Blue Teaming

King of the Hill Prep Week 2

Agenda

- Persistence
- Sysinternals things
- Windows Firewall

What is persistence?

- Attempting to maintain access to a device after exploitation
- Through reboot is the hard part
- Reduces the likelihood of burning an exploit
- Harder on some platforms than others

The Registry

- A weird windows thing
- Not really on disk (sorta)
- A hierarchical database, 5 root keys
  - HKLM - computer specific
  - HKCC - runtime info
  - HKCU - specific to the logged in user
  - HKCR - info for all registered users
  - HKU - all users
- Each hive has multiple keys under it

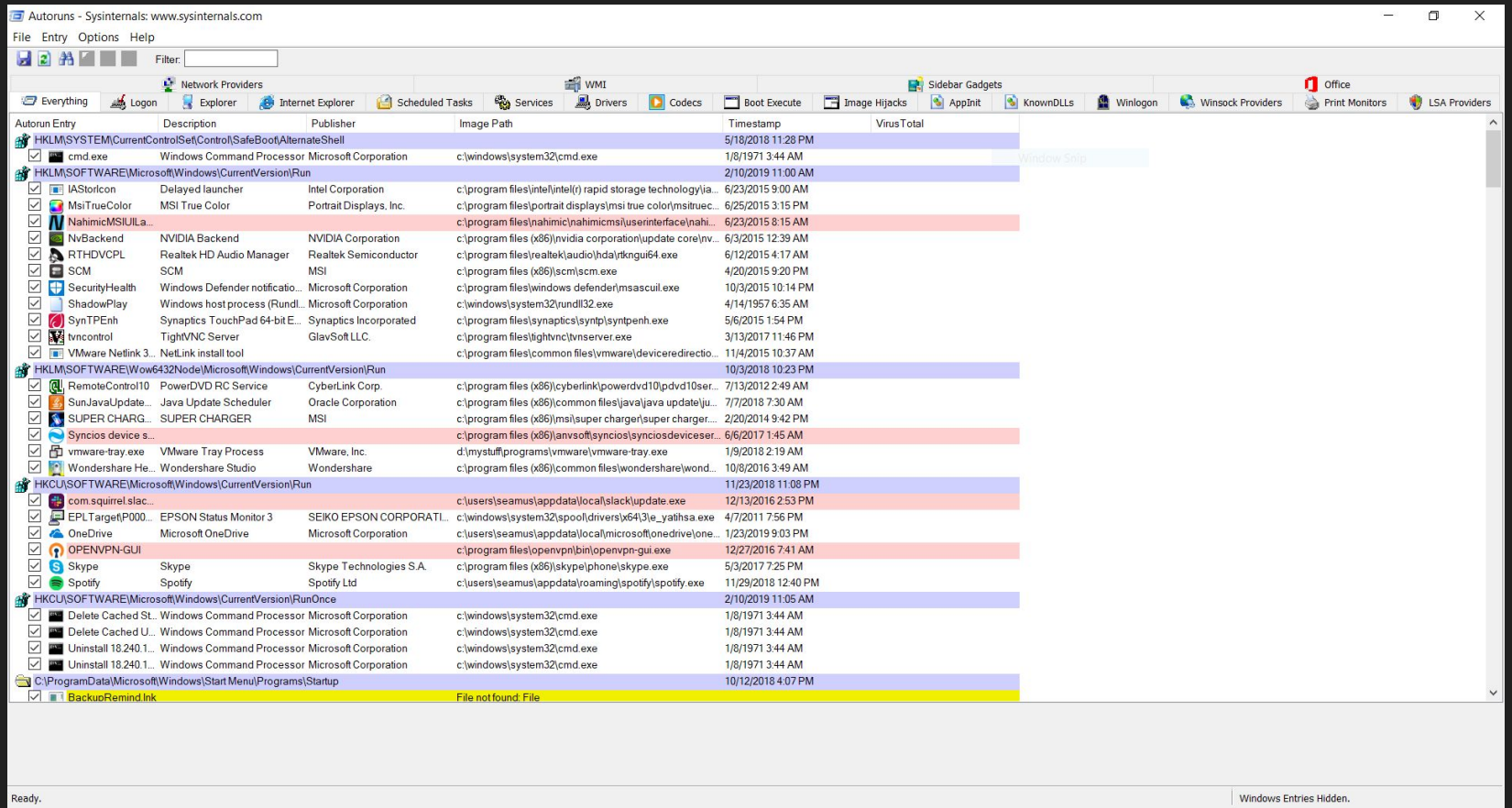
Persistence Techniques

- Services
- Scheduled Task
- Run keys/other registry keys
- DLL Hijacking

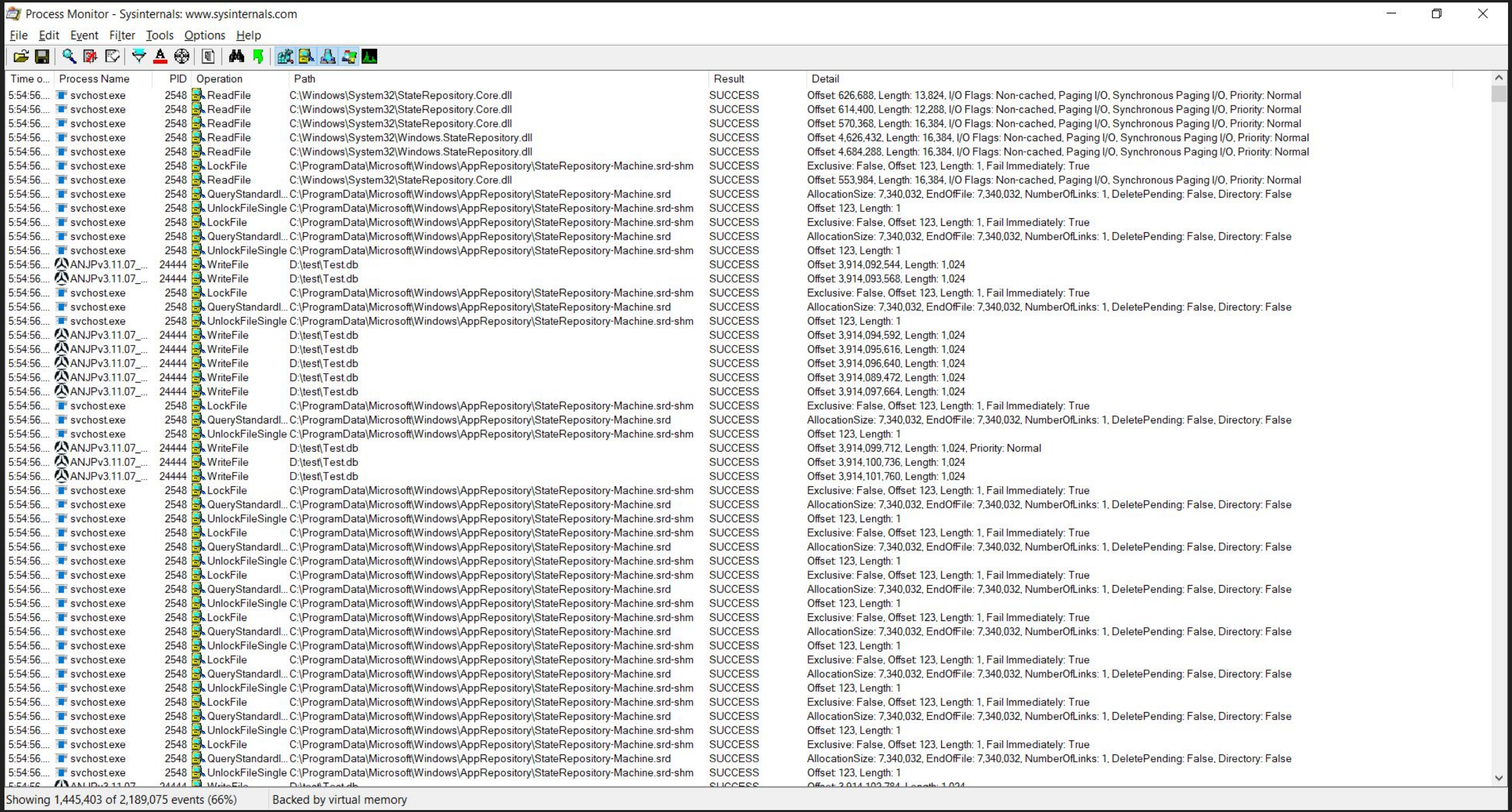
Sysinternals

- A set of tools to manage, monitor, and diagnose things in windows
- Created in 1996, updated for each version of windows
- Acquired by Microsoft and closed-sourced in 2006
- Really useful for both blue-teaming, and getting a better idea of how windows works
- live.sysinternals.com

Autoruns


Autoruns - Sysinternals: www.sysinternals.com
File Entry Options Help
Filter:
Network Providers
WMI
Sidebar Gadgets
Office
Everything
Logon
Explorer
Internet Explorer
Scheduled Tasks
Services
Drivers
Codecs
Boot Execute
Image Hijacks
AppInit
KnownDLLs
Winlogon
Winsock Providers
Print Monitors
LSA Providers
Autorun Entry
Description
Publisher
Image Path
Timestamp
VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell
5/18/2018 11:28 PM
cmd.exe
Windows Command Processor
Microsoft Corporation
c:\windows\system32\cmd.exe
1/8/1971 3:44 AM
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
2/10/2019 11:00 AM
IAStorIcon
Delayed launcher
Intel Corporation
c:\program files\intel\intel(r) rapid storage technology\ia...
6/23/2015 9:00 AM
MsiTrueColor
MSI True Color
Portrait Displays, Inc.
c:\program files\portrait displays\msi true color\msitruec...
6/25/2015 3:15 PM
NahimicMSIUILa...
c:\program files\nahimic\nahimicmsi\userinterface\nahi...
6/23/2015 8:15 AM
NvBackend
NVIDIA Backend
NVIDIA Corporation
c:\program files (x86)\nvidia corporation\update core\nv...
6/3/2015 12:39 AM
RTHDVCPL
Realtek HD Audio Manager
Realtek Semiconductor
c:\program files\realtek\audio\hda\rtkngui64.exe
6/12/2015 4:17 AM
SCM
SCM
MSI
c:\program files (x86)\scm\scm.exe
4/20/2015 9:20 PM
SecurityHealth
Windows Defender notificatio...
Microsoft Corporation
c:\program files\windows defender\msascuil.exe
10/3/2015 10:14 PM
ShadowPlay
Windows host process (Rundl...
Microsoft Corporation
c:\windows\system32\rundll32.exe
4/14/1957 6:35 AM
SynTPEnh
Synaptics TouchPad 64-bit E...
Synaptics Incorporated
c:\program files\synaptics\syntp\syntpenh.exe
5/6/2015 1:54 PM
tvncontrol
TightVNC Server
GlavSoft LLC.
c:\program files\tightvnc\tvnserver.exe
3/13/2017 11:46 PM
VMware Netlink 3...
NetLink install tool
c:\program files\common files\vmware\deviceredirectio...
11/4/2015 10:37 AM
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
10/3/2018 10:23 PM
RemoteControl10
PowerDVD RC Service
CyberLink Corp.
c:\program files (x86)\cyberlink\powerdvd10\pdvd10ser...
7/13/2012 2:49 AM
SunJavaUpdate...
Java Update Scheduler
Oracle Corporation
c:\program files (x86)\common files\java\java update\ju...
7/7/2018 7:30 AM
SUPER CHARG...
SUPER CHARGER
MSI
c:\program files (x86)\msi\super charger\super charger....
2/20/2014 9:42 PM
Syncios device s...
c:\program files (x86)\anvsoft\syncios\synciosdeviceser...
6/6/2017 1:45 AM
vmware-tray.exe
VMware Tray Process
VMware, Inc.
d:\mystuff\programs\vmware\vmware-tray.exe
1/9/2018 2:19 AM
Wondershare He...
Wondershare Studio
Wondershare
c:\program files (x86)\common files\wondershare\wond...
10/8/2016 3:49 AM
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
11/23/2018 11:08 PM
com.squirrel.slac...
c:\users\seamus\appdata\local\slack\update.exe
12/13/2016 2:53 PM
EPLTarget\P000...
EPSON Status Monitor 3
SEIKO EPSON CORPORATI...
c:\windows\system32\spool\drivers\x64\3\e_yatihsa.exe
4/7/2011 7:56 PM
OneDrive
Microsoft OneDrive
Microsoft Corporation
c:\users\seamus\appdata\local\microsoft\onedrive\one...
1/23/2019 9:03 PM
OPENVPN-GUI
c:\program files\openvpn\bin\openvpn-gui.exe
12/27/2016 7:41 AM
Skype
Skype
Skype Technologies S.A.
c:\program files (x86)\skype\phone\skype.exe
5/3/2017 7:25 PM
Spotify
Spotify
Spotify Ltd
c:\users\seamus\appdata\roaming\spotify\spotify.exe
11/29/2018 12:40 PM
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
2/10/2019 11:05 AM
Delete Cached St...
Windows Command Processor
Microsoft Corporation
c:\windows\system32\cmd.exe
1/8/1971 3:44 AM
Delete Cached U...
Windows Command Processor
Microsoft Corporation
c:\windows\system32\cmd.exe
1/8/1971 3:44 AM
Uninstall 18.240.1...
Windows Command Processor
Microsoft Corporation
c:\windows\system32\cmd.exe
1/8/1971 3:44 AM
Uninstall 18.240.1...
Windows Command Processor
Microsoft Corporation
c:\windows\system32\cmd.exe
1/8/1971 3:44 AM
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
10/12/2018 4:07 PM
BackupRemind.lnk
File not found: File
Ready.
Windows Entries Hidden.

Procmon



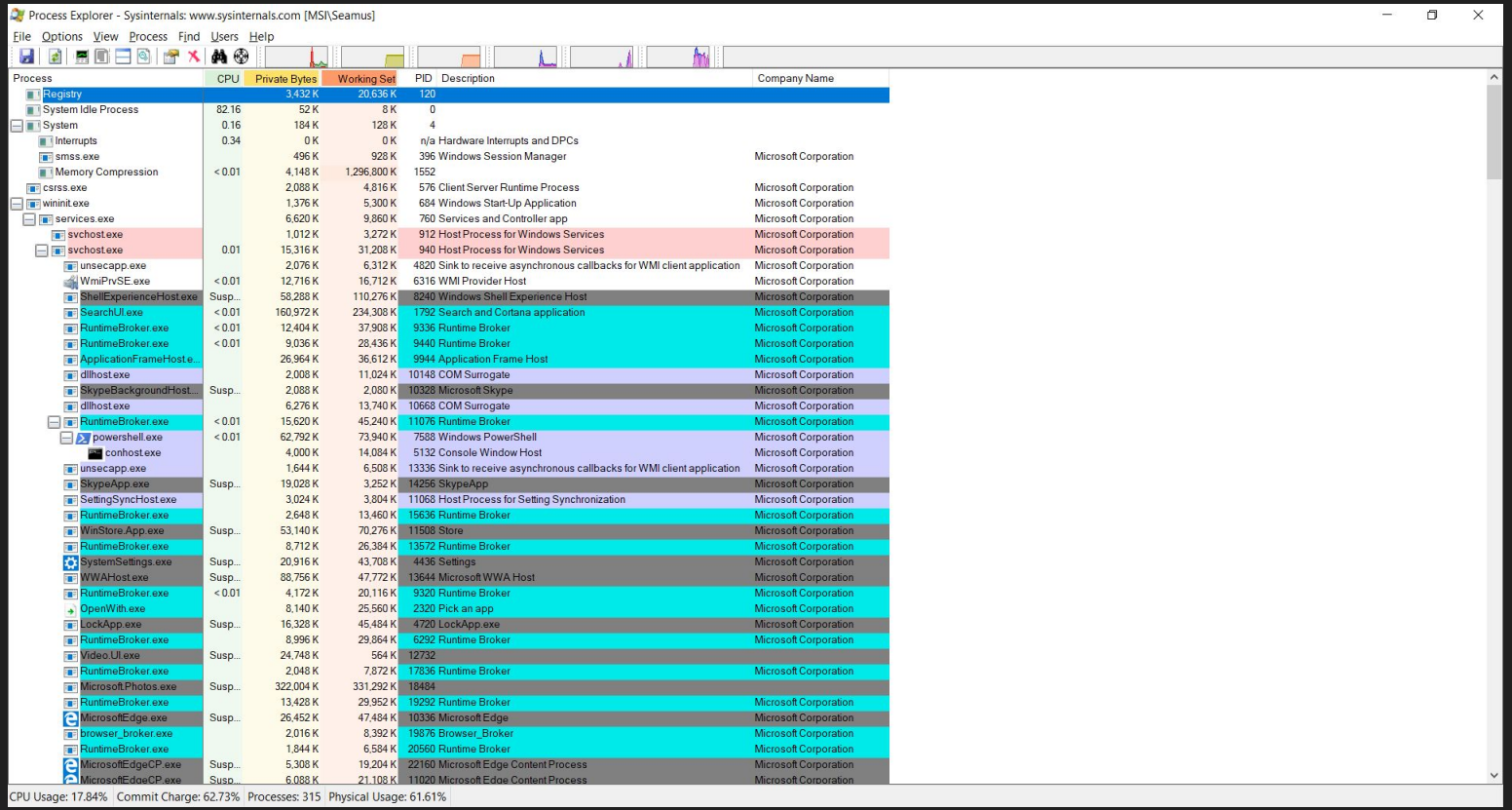
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

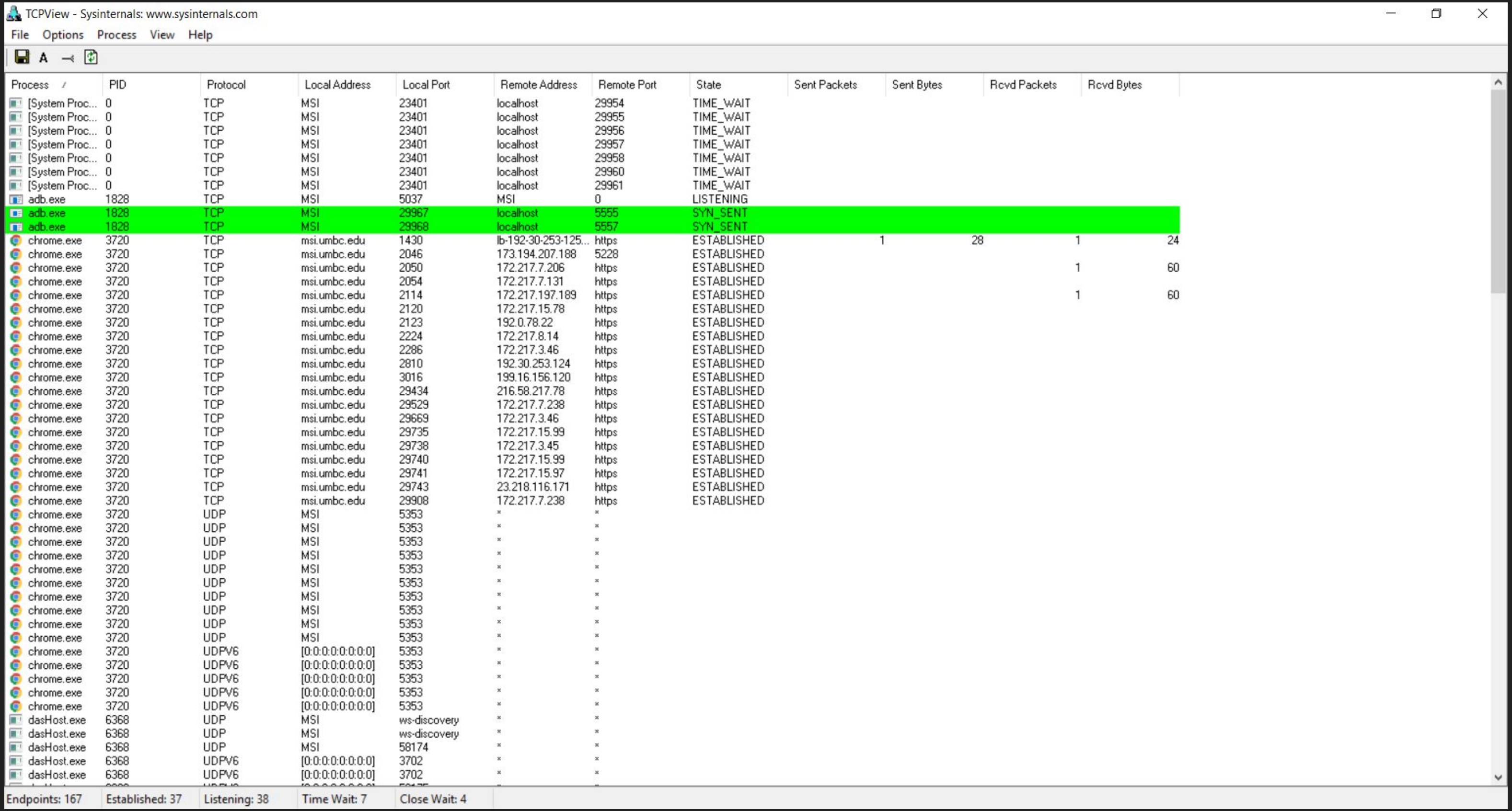
Time o...	Process Name	PID	Operation	Path	Result	Detail
5:54:56....	svchost.exe	2548	ReadFile	C:\Windows\System32\StateRepository.Core.dll	SUCCESS	Offset: 626,688, Length: 13,824, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
5:54:56....	svchost.exe	2548	ReadFile	C:\Windows\System32\StateRepository.Core.dll	SUCCESS	Offset: 614,400, Length: 12,288, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
5:54:56....	svchost.exe	2548	ReadFile	C:\Windows\System32\StateRepository.Core.dll	SUCCESS	Offset: 570,368, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
5:54:56....	svchost.exe	2548	ReadFile	C:\Windows\System32\Windows.StateRepository.dll	SUCCESS	Offset: 4,626,432, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
5:54:56....	svchost.exe	2548	ReadFile	C:\Windows\System32\Windows.StateRepository.dll	SUCCESS	Offset: 4,684,288, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
5:54:56....	svchost.exe	2548	LockFile	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Exclusive: False, Offset: 123, Length: 1, Fail Immediately: True
5:54:56....	svchost.exe	2548	ReadFile	C:\Windows\System32\StateRepository.Core.dll	SUCCESS	Offset: 553,984, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
5:54:56....	svchost.exe	2548	QueryStandardI...	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd	SUCCESS	AllocationSize: 7,340,032, EndOfFile: 7,340,032, NumberOfLinks: 1, DeletePending: False, Directory: False
5:54:56....	svchost.exe	2548	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Offset: 123, Length: 1
5:54:56....	svchost.exe	2548	LockFile	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Exclusive: False, Offset: 123, Length: 1, Fail Immediately: True
5:54:56....	svchost.exe	2548	QueryStandardI...	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd	SUCCESS	AllocationSize: 7,340,032, EndOfFile: 7,340,032, NumberOfLinks: 1, DeletePending: False, Directory: False
5:54:56....	svchost.exe	2548	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Offset: 123, Length: 1
5:54:56....	ANJPv3.11.07_...	24444	WriteFile	D:\test\Test.db	SUCCESS	Offset: 3,914,092,544, Length: 1,024
5:54:56....	ANJPv3.11.07_...	24444	WriteFile	D:\test\Test.db	SUCCESS	Offset: 3,914,093,568, Length: 1,024
5:54:56....	svchost.exe	2548	LockFile	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Exclusive: False, Offset: 123, Length: 1, Fail Immediately: True
5:54:56....	svchost.exe	2548	QueryStandardI...	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd	SUCCESS	AllocationSize: 7,340,032, EndOfFile: 7,340,032, NumberOfLinks: 1, DeletePending: False, Directory: False
5:54:56....	svchost.exe	2548	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Offset: 123, Length: 1
5:54:56....	ANJPv3.11.07_...	24444	WriteFile	D:\test\Test.db	SUCCESS	Offset: 3,914,094,592, Length: 1,024
5:54:56....	ANJPv3.11.07_...	24444	WriteFile	D:\test\Test.db	SUCCESS	Offset: 3,914,095,616, Length: 1,024
5:54:56....	ANJPv3.11.07_...	24444	WriteFile	D:\test\Test.db	SUCCESS	Offset: 3,914,096,640, Length: 1,024
5:54:56....	ANJPv3.11.07_...	24444	WriteFile	D:\test\Test.db	SUCCESS	Offset: 3,914,089,472, Length: 1,024
5:54:56....	ANJPv3.11.07_...	24444	WriteFile	D:\test\Test.db	SUCCESS	Offset: 3,914,097,664, Length: 1,024
5:54:56....	svchost.exe	2548	LockFile	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Exclusive: False, Offset: 123, Length: 1, Fail Immediately: True
5:54:56....	svchost.exe	2548	QueryStandardI...	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd	SUCCESS	AllocationSize: 7,340,032, EndOfFile: 7,340,032, NumberOfLinks: 1, DeletePending: False, Directory: False
5:54:56....	svchost.exe	2548	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Offset: 123, Length: 1
5:54:56....	ANJPv3.11.07_...	24444	WriteFile	D:\test\Test.db	SUCCESS	Offset: 3,914,099,712, Length: 1,024, Priority: Normal
5:54:56....	ANJPv3.11.07_...	24444	WriteFile	D:\test\Test.db	SUCCESS	Offset: 3,914,100,736, Length: 1,024
5:54:56....	ANJPv3.11.07_...	24444	WriteFile	D:\test\Test.db	SUCCESS	Offset: 3,914,101,760, Length: 1,024
5:54:56....	svchost.exe	2548	LockFile	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Exclusive: False, Offset: 123, Length: 1, Fail Immediately: True
5:54:56....	svchost.exe	2548	QueryStandardI...	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd	SUCCESS	AllocationSize: 7,340,032, EndOfFile: 7,340,032, NumberOfLinks: 1, DeletePending: False, Directory: False
5:54:56....	svchost.exe	2548	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Offset: 123, Length: 1
5:54:56....	svchost.exe	2548	LockFile	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Exclusive: False, Offset: 123, Length: 1, Fail Immediately: True
5:54:56....	svchost.exe	2548	QueryStandardI...	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd	SUCCESS	AllocationSize: 7,340,032, EndOfFile: 7,340,032, NumberOfLinks: 1, DeletePending: False, Directory: False
5:54:56....	svchost.exe	2548	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Offset: 123, Length: 1
5:54:56....	svchost.exe	2548	LockFile	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Exclusive: False, Offset: 123, Length: 1, Fail Immediately: True
5:54:56....	svchost.exe	2548	QueryStandardI...	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd	SUCCESS	AllocationSize: 7,340,032, EndOfFile: 7,340,032, NumberOfLinks: 1, DeletePending: False, Directory: False
5:54:56....	svchost.exe	2548	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Offset: 123, Length: 1
5:54:56....	svchost.exe	2548	LockFile	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Exclusive: False, Offset: 123, Length: 1, Fail Immediately: True
5:54:56....	svchost.exe	2548	QueryStandardI...	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd	SUCCESS	AllocationSize: 7,340,032, EndOfFile: 7,340,032, NumberOfLinks: 1, DeletePending: False, Directory: False
5:54:56....	svchost.exe	2548	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Offset: 123, Length: 1
5:54:56....	svchost.exe	2548	LockFile	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Exclusive: False, Offset: 123, Length: 1, Fail Immediately: True
5:54:56....	svchost.exe	2548	QueryStandardI...	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd	SUCCESS	AllocationSize: 7,340,032, EndOfFile: 7,340,032, NumberOfLinks: 1, DeletePending: False, Directory: False
5:54:56....	svchost.exe	2548	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Offset: 123, Length: 1
5:54:56....	svchost.exe	2548	LockFile	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Exclusive: False, Offset: 123, Length: 1, Fail Immediately: True
5:54:56....	svchost.exe	2548	QueryStandardI...	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd	SUCCESS	AllocationSize: 7,340,032, EndOfFile: 7,340,032, NumberOfLinks: 1, DeletePending: False, Directory: False
5:54:56....	svchost.exe	2548	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Offset: 123, Length: 1
5:54:56....	svchost.exe	2548	LockFile	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Exclusive: False, Offset: 123, Length: 1, Fail Immediately: True
5:54:56....	svchost.exe	2548	QueryStandardI...	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd	SUCCESS	AllocationSize: 7,340,032, EndOfFile: 7,340,032, NumberOfLinks: 1, DeletePending: False, Directory: False
5:54:56....	svchost.exe	2548	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-shm	SUCCESS	Offset: 123, Length: 1

Showing 1,445,403 of 2,189,075 events (66%) Backed by virtual memory

ProcExp


Process Explorer - Sysinternals: www.sysinternals.com [MSI\Seamus]
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description Company Name
Registry 3,432 K 20,636 K 120
System Idle Process 82.16 52 K 8 K 0
System 0.16 184 K 128 K 4
Interrupts 0.34 0 K 0 K n/a Hardware Interrupts and DPCs
smss.exe 496 K 928 K 396 Windows Session Manager Microsoft Corporation
Memory Compression < 0.01 4,148 K 1,296,800 K 1552
csrss.exe 2,088 K 4,816 K 576 Client Server Runtime Process Microsoft Corporation
wininit.exe 1,376 K 5,300 K 684 Windows Start-Up Application Microsoft Corporation
services.exe 6,620 K 9,860 K 760 Services and Controller app Microsoft Corporation
svchost.exe 1,012 K 3,272 K 912 Host Process for Windows Services Microsoft Corporation
svchost.exe 0.01 15,316 K 31,208 K 940 Host Process for Windows Services Microsoft Corporation
unsecapp.exe 2,076 K 6,312 K 4820 Sink to receive asynchronous callbacks for WMI client application Microsoft Corporation
WmiPrvSE.exe < 0.01 12,716 K 16,712 K 6316 WMI Provider Host Microsoft Corporation
ShellExperienceHost.exe Susp... 58,288 K 110,276 K 8240 Windows Shell Experience Host Microsoft Corporation
SearchUI.exe < 0.01 160,972 K 234,308 K 1792 Search and Cortana application Microsoft Corporation
RuntimeBroker.exe < 0.01 12,404 K 37,908 K 9336 Runtime Broker Microsoft Corporation
RuntimeBroker.exe < 0.01 9,036 K 28,436 K 9440 Runtime Broker Microsoft Corporation
ApplicationFrameHost.e... 26,964 K 36,612 K 9944 Application Frame Host Microsoft Corporation
dllhost.exe 2,008 K 11,024 K 10148 COM Surrogate Microsoft Corporation
SkypeBackgroundHost.... Susp... 2,088 K 2,080 K 10328 Microsoft Skype Microsoft Corporation
dllhost.exe 6,276 K 13,740 K 10668 COM Surrogate Microsoft Corporation
RuntimeBroker.exe < 0.01 15,620 K 45,240 K 11076 Runtime Broker Microsoft Corporation
powershell.exe < 0.01 62,792 K 73,940 K 7588 Windows PowerShell Microsoft Corporation
conhost.exe 4,000 K 14,084 K 5132 Console Window Host Microsoft Corporation
unsecapp.exe 1,644 K 6,508 K 13336 Sink to receive asynchronous callbacks for WMI client application Microsoft Corporation
SkypeApp.exe Susp... 19,028 K 3,252 K 14256 SkypeApp Microsoft Corporation
SettingSyncHost.exe 3,024 K 3,804 K 11068 Host Process for Setting Synchronization Microsoft Corporation
RuntimeBroker.exe 2,648 K 13,460 K 15636 Runtime Broker Microsoft Corporation
WinStore.App.exe Susp... 53,140 K 70,276 K 11508 Store Microsoft Corporation
RuntimeBroker.exe 8,712 K 26,384 K 13572 Runtime Broker Microsoft Corporation
SystemSettings.exe Susp... 20,916 K 43,708 K 4436 Settings Microsoft Corporation
WWAHost.exe Susp... 88,756 K 47,772 K 13644 Microsoft WWA Host Microsoft Corporation
RuntimeBroker.exe < 0.01 4,172 K 20,116 K 9320 Runtime Broker Microsoft Corporation
OpenWith.exe 8,140 K 25,560 K 2320 Pick an app Microsoft Corporation
LockApp.exe Susp... 16,328 K 45,484 K 4720 LockApp.exe Microsoft Corporation
RuntimeBroker.exe 8,996 K 29,864 K 6292 Runtime Broker Microsoft Corporation
Video.UI.exe Susp... 24,748 K 564 K 12732
RuntimeBroker.exe 2,048 K 7,872 K 17836 Runtime Broker Microsoft Corporation
Microsoft.Photos.exe Susp... 322,004 K 331,292 K 18484
RuntimeBroker.exe 13,428 K 29,952 K 19292 Runtime Broker Microsoft Corporation
MicrosoftEdge.exe Susp... 26,452 K 47,484 K 10336 Microsoft Edge Microsoft Corporation
browser_broker.exe 2,016 K 8,392 K 19876 Browser_Broker Microsoft Corporation
RuntimeBroker.exe 1,844 K 6,584 K 20560 Runtime Broker Microsoft Corporation
MicrosoftEdgeCP.exe Susp... 5,308 K 19,204 K 22160 Microsoft Edge Content Process Microsoft Corporation
MicrosoftEdgeCP.exe Susp... 6,088 K 21,108 K 11020 Microsoft Edge Content Process Microsoft Corporation
CPU Usage: 17.84% Commit Charge: 62.73% Processes: 315 Physical Usage: 61.61%

TcpView



TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Proc...	0	TCP	MSI	23401	localhost	29954	TIME_WAIT				
[System Proc...	0	TCP	MSI	23401	localhost	29955	TIME_WAIT				
[System Proc...	0	TCP	MSI	23401	localhost	29956	TIME_WAIT				
[System Proc...	0	TCP	MSI	23401	localhost	29957	TIME_WAIT				
[System Proc...	0	TCP	MSI	23401	localhost	29958	TIME_WAIT				
[System Proc...	0	TCP	MSI	23401	localhost	29960	TIME_WAIT				
[System Proc...	0	TCP	MSI	23401	localhost	29961	TIME_WAIT				
adb.exe	1828	TCP	MSI	5037	MSI	0	LISTENING				
adb.exe	1828	TCP	MSI	29967	localhost	5555	SYN_SENT				
adb.exe	1828	TCP	MSI	29968	localhost	5557	SYN_SENT				
chrome.exe	3720	TCP	msi.umbc.edu	1430	lb-192-30-253-125...	https	ESTABLISHED	1	28	1	24
chrome.exe	3720	TCP	msi.umbc.edu	2046	173.194.207.188	5228	ESTABLISHED				
chrome.exe	3720	TCP	msi.umbc.edu	2050	172.217.7.206	https	ESTABLISHED			1	60
chrome.exe	3720	TCP	msi.umbc.edu	2054	172.217.7.131	https	ESTABLISHED				
chrome.exe	3720	TCP	msi.umbc.edu	2114	172.217.197.189	https	ESTABLISHED			1	60
chrome.exe	3720	TCP	msi.umbc.edu	2120	172.217.15.78	https	ESTABLISHED				
chrome.exe	3720	TCP	msi.umbc.edu	2123	192.0.78.22	https	ESTABLISHED				
chrome.exe	3720	TCP	msi.umbc.edu	2224	172.217.8.14	https	ESTABLISHED				
chrome.exe	3720	TCP	msi.umbc.edu	2286	172.217.3.46	https	ESTABLISHED				
chrome.exe	3720	TCP	msi.umbc.edu	2810	192.30.253.124	https	ESTABLISHED				
chrome.exe	3720	TCP	msi.umbc.edu	3016	199.16.156.120	https	ESTABLISHED				
chrome.exe	3720	TCP	msi.umbc.edu	29434	216.58.217.78	https	ESTABLISHED				
chrome.exe	3720	TCP	msi.umbc.edu	29529	172.217.7.238	https	ESTABLISHED				
chrome.exe	3720	TCP	msi.umbc.edu	29669	172.217.3.46	https	ESTABLISHED				
chrome.exe	3720	TCP	msi.umbc.edu	29735	172.217.15.99	https	ESTABLISHED				
chrome.exe	3720	TCP	msi.umbc.edu	29738	172.217.3.45	https	ESTABLISHED				
chrome.exe	3720	TCP	msi.umbc.edu	29740	172.217.15.99	https	ESTABLISHED				
chrome.exe	3720	TCP	msi.umbc.edu	29741	172.217.15.97	https	ESTABLISHED				
chrome.exe	3720	TCP	msi.umbc.edu	29743	23.218.116.171	https	ESTABLISHED				
chrome.exe	3720	TCP	msi.umbc.edu	29908	172.217.7.238	https	ESTABLISHED				
chrome.exe	3720	UDP	MSI	5353	*	*					
chrome.exe	3720	UDP	MSI	5353	*	*					
chrome.exe	3720	UDP	MSI	5353	*	*					
chrome.exe	3720	UDP	MSI	5353	*	*					
chrome.exe	3720	UDP	MSI	5353	*	*					
chrome.exe	3720	UDP	MSI	5353	*	*					
chrome.exe	3720	UDP	MSI	5353	*	*					
chrome.exe	3720	UDP	MSI	5353	*	*					
chrome.exe	3720	UDP	MSI	5353	*	*					
chrome.exe	3720	UDP	MSI	5353	*	*					
chrome.exe	3720	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*					
chrome.exe	3720	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*					
chrome.exe	3720	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*					
chrome.exe	3720	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*					
chrome.exe	3720	UDPV6	[0:0:0:0:0:0:0:0]	5353	*	*					
dasHost.exe	6368	UDP	MSI	ws-discovery	*	*					
dasHost.exe	6368	UDP	MSI	ws-discovery	*	*					
dasHost.exe	6368	UDP	MSI	58174	*	*					
dasHost.exe	6368	UDPV6	[0:0:0:0:0:0:0:0]	3702	*	*					
dasHost.exe	6368	UDPV6	[0:0:0:0:0:0:0:0]	3702	*	*					

Endpoints: 167 | Established: 37 | Listening: 38 | Time Wait: 7 | Close Wait: 4

Other Notable Sysinternals Tools

- PsExec - useful for running commands as someone else
  - On remote computers
  - Or elevating your privs
- RAMMap - shows a map of how the system RAM is being used
- VMMap - shows the memory space of a specfic process
- SysMon

SysMon Magic

- Service + Driver that stays persistent across reboots, and logs things to the windows event log
- Really powerful since it gives you a lot more configuration over what to log then the default windows logs do
- Sort of a poor mans EDR
  - Much cheaper than ~~Clownstrike~~ Crowdstrike Falcon, Cylance, etc

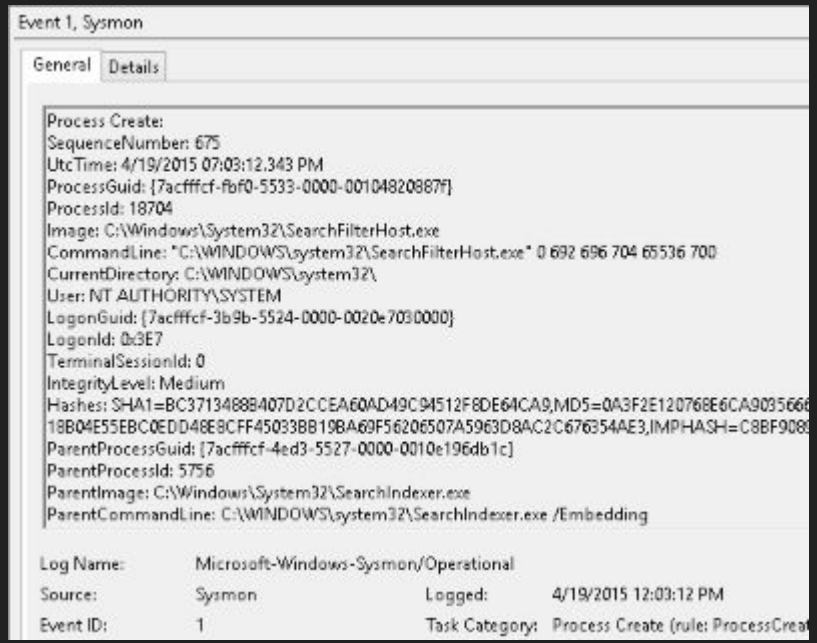
Sysmon can log lots of things

- Process creation with full command line
- The hash of the process image
- Use process GUID instead of PID
- Log driver loads AND DIls, with hashes
- Logs opening physical devices for raw access
- Log network connections and associated metadata
- Detects file modification
- Logs early on boot to catch more sophisticated malware

Sysmon Cont’d

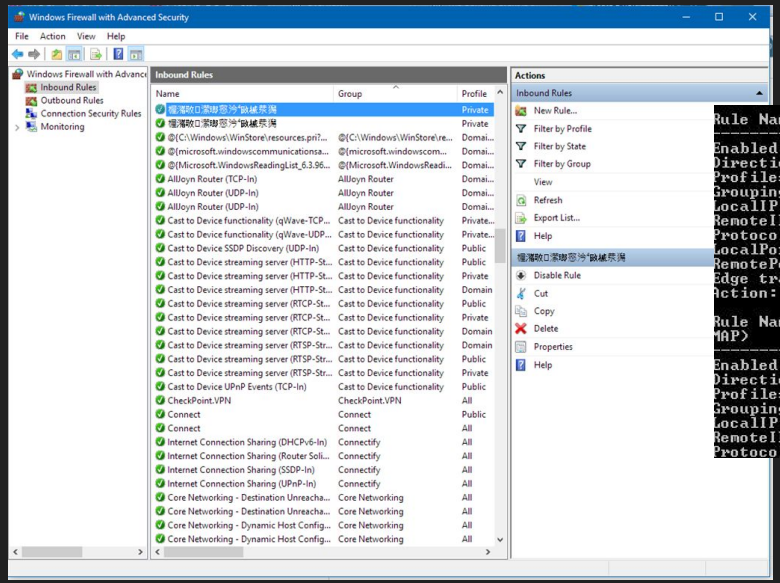
- Configured via XML, time consuming

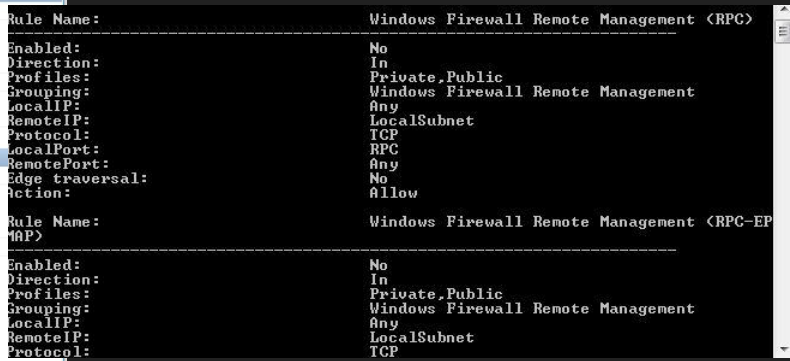
```
<Sysmon  schemaversion="3.2">
  <!-- Capture all the hashes -->
  <HashAlgorithms>*</HashAlgorithms>
  <EventFiltering>
    <!-- Log all drivers except if the signature -->
    <!-- contains Microsoft or Windows -->
    <DriverLoad onmatch="exclude">
      <Signature condition="contains">microsoft</Signature>
      <Signature condition="contains">windows</Signature>
    </DriverLoad>
    <!-- Do not log process termination -->
    <ProcessTerminate onmatch="include"/>
    <!-- Log network connection if the destination port equals 443 -->
    <!-- or 80, and the process isn't InternetExplorer -->
    <NetworkConnect onmatch="include">
      <DestinationPort>443</DestinationPort>
      <DestinationPort>80</DestinationPort>
    </NetworkConnect>
    <NetworkConnect onmatch="exclude">
      <Image condition="end with">iexplore.exe</Image>
    </NetworkConnect>
  </EventFiltering>
</Sysmon>
```



Firewalls and Windows

- Have two firewall options, and two options for management
- Windows Firewall - XP/2003
- Windows Firewall with Advanced Security (WFAS) - Vista+





Windows Firewall Basics

- 3 separate profiles
  - Domain
  - Public
  - Private
- 4 types of rules
  - Program - block or allow a specific program
  - Port - block or allow a port, range of ports, OR a protocol
  - Predefined - these come with windows
  - Custom - combination of program, port, IP address, or protocol
- Direction - can specify in the rule