	Thu Jun 28 09:08:30 2007	C&D RT#1346368
[redacted]	00:0d:61:30:5f:a8	Tue Jun 26 08:59:59 2007	scanning ports 139 and 445
[redacted]	00:0d:93:6b:93:46	Wed Jul 09 16:25:05 2008	scanning port 2967

***All* blocks on OUCS remote access services and Graduate Accommodation** **(shown to aid user support queries; these will not necessarily relate to users from your unit)**

Dialup Services	tcp/135	Thu Apr 15 12:24:25 2004	
Dialup Services	tcp/445	Sun Apr 18 21:53:59 2004	
Graduate Accom	00:00:e2:99:e8:8b	Fri Oct 13 23:28:25 2006	scanning 135 445
Graduate Accom	00:03:0d:2e:d2:5d	Tue May 23 08:49:47 2006	ping swep
Graduate Accom	00:0c:76:8d:6d:22	Tue Feb 26 22:55:26 2008	C&D RT#1177113 ID: 14-16347875
Graduate Accom	00:0d:60:75:d5:2b	Mon Jan 08 09:06:53 2007	RT1037767 connect to malicious IRC
Graduate Accom	00:0d:61:30:5f:a8	Tue Aug 28 09:31:13 2007	C&D RT#1111290
Graduate Accom	00:0d:93:6b:93:46	Thu Jul 26 18:00:15 2007	C&D and other abuse RT#1099430
Graduate Accom	00:10:5a:63:ca:ca	Fri Nov 24 15:20:17 2006	C&D RT#1026203 (Notice ID: 182-915551)
Graduate Accom	00:10:a4:96:a0:42	Tue May 24 09:37:00 2005	cease & desist: rt#785199, ID 21-94699
Graduate Accom	00:10:c6:dd:9e:c2	Thu Jul 26 18:01:02 2007	C&D and other abuse RT#1099430
Graduate Accom	00:11:24:7f:cf:80	Thu Jul 26 15:53:03 2007	C&D rt#1099430 also unregistered host using static IP
Graduate Accom	00:11:25:d4:d2:a7	Fri Dec 16 10:05:25 2005	C&D RT#926339 ID: 14-3181334
Graduate Accom	00:16:41:a7:c1:28	Mon Jun 04 20:20:38 2007	C&D 1084410 ID: 14-14713092
Graduate Accom	00:17:f2:e1:c0:de	Wed Feb 20 00:17:03 2008	C&D RT#1175170 ID: 14-16271594
Graduate Accom	00:19:e3:61:dd:7b	Sat May 03 10:47:37 2008	C&D RT#1198024 ID: 14-16681178
Graduate Accom	00:a0:d1:22:f8:b7	Thu Jun 28 09:08:30 2007	C&D14-15020298 RD#1090469
Graduate Accom	00:b0:d0:e7:3e:0f	Tue Jun 26 08:59:59 2007	C&D 14-14989521 RT#1089581



Passwor

reason
warez: tcp 2020
C&D RT#1346368
scanning ports 139 and 445
scanning port 2967

All bloc

Dialup S
Dialup S
Graduat
Graduat
Graduat
Graduat
Graduat
Graduat
Graduat
Graduat
Graduat
Graduat
Graduat

Graduate Accom	00:16:41:a7:c1:28	Mon Jun 04 20:20:38 2007	C&D 1084410 ID: 14-14713092
Graduate Accom	00:17:f2:e1:c0:de	Wed Feb 20 00:17:03 2008	C&D RT#1175170 ID: 14-16271594
Graduate Accom	00:19:e3:61:dd:7b	Sat May 03 10:47:37 2008	C&D RT#1198024 ID: 14-16681178
Graduate Accom	00:a0:d1:22:f8:b7	Thu Jun 28 09:08:30 2007	C&D14-15020298 RD#1090469
Graduate Accom	00:b0:d0:e7:3e:0f	Tue Jun 26 08:59:59 2007	C&D 14-14989521 RT#1089581

Initial Steps

- Windows Update
  - Remember doesn't update applications (e.g. MS Office)
  - MS Update
- Ensure AV and Anti-spyware is installed and up to date
  - Run scans

Then What?

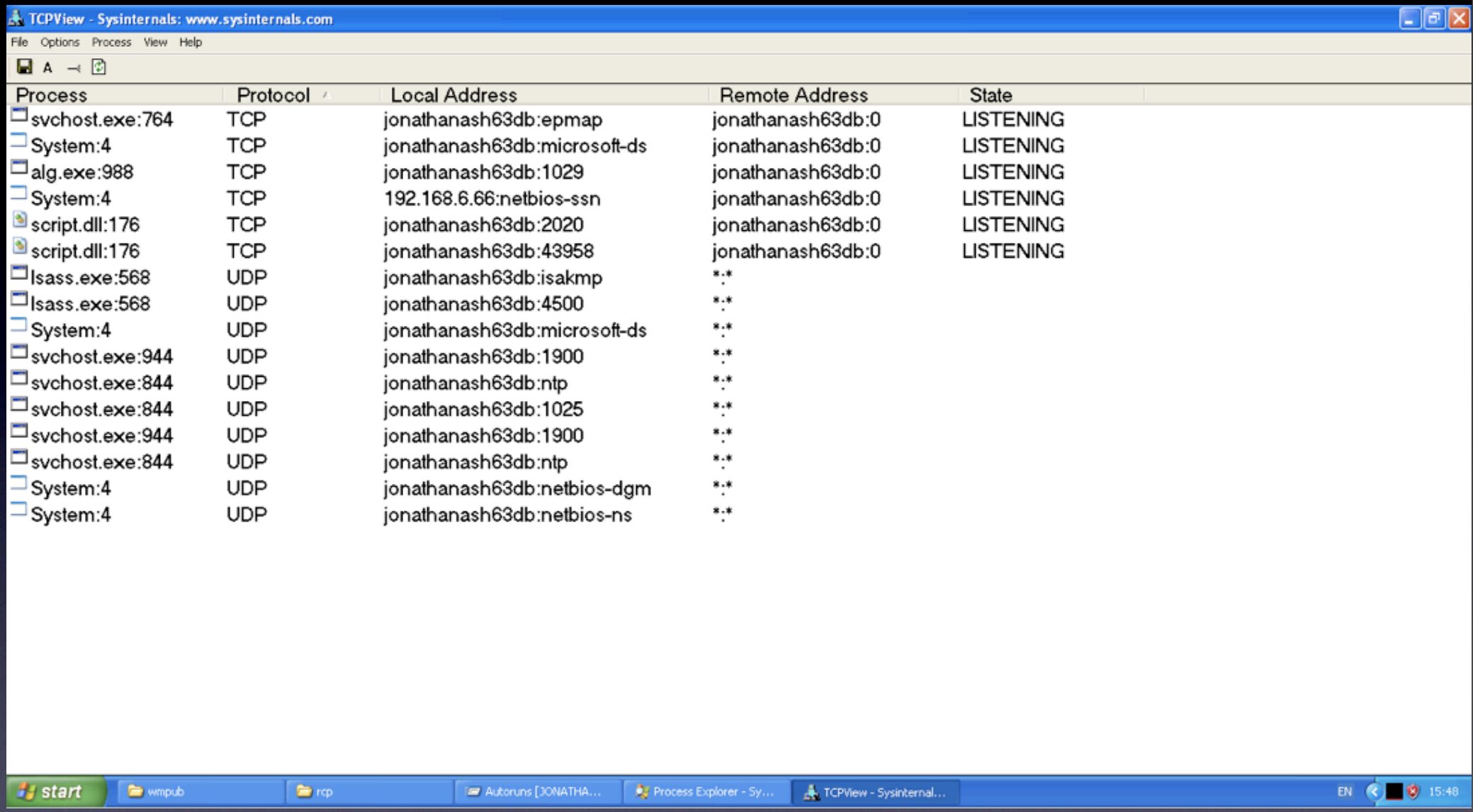
- Contact OxCERT
  - We may be able to give you further useful information.
  - Type/time of infection
  - Any files to look for
  - Virus signature availability

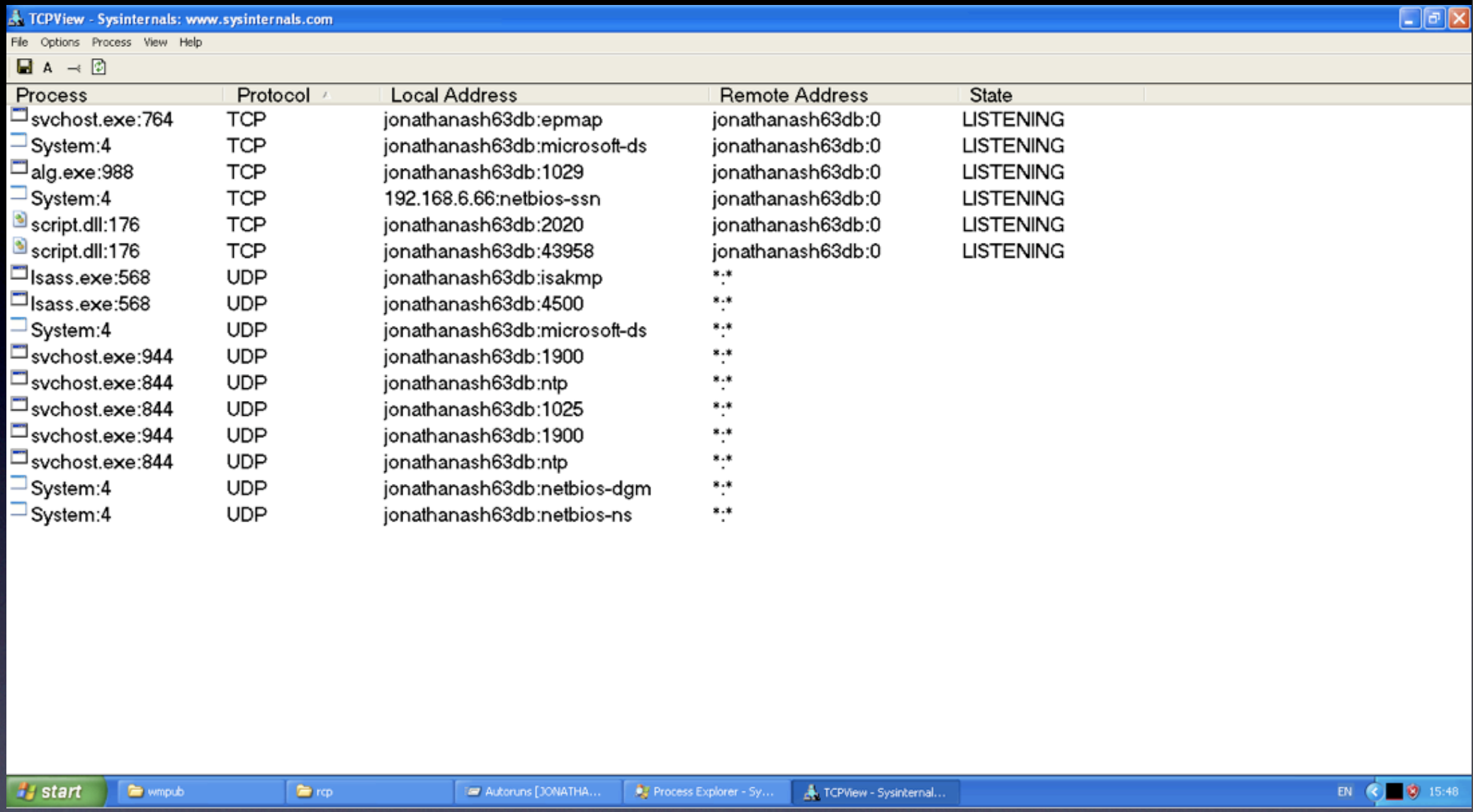
Further Investigation

- Turn OFF ‘Hide system folders’
- Turn ON ‘Show hidden files’
- Turn OFF ‘Hide protected OS files’
- Useful Tools:
  - http://www.microsoft.com/technet/sysinternals/default.mspx
  - netstat / TCPView
  - Process Explorer
  - Autoruns

TCPView

- Shows listings of TCP and UDP endpoints.
- Local/remote addresses & ports.
- State of TCP connections
- www.treachery.net/tools/ports


TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help
Process Protocol Local Address Remote Address State
svchost.exe:764 TCP jonathanash63db:epmap jonathanash63db:0 LISTENING
System:4 TCP jonathanash63db:microsoft-ds jonathanash63db:0 LISTENING
alg.exe:988 TCP jonathanash63db:1029 jonathanash63db:0 LISTENING
System:4 TCP 192.168.6.66:netbios-ssn jonathanash63db:0 LISTENING
script.dll:176 TCP jonathanash63db:2020 jonathanash63db:0 LISTENING
script.dll:176 TCP jonathanash63db:43958 jonathanash63db:0 LISTENING
lsass.exe:568 UDP jonathanash63db:isakmp *:*
lsass.exe:568 UDP jonathanash63db:4500 *:*
System:4 UDP jonathanash63db:microsoft-ds *:*
svchost.exe:944 UDP jonathanash63db:1900 *:*
svchost.exe:844 UDP jonathanash63db:ntp *:*
svchost.exe:844 UDP jonathanash63db:1025 *:*
svchost.exe:944 UDP jonathanash63db:1900 *:*
svchost.exe:844 UDP jonathanash63db:ntp *:*
System:4 UDP jonathanash63db:netbios-dgm *:*
System:4 UDP jonathanash63db:netbios-ns *:*
start
wmpub
rcp
Autoruns [JONATHA...
Process Explorer - Sy...
TCPView - Sysinternal...
EN
15:48

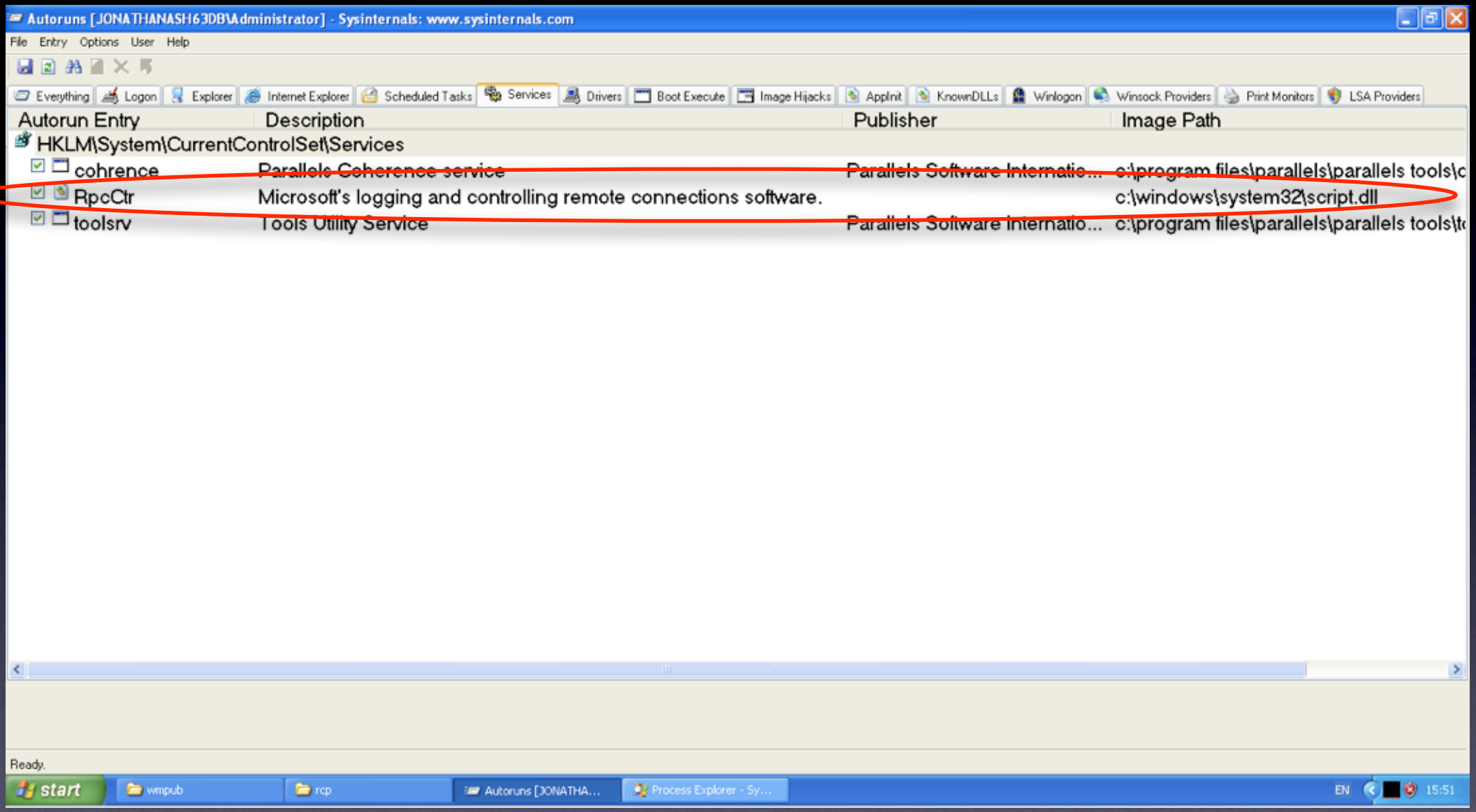

TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help
Process Protocol Local Address Remote Address State
svchost.exe:764 TCP jonathanash63db:epmap jonathanash63db:0 LISTENING
System:4 TCP jonathanash63db:microsoft-ds jonathanash63db:0 LISTENING
alg.exe:988 TCP jonathanash63db:1029 jonathanash63db:0 LISTENING
System:4 TCP 192.168.6.66:netbios-ssn jonathanash63db:0 LISTENING
script.dll:176 TCP jonathanash63db:2020 jonathanash63db:0 LISTENING
script.dll:176 TCP jonathanash63db:43958 jonathanash63db:0 LISTENING
lsass.exe:568 UDP jonathanash63db:isakmp *:*
lsass.exe:568 UDP jonathanash63db:4500 *:*
System:4 UDP jonathanash63db:microsoft-ds *:*
svchost.exe:944 UDP jonathanash63db:1900 *:*
svchost.exe:844 UDP jonathanash63db:ntp *:*
svchost.exe:844 UDP jonathanash63db:1025 *:*
svchost.exe:944 UDP jonathanash63db:1900 *:*
svchost.exe:844 UDP jonathanash63db:ntp *:*
System:4 UDP jonathanash63db:netbios-dgm *:*
System:4 UDP jonathanash63db:netbios-ns *:*
start
wmpub
rcp
Autoruns [JONATHA...
Process Explorer - Sy...
TCPView - Sysinternal...
EN
15:48

TCPView

- Shows listings of TCP and UDP endpoints.
- Local/remote addresses & ports.
- State of TCP connections
- www.treachery.net/tools/ports

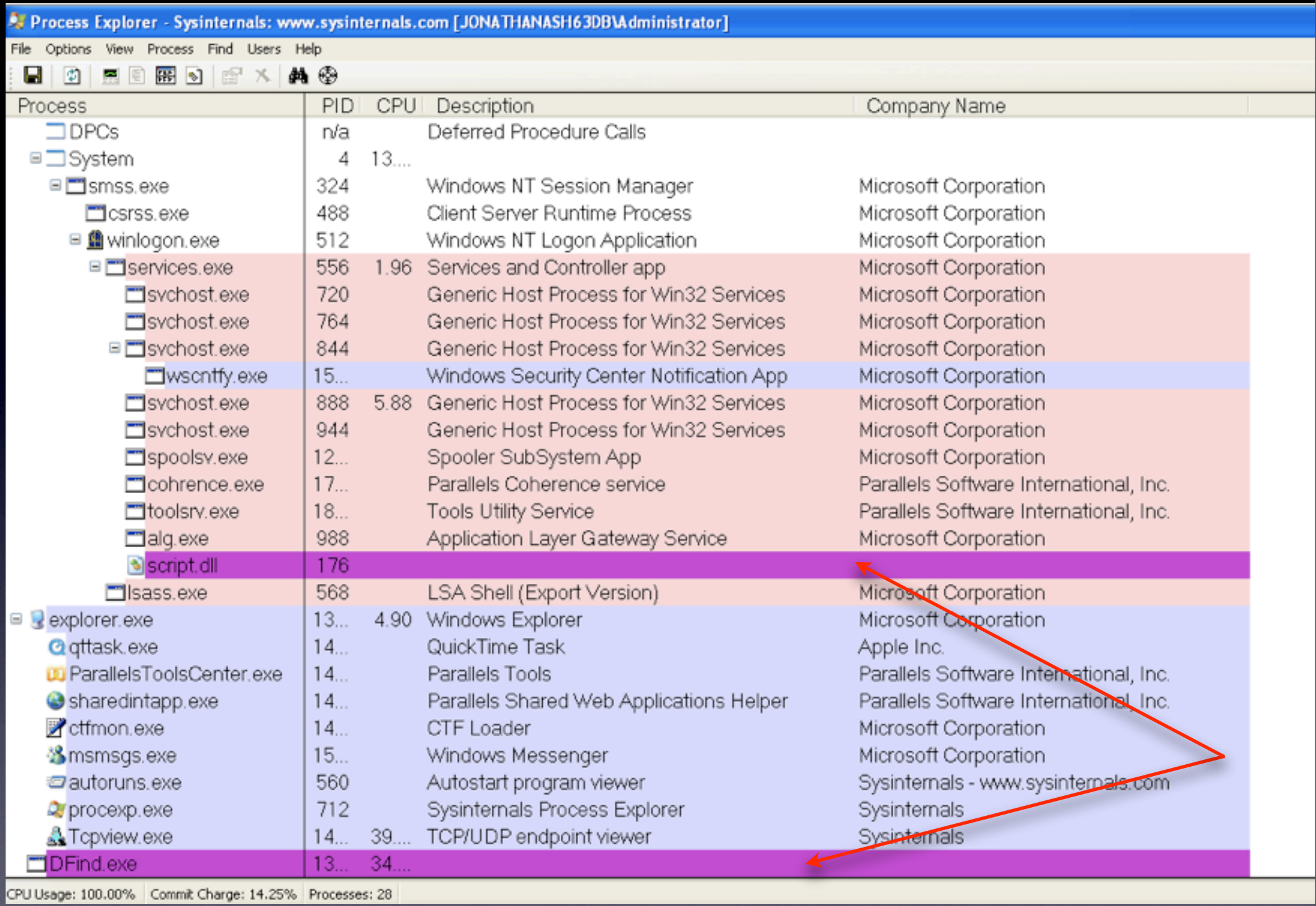
Autoruns

- Programs configured to run during system boot or login
- Startup Folder & Registry Keys


Autoruns [JONATHANASH63DB\Administrator] - Sysinternals: www.sysinternals.com
File Entry Options User Help
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Boot Execute Image Hijacks AppInit KnownDLLs Winlogon Winsock Providers Print Monitors LSA Providers
Autorun Entry Description Publisher Image Path
HKLM\System\CurrentControlSet\Services
cohrence Parallels Coherence service Parallels Software Internatio... c:\program files\parallels\parallels tools\c
RpcCtr Microsoft's logging and controlling remote connections software. c:\windows\system32\script.dll
toolsrv Tools Utility Service Parallels Software Internatio... c:\program files\parallels\parallels tools\t
Ready.
start
wmpub
rcp
Autoruns [JONATHA...
Process Explorer - Sy...
EN
15:51

Process Explorer

- Display of process activity
- Includes which handles each process has running
  - DLLs
  - memory-mapped files
- Verify process images


Process Explorer - Sysinternals: www.sysinternals.com [JONATHANASH63DB\Administrator]
File Options View Process Find Users Help
Process PID CPU Description Company Name
DPCs n/a Deferred Procedure Calls
System 4 13....
smss.exe 324 Windows NT Session Manager Microsoft Corporation
csrss.exe 488 Client Server Runtime Process Microsoft Corporation
winlogon.exe 512 Windows NT Logon Application Microsoft Corporation
services.exe 556 1.96 Services and Controller app Microsoft Corporation
svchost.exe 720 Generic Host Process for Win32 Services Microsoft Corporation
svchost.exe 764 Generic Host Process for Win32 Services Microsoft Corporation
svchost.exe 844 Generic Host Process for Win32 Services Microsoft Corporation
wscntfy.exe 15... Windows Security Center Notification App Microsoft Corporation
svchost.exe 888 5.88 Generic Host Process for Win32 Services Microsoft Corporation
svchost.exe 944 Generic Host Process for Win32 Services Microsoft Corporation
spoolsv.exe 12... Spooler SubSystem App Microsoft Corporation
cohrence.exe 17... Parallels Coherence service Parallels Software International, Inc.
toolsrv.exe 18... Tools Utility Service Parallels Software International, Inc.
alg.exe 988 Application Layer Gateway Service Microsoft Corporation
script.dll 176
lsass.exe 568 LSA Shell (Export Version) Microsoft Corporation
explorer.exe 13... 4.90 Windows Explorer Microsoft Corporation
qttask.exe 14... QuickTime Task Apple Inc.
ParallelsToolsCenter.exe 14... Parallels Tools Parallels Software International, Inc.
sharedintapp.exe 14... Parallels Shared Web Applications Helper Parallels Software International, Inc.
ctfmon.exe 14... CTF Loader Microsoft Corporation
msmsgs.exe 15... Windows Messenger Microsoft Corporation
autoruns.exe 560 Autostart program viewer Sysinternals - www.sysinternals.com
procexp.exe 712 Sysinternals Process Explorer Sysinternals
Tcpview.exe 14... 39.... TCP/UDP endpoint viewer Sysinternals
DFind.exe 13... 34....
CPU Usage: 100.00% Commit Charge: 14.25% Processes: 28

Process Checklist

- Things to look for:
  - no icon
  - no description
  - unverified “Microsoft” processes
  - live in the Windows directory
  - are packed
  - include suspicious strings

Process Checklist (2)

- Normal set of processes?
- www.liutilities.com/products/wintaskpro/processlibrary

Getting Rid of Processes

- Suspend/kill process
- Delete files
- Remove startup links
- Restart
- Repeat!

Anything Else ?

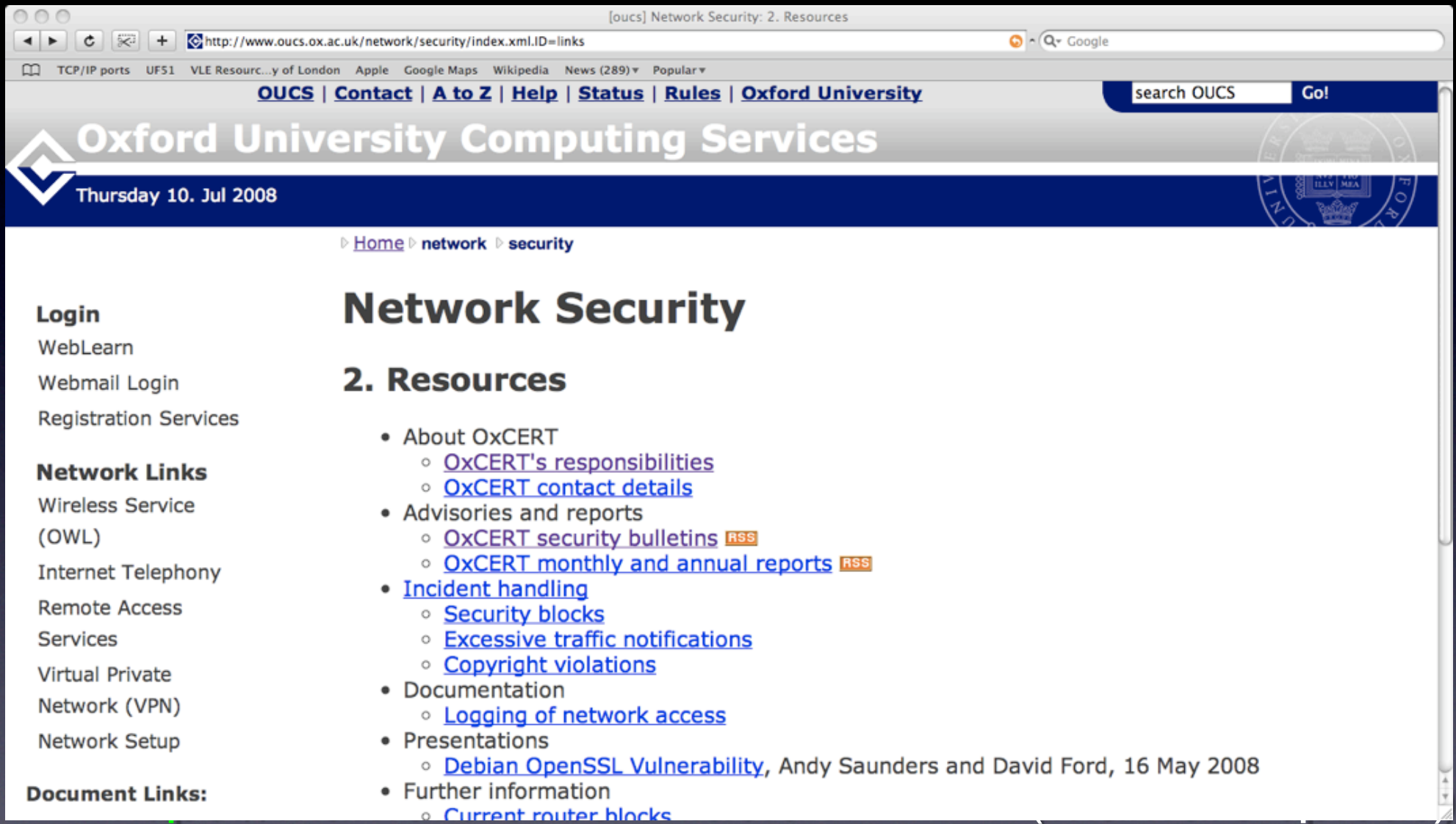
- Look in %systemroot%\recycled
  - or <anydrive>\recycled
  - ‘dir / AH / OD / P’
- Use Windows search
- Re-install OS

Contact us

- Daily/routine matters: security@oucs.ox.ac.uk
- jonathan.ashton@oucs.ox.ac.uk x83672
- robin.stevens@oucs.ox.ac.uk x73212
- david.ford@oucs.ox.ac.uk x73208

- http://www.oucs.ox.ac.uk/network/security
- http://www.ict.ox.ac.uk/oxford/compsecurity (web)
- https://malware.oucs.ox.ac.uk (malware upload)

Contact us


[oucs] Network Security: 2. Resources
http://www.oucs.ox.ac.uk/network/security/index.xml.ID=links
Google
TCP/IP ports
UF51
VLE Resourc...y of London
Apple
Google Maps
Wikipedia
News (289)
Popular
OUCS | Contact | A to Z | Help | Status | Rules | Oxford University
search OUCS
Go!
Oxford University Computing Services
Thursday 10. Jul 2008
Home network security
Login
WebLearn
Webmail Login
Registration Services
Network Links
Wireless Service (OWL)
Internet Telephony
Remote Access Services
Virtual Private Network (VPN)
Network Setup
Document Links:
Network Security
2. Resources
About OxCERT
OxCERT's responsibilities
OxCERT contact details
Advisories and reports
OxCERT security bulletins RSS
OxCERT monthly and annual reports RSS
Incident handling
Security blocks
Excessive traffic notifications
Copyright violations
Documentation
Logging of network access
Presentations
Debian OpenSSL Vulnerability, Andy Saunders and David Ford, 16 May 2008
Further information
Current router blocks

Contact us


http://www.oucs.ox.ac.u
TCP/IP ports
UFS1
VLE Resourc...y of London
OUCS | C
Oxford Unive
Thursday 10. Jul 2008
Login
WebLearn
Webmail Login
Registration Services
Network Links
Wireless Service (OWL)
Internet Telephony
Remote Access Services
Virtual Private Network (VPN)
Network Setup
Document Links:
OxCERT
IT Rules
Networks
OUCS
Go!
Network Security
ICT
oxford
compsecurity
Latest viruses and worms information
Symantec Security Response
Sophos Virus Information
McAfee Virus Information Library
Latest advisories and software security updates
CERT Current Activity, Vulnerabilities, Incidents and Fixes
BugTraq mailing list - Announcement and discussion of vulnerabilities: what they are, how to exploit them, how to fix them.
Seclists.org - Several mailing lists for discusssions of latest news, exploits. Includes archives.
LinuxSecurity.com Advisories - Latest advisories for most Linux distributions.
Microsoft Security Home Page - Incidents, security updates and news for Microsoft operating systems only.
WindowsITPro - Latest security issues and articles for Microsoft products.
Technical articles and white papers
Checking UNIX/Linux Systems for Signs of Compromise - Outlines concrete actions to take when dealing with a compromised *nix system. Includes links to essential tools.
Checking Microsoft Windows Systems for Signs of Compromise - Outlines concrete actions to take when dealing with a compromised Windows system. Includes links to essential tools.
CERT Security Improvement Modules - Provides step-by-step guidance to secure desktops and web servers, to detect signs of intrusion, to deploy firewalls and other issues.
FIRST Best Practice Guide Library - Set of security guides written by FIRST members.
US-CERT Reading Room and US-CERT Publications - Collection of security related articles and documents.
General resources
CERT Coordination Center - Reporting centre for internet security problems. Provides advice and solutions to security problems.
FIRST (Forum of Incident Response and Security Teams) - OxCERT is a member of FIRST.
SecurityFocus - Resource centre for vulneraibilities, exploits, secure practicies, tools.
Viruses Resources Centre (CERT document)
Top 100 Security Tools - Links to the most used security tools, for all Operating Systems.
European CERT Teams
Further information
Current router blocks

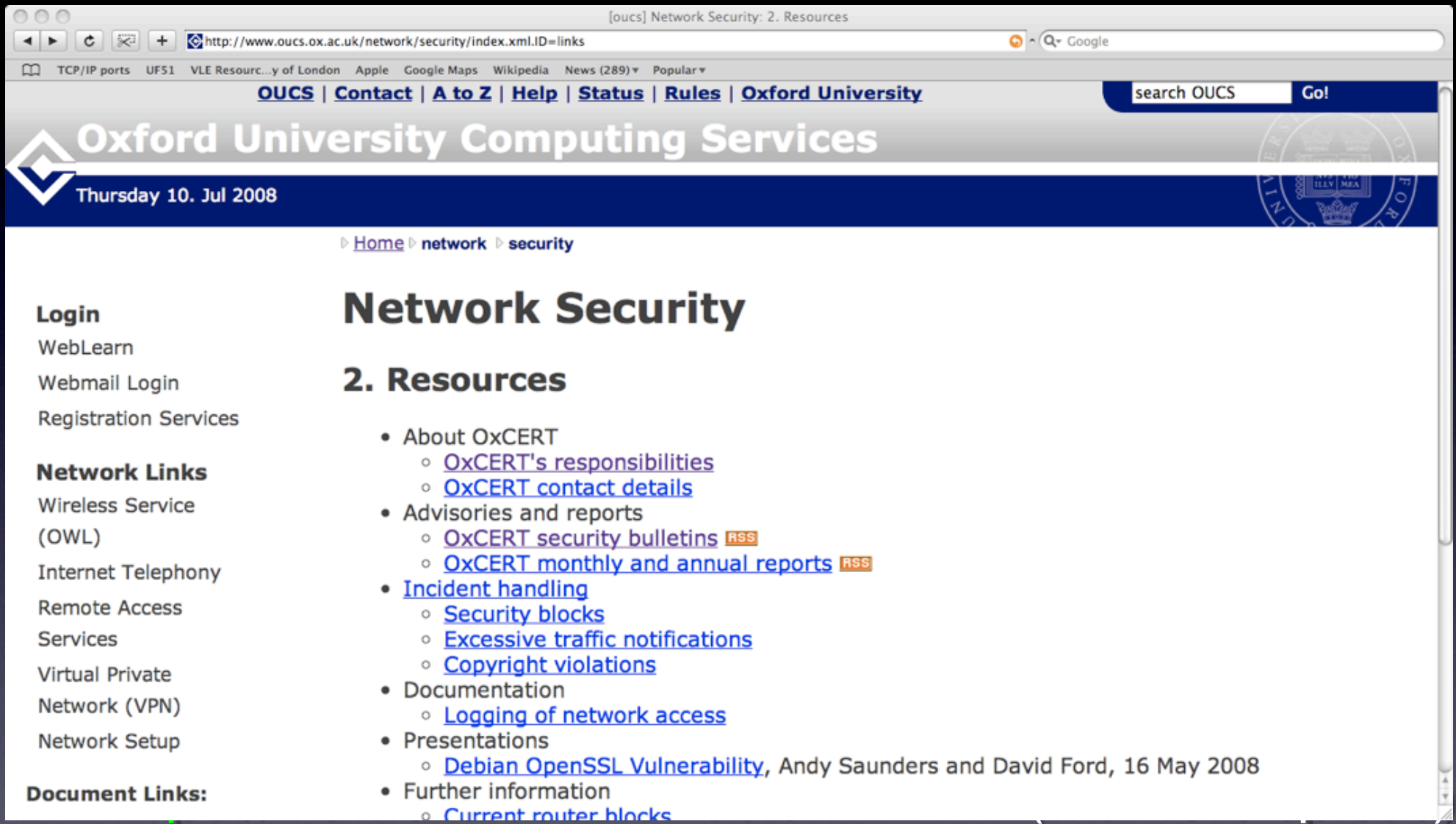
Contact us


Network Security
ICT
oxford
compsecurity
University of Oxford
Network Security - Malware Upload Service
The network security team is interested in getting a copy of malware files that IT officers may come across.
We are particularly interested in malware files that are not detected by anti-virus programs. After successfully analysing these files, we are able to take preemptive measures to protect the network from similar compromises.
Please feel free to include logs, temp files, binaries and other relevant files for any operating system. Only one file can be uploaded at a time. Please feel free to archive files together if necessary (.tar .zip etc).
Step 1 : Enter your email address
Step 2 : Add a comment (optional)
Step 3 : Choose a file to upload
Choose File
no file selected
Step 4 : Click "Upload File"
Upload File
How to contact the Network Security Team ?
security@oucs.ox.ac.uk for all "daily/routine" matters
oxcert@ox.ac.uk to report an incident ONLY (high priority)
probe-report@oxcert.ox.ac.uk to report port scans (lower priority)
Our PGP key and our full contact details are here.
Technical Papers
Checking Microsoft Windows Systems for Signs of Compromise
Checking UNIX/Linux Systems for Signs of Compromise
Links
Router Blocks
Firewall Blocks
Oxford University Network Security Web Site

Contact us


http://www.oucs.ox.ac.u
TCP/IP ports
UFS1
VLE Resourc...y of London
OUCS | C
Oxford Unive
Thursday 10. Jul 2008
Login
WebLearn
Webmail Login
Registration Services
Network Links
Wireless Service (OWL)
Internet Telephony
Remote Access Services
Virtual Private Network (VPN)
Network Setup
Document Links:
OxCERT
IT Rules
Networks
OUCS
Go!
Network Security
ICT
oxford
compsecurity
Latest viruses and worms information
Symantec Security Response
Sophos Virus Information
McAfee Virus Information Library
Latest advisories and software security updates
CERT Current Activity, Vulnerabilities, Incidents and Fixes
BugTraq mailing list - Announcement and discussion of vulnerabilities: what they are, how to exploit them, how to fix them.
Seclists.org - Several mailing lists for discusssions of latest news, exploits. Includes archives.
LinuxSecurity.com Advisories - Latest advisories for most Linux distributions.
Microsoft Security Home Page - Incidents, security updates and news for Microsoft operating systems only.
WindowsITPro - Latest security issues and articles for Microsoft products.
Technical articles and white papers
Checking UNIX/Linux Systems for Signs of Compromise - Outlines concrete actions to take when dealing with a compromised *nix system. Includes links to essential tools.
Checking Microsoft Windows Systems for Signs of Compromise - Outlines concrete actions to take when dealing with a compromised Windows system. Includes links to essential tools.
CERT Security Improvement Modules - Provides step-by-step guidance to secure desktops and web servers, to detect signs of intrusion, to deploy firewalls and other issues.
FIRST Best Practice Guide Library - Set of security guides written by FIRST members.
US-CERT Reading Room and US-CERT Publications - Collection of security related articles and documents.
General resources
CERT Coordination Center - Reporting centre for internet security problems. Provides advice and solutions to security problems.
FIRST (Forum of Incident Response and Security Teams) - OxCERT is a member of FIRST.
SecurityFocus - Resource centre for vulneraibilities, exploits, secure practicies, tools.
Viruses Resources Centre (CERT document)
Top 100 Security Tools - Links to the most used security tools, for all Operating Systems.
European CERT Teams
Further information
Current router blocks

Contact us


[oucs] Network Security: 2. Resources
http://www.oucs.ox.ac.uk/network/security/index.xml.ID=links
Google
TCP/IP ports
UF51
VLE Resourc...y of London
Apple
Google Maps
Wikipedia
News (289)
Popular
OUCS | Contact | A to Z | Help | Status | Rules | Oxford University
search OUCS
Go!
Oxford University Computing Services
Thursday 10. Jul 2008
Home network security
Login
WebLearn
Webmail Login
Registration Services
Network Links
Wireless Service (OWL)
Internet Telephony
Remote Access Services
Virtual Private Network (VPN)
Network Setup
Document Links:
Network Security
2. Resources
About OxCERT
OxCERT's responsibilities
OxCERT contact details
Advisories and reports
OxCERT security bulletins RSS
OxCERT monthly and annual reports RSS
Incident handling
Security blocks
Excessive traffic notifications
Copyright violations
Documentation
Logging of network access
Presentations
Debian OpenSSL Vulnerability, Andy Saunders and David Ford, 16 May 2008
Further information
Current router blocks

Contact us

- Daily/routine matters: security@oucs.ox.ac.uk
- jonathan.ashton@oucs.ox.ac.uk x83672
- robin.stevens@oucs.ox.ac.uk x73212
- david.ford@oucs.ox.ac.uk x73208

- http://www.oucs.ox.ac.uk/network/security
- http://www.ict.ox.ac.uk/oxford/compsecurity (web)
- https://malware.oucs.ox.ac.uk (malware upload)