

Cyber Defense Organization



Windows Primer Worksheet - Liam Smith 4/10/2019

tinyurl.com/CDOSpr19WindowsPrimer

Worksheet	2
What you need	2
What am I trying to do?	2
Windows Firewall	3
Services	5
Command Line	7
Getting Started	7
CMD Basics	7
Common Commands	7
Net Suite	8
Core NET Suite	8
SysInternals	10
Process Explorer	11
Autoruns	11
TCP View	12
Event Viewer	13
Event Logs	13
Firewall Through Command Line	16
Networking and Firewall	16

Worksheet

What you need

Any windows machine (above windows home edition) should have all of these tools and commands. Some may not work if they are not part of a Window Active Directory Domain. I have tried to make this worksheet completely "Service-free" so no DNS/AD/DHCP/WSUS/IIS/PLSHELP/SCCM.

What am I trying to do?

#	Goal		
1	Window Firewall		
	Identify and explain several windows firewall rules Create a rule to allow all ICMP traffic. Change the Logging Location to the Desktop		
2	Services		
	Open the Services, and find services related to computer networking. Stop them. Find services that start at boot. Explain the Different startup types. Explain the different service state types. Stop Services until you break the computer.		
3	Command Line		
	Show Processes. Show listening ports. Tell Liam why ipconfig is better than ifconfig. Kill Processes until the computer breaks.	NET: Create a new user Find workstation information, hostname etc. Local Groups Admin Users	
4	Sysinternals - Download them all!		
	Process Explorer	TCP View	AutoRuns

	Find one interesting process, and tell me everything about it. Run everything through virus total	Idc just explain to me what is happening	Find 3 things there, and google till you can explain why they are good/bad.
--	---	--	---

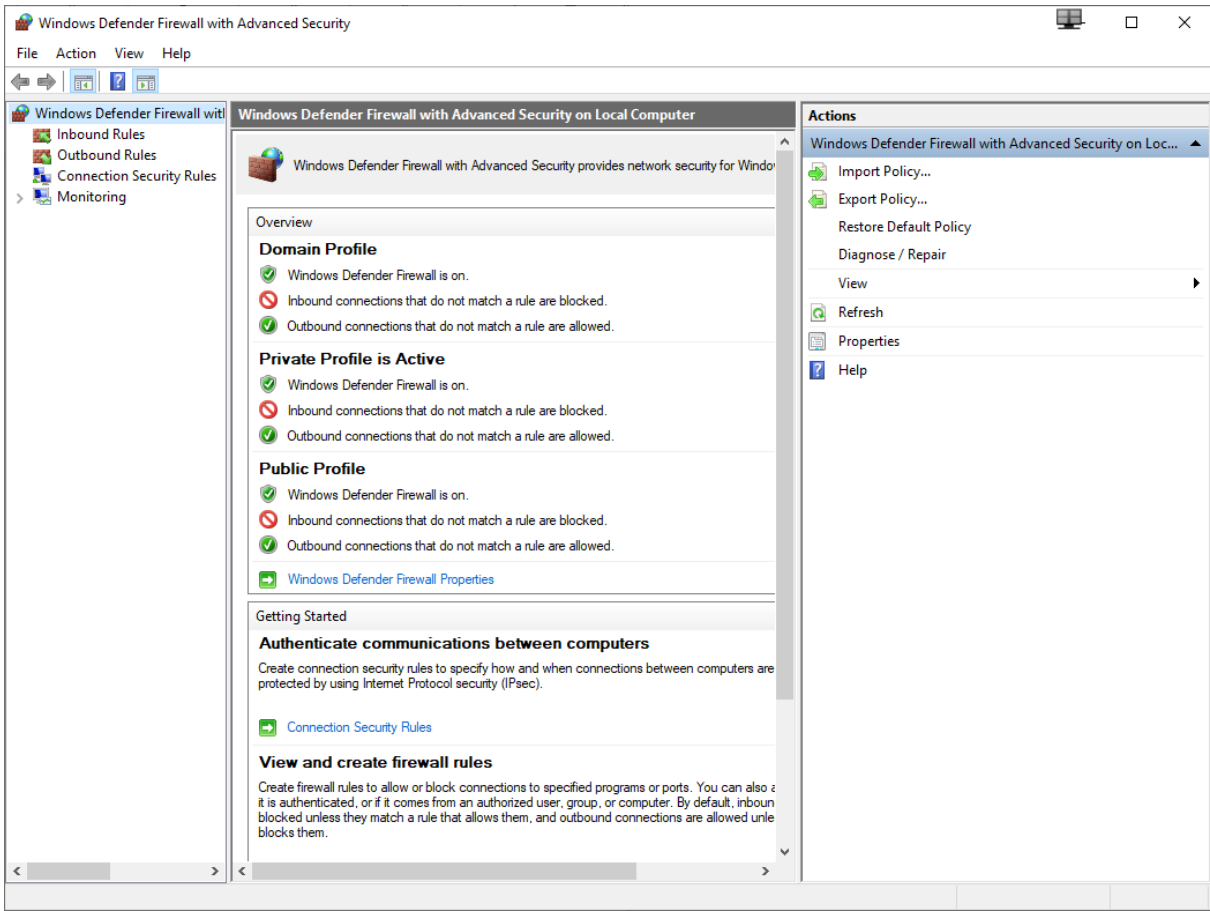
Windows Firewall

Windows Firewall is an application that filters information coming to your system from the Internet and blocking potentially harmful programs. The software blocks most programs from communicating through the firewall.

This is first in the list for a reason! The firewall should become your new best friend. <3 ... well, it's my only friend. Anyway, it can do a lot of stuff, and if you “get good” at understanding, auditing, creating, administering, it, you are well on your way.

To open: **Windows Key + R -> WF.msc**

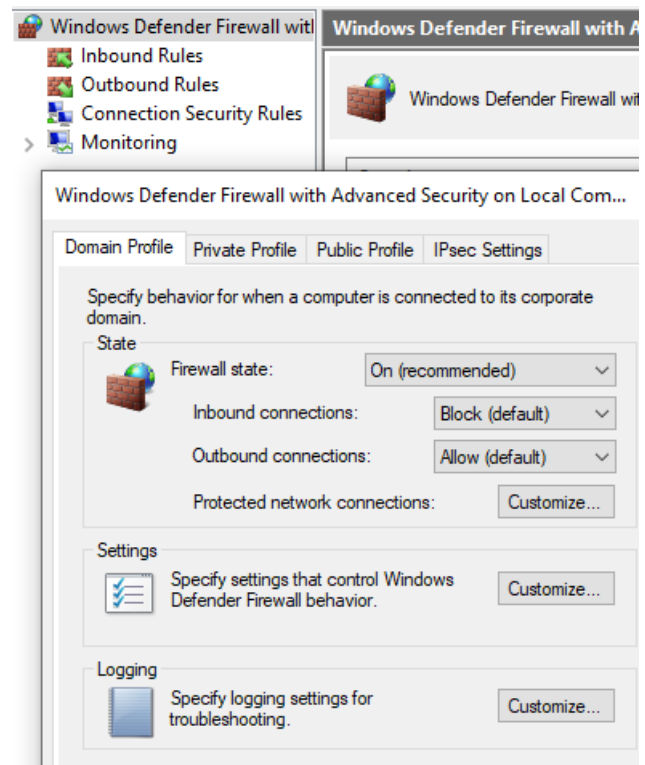
You have three different profiles - **Domain, Private Public**. These are three different “States” the firewall can be in. For the most part, the firewall will be operating with “Domain”.



Inbound Rules - Applied to traffic that is coming from the network to the device.

Outbound Rules - Applied to programs attempting to leave the machine and “talk out”.

If you do - **Windows Defender Firewall + RightClick -> properties.** You can see the settings of each profile. Including logging.

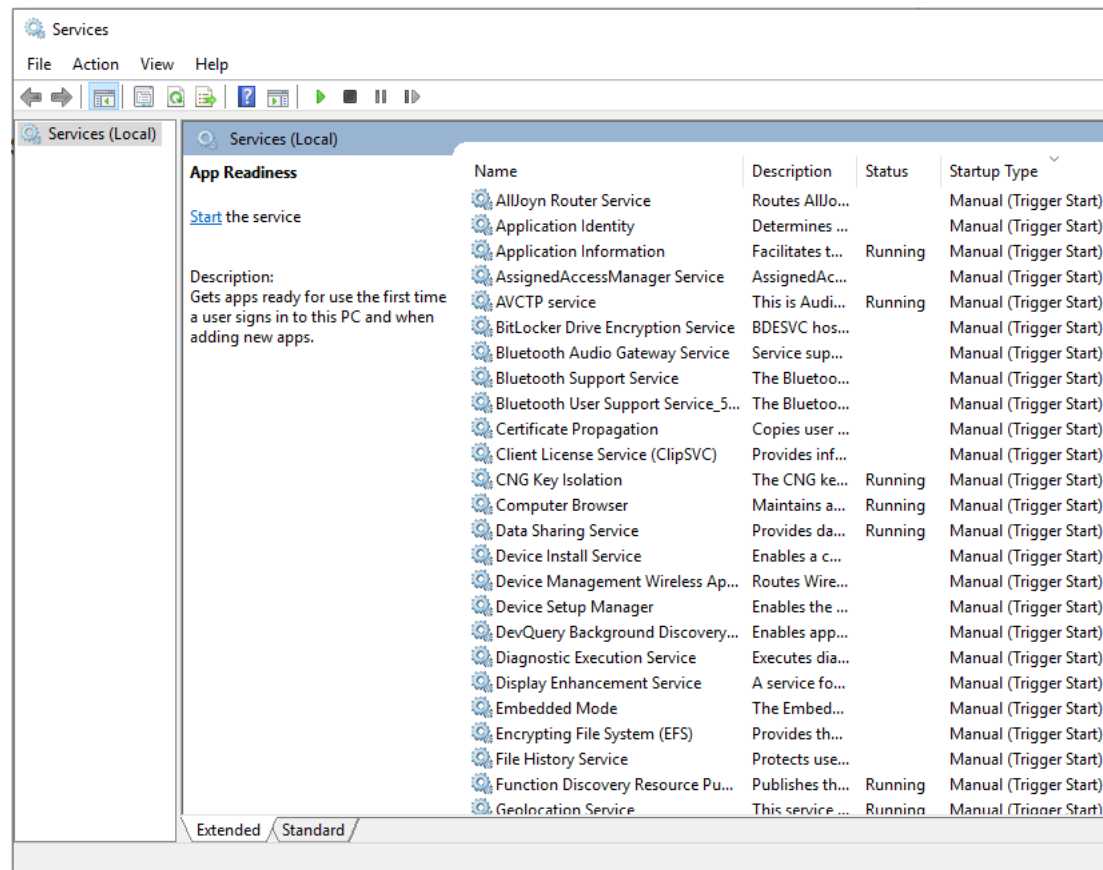


Services

Windows service is a computer program, which will run in the background.

Why windows service?

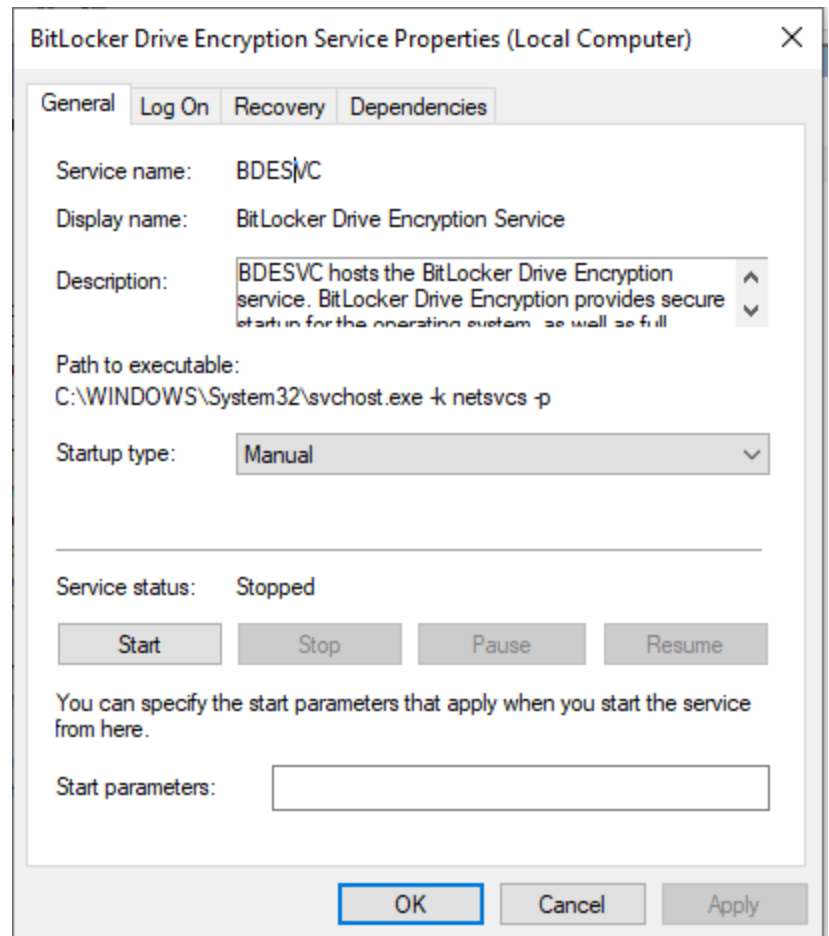
When some action has to be performed at a particular time, or need to be performed continuously in a specific time interval without user interaction then the solution is Windows service. As windows service will run in the background, the programming logic which we have written will be executed in the specified time interval without user interaction.



To open: **Windows Key + R -> services.msc**

You can **RightClick on a service + Properties**. To see the Name, description, startup type, location, and more! And control the service.

Every service is started by a user, most of the time "Local System Account" which is the lowest level user.



Command Line

Getting Started

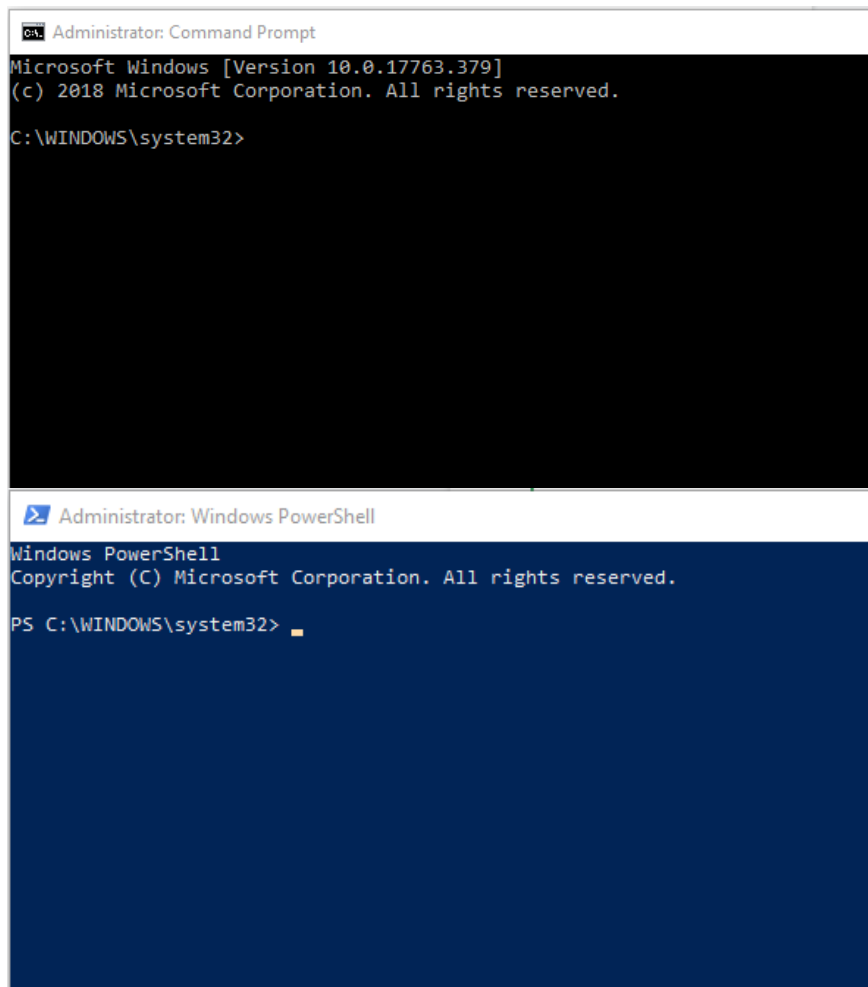
When using the command line in windows, you have two options: Comand Prompt and PowerShell.

Make sure you Right+Click -> Run As Administrator.

You can tell the difference from Admin vs Normal level by looking at the top line “Administrator: Command Prompt”

[Cheat Sheet.](#)

CMD Basics



cd	Print Working Directory
dir	List Directory Contents
cls	Clear the Prompt
shutdown /r	Shutdown

Common Commands

Command	Explained	Command	Explained
Tasklist	List Proccess	ping	Ping a machine

Taskkill	Kill a process with PID	del	Delete a file
nslookup	Lookup DNS Record	rmdir	Remove Directory
ipconfig /all	Network Configuration	copy	Copy a files.
tracert	Traceroute	tree	See directory Contents
systeminfo	See Systeminfo	attrib	see
find	Grep equivalent, Find a string	Schtasks	List all scheduled Tasks
hostname	See hostname		

Net Suite

The net suite is one of the most powerful sets of command on the Command Prompt. Learning it will be worth your time!

```
C:\Users\William Smith>net
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

All of the prompts start with “net.”

Core NET Suite

Task	Command
Get help on all the parts	Net help <command>
Groups that exist on the machine	net localgroup Net localgroup <group>
Groups on the Domain	net group net group <group name>
Output of the workstation config	net config workstation
See all shares on the machine	net share NET SHARE <share> NET SHARE <share> \delete
List users on the machine	Net user /active:{yes no} /passwordchg:{yes no} (can user change thier password)

	/logonpasswordchg:{yes no} /workstations:{computername[,...] *} (what computer can you log onto)
List all sessions connected to this machine	NET SESSION
Disconnect all sessions connected to this machine (without any prompts)	NET SESSION /DELETE /y
Create user for one machine	Net user <username> * /add /passwordchg:no /workstations:<machine> Net group "Domain Admins" <User> /add /domain

SysInternals

The Sysinternals web site was created in 1996 by Mark Russinovich to host his advanced system utilities and technical information. Whether you're an IT Pro or a developer, you'll find Sysinternals utilities to help you manage, troubleshoot and diagnose your Windows systems and applications.

An amazing talk, (warning long), [Malware Hunting with the Sysinternals Tools](#).

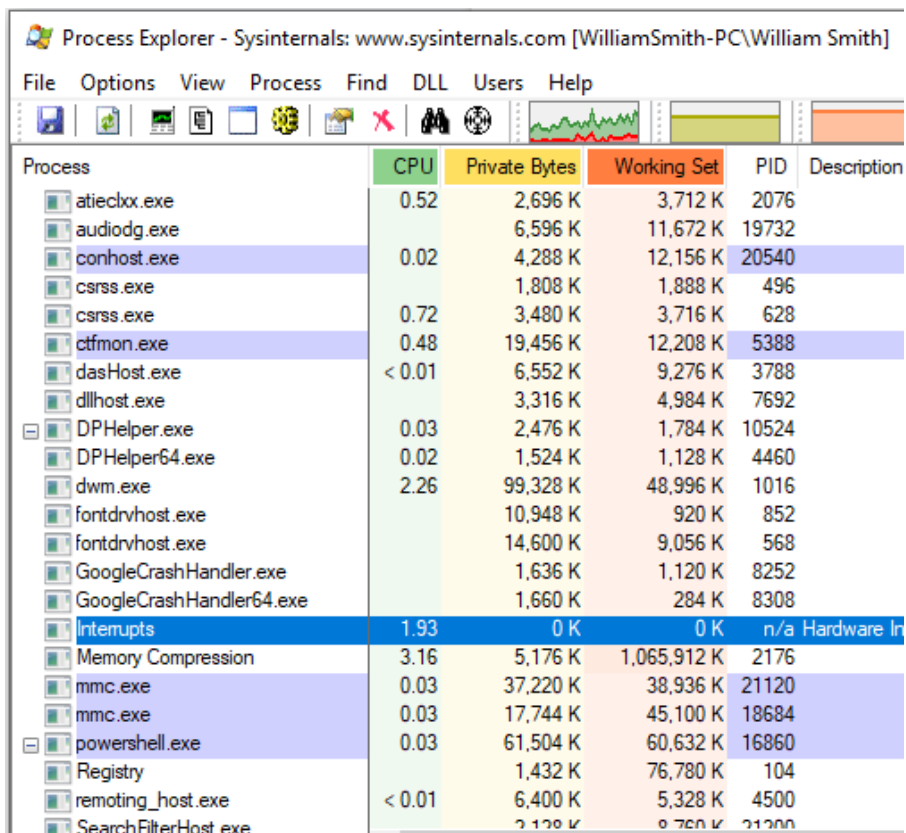
Download here: <https://live.sysinternals.com/>

Tool Name	Function
procexp.exe	Process explorer basically a better task manager.
autoruns.exe	See all of the activities that run at boot.
Tcpview.exe	See all connections. A better netstat.
Procmon.exe	Process Monitor, very advanced tool, can see everything the machine is doing.

Process Explorer

Process Explorer can be used to track down problems. For example, it provides a means to list or search for named resources that are held by a process or all processes. This can be used to track down what is holding a file open and preventing its use by another program. As another example, it can show the command lines used to start a program, allowing otherwise identical processes to be distinguished.

A great introduction to process explorer, [here](#).



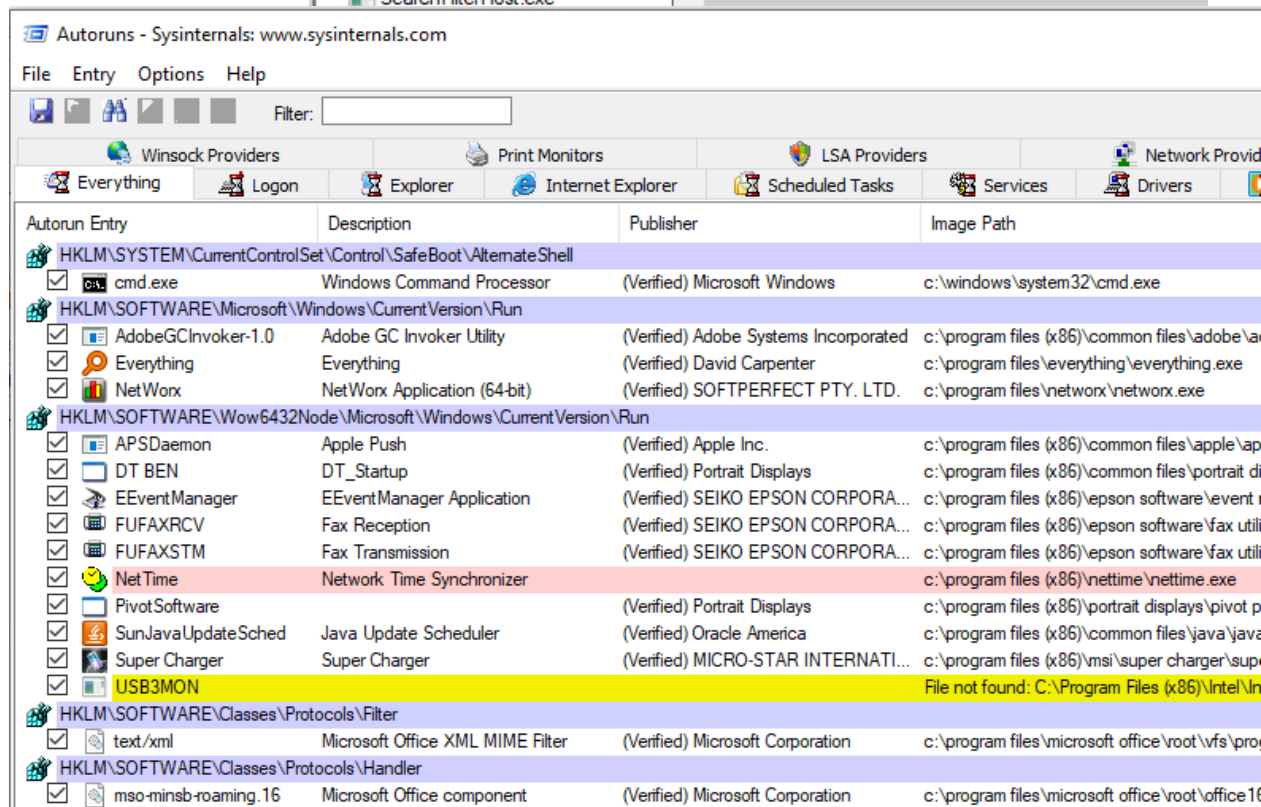
Process Explorer - Sysinternals: www.sysinternals.com [WilliamSmith-PC\William Smith]

File Options View Process Find DLL Users Help

Process	CPU	Private Bytes	Working Set	PID	Description
atieclxx.exe	0.52	2,696 K	3,712 K	2076	
audiodg.exe		6,596 K	11,672 K	19732	
conhost.exe	0.02	4,288 K	12,156 K	20540	
csrss.exe		1,808 K	1,888 K	496	
csrss.exe	0.72	3,480 K	3,716 K	628	
ctfmon.exe	0.48	19,456 K	12,208 K	5388	
dasHost.exe	< 0.01	6,552 K	9,276 K	3788	
dllhost.exe		3,316 K	4,984 K	7692	
DPHelper.exe	0.03	2,476 K	1,784 K	10524	
DPHelper64.exe	0.02	1,524 K	1,128 K	4460	
dwm.exe	2.26	99,328 K	48,996 K	1016	
fontdrvhost.exe		10,948 K	920 K	852	
fontdrvhost.exe		14,600 K	9,056 K	568	
GoogleCrashHandler.exe		1,636 K	1,120 K	8252	
GoogleCrashHandler64.exe		1,660 K	284 K	8308	
Interrupts	1.93	0 K	0 K	n/a	Hardware Interrupts
Memory Compression	3.16	5,176 K	1,065,912 K	2176	
mmc.exe	0.03	37,220 K	38,936 K	21120	
mmc.exe	0.03	17,744 K	45,100 K	18684	
powershell.exe	0.03	61,504 K	60,632 K	16860	
Registry		1,432 K	76,780 K	104	
remoting_host.exe	< 0.01	6,400 K	5,328 K	4500	
SearchFilterHost.exe		2,120 K	8,760 K	21200	

Autoruns

This utility, which has the most comprehensive knowledge of auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login, and when you start various built-in Windows applications like Internet Explorer, Explorer and media players. These programs and drivers include



Autoruns - Sysinternals: www.sysinternals.com

File Entry Options Help

Filter:

Winsock Providers Print Monitors LSA Providers Network Providers

Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers

Autorun Entry	Description	Publisher	Image Path
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell			
<input checked="" type="checkbox"/> cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> AdobeGCInvoker-1.0	Adobe GC Invoker Utility	(Verified) Adobe Systems Incorporated	c:\program files (x86)\common files\adobe\ap...
<input checked="" type="checkbox"/> Everything	Everything	(Verified) David Carpenter	c:\program files\everything\everything.exe
<input checked="" type="checkbox"/> NetWorx	NetWorx Application (64-bit)	(Verified) SOFTPERFECT PTY. LTD.	c:\program files\networx\networx.exe
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run			
<input checked="" type="checkbox"/> APSDaemon	Apple Push	(Verified) Apple Inc.	c:\program files (x86)\common files\apple\ap...
<input checked="" type="checkbox"/> DT BEN	DT_Startup	(Verified) Portrait Displays	c:\program files (x86)\common files\portrait di...
<input checked="" type="checkbox"/> EEventManager	EEventManager Application	(Verified) SEIKO EPSON CORPORA...	c:\program files (x86)\epson software\event...
<input checked="" type="checkbox"/> FUFAXRCV	Fax Reception	(Verified) SEIKO EPSON CORPORA...	c:\program files (x86)\epson software\xfax uti...
<input checked="" type="checkbox"/> FUFAXSTM	Fax Transmission	(Verified) SEIKO EPSON CORPORA...	c:\program files (x86)\epson software\xfax uti...
<input checked="" type="checkbox"/> NetTime	Network Time Synchronizer		c:\program files (x86)\nettime\nettime.exe
<input checked="" type="checkbox"/> PivotSoftware		(Verified) Portrait Displays	c:\program files (x86)\portrait displays\pivot p...
<input checked="" type="checkbox"/> SunJavaUpdateSched	Java Update Scheduler	(Verified) Oracle America	c:\program files (x86)\common files\java\java...
<input checked="" type="checkbox"/> Super Charger	Super Charger	(Verified) MICRO-STAR INTERNATI...	c:\program files (x86)\msi\super charger\sup...
<input checked="" type="checkbox"/> USB3MON			File not found: C:\Program Files (x86)\Intel\In...
HKLM\SOFTWARE\Classes\Protocols\Filter			
<input checked="" type="checkbox"/> text/xml	Microsoft Office XML MIME Filter	(Verified) Microsoft Corporation	c:\program files\microsoft office\root\vfs\pro...
HKLM\SOFTWARE\Classes\Protocols\Handler			
<input checked="" type="checkbox"/> mso-minsb-roaming.16	Microsoft Office component	(Verified) Microsoft Corporation	c:\program files\microsoft office\root\office 16...

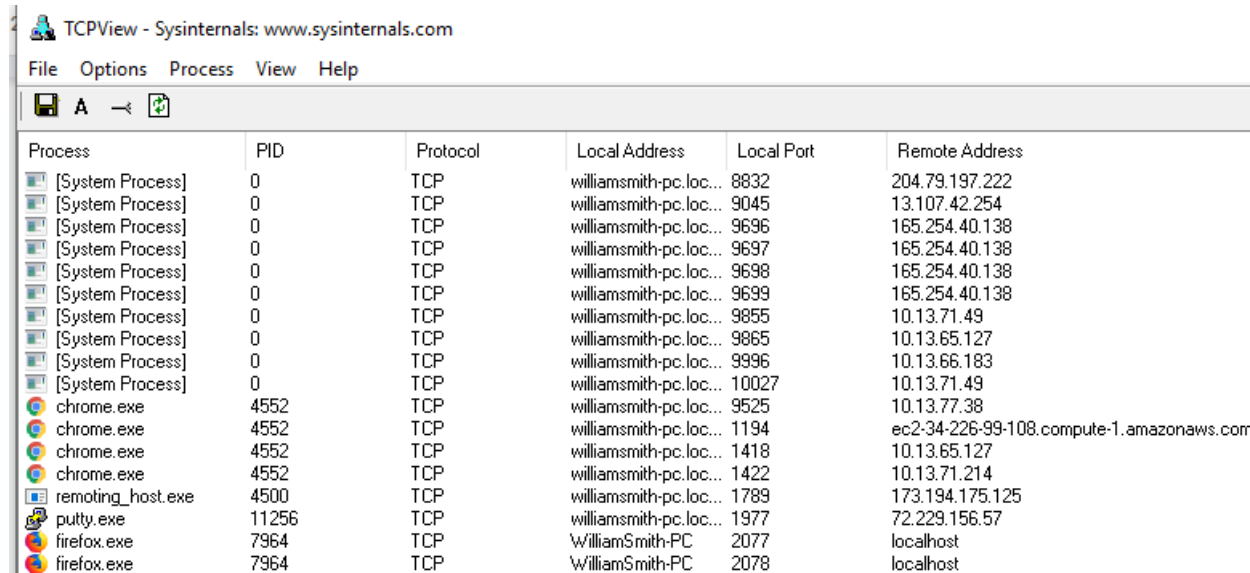
ones in your startup folder, Run, RunOnce, and other Registry keys. Autoruns reports Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, auto-start services, and much more. Autoruns goes way beyond other autostart utilities.

Introduction to Autoruns [here](#). And an interesting talk on evading it [here](#).

TCP View

TL;DR a better netstat.

Play with it. Idk man. I have like 30 minutes before the meeting.

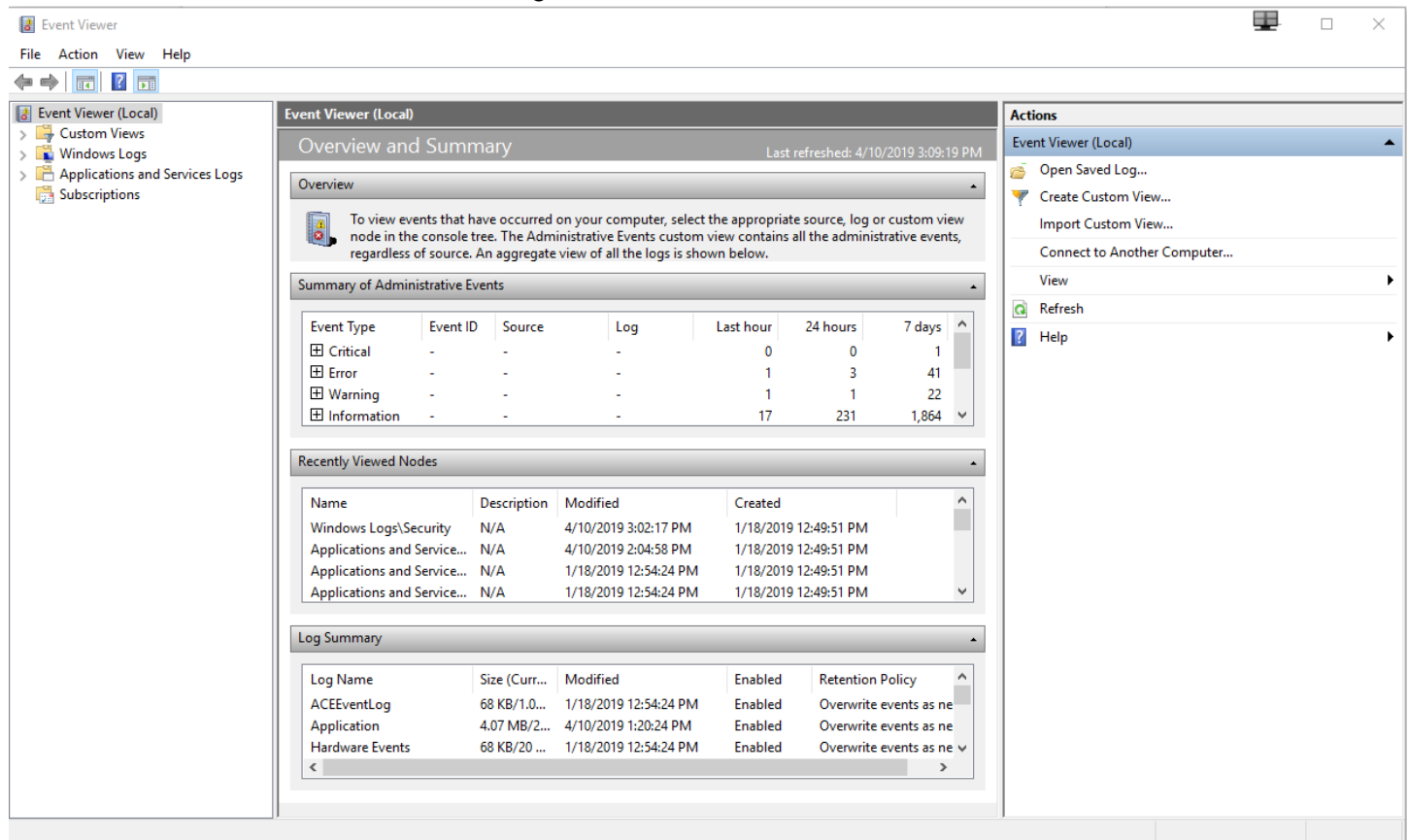


The screenshot shows the TCPView application window from Sysinternals. The title bar reads 'TCPView - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Options', 'Process', 'View', and 'Help'. Below the menu bar is a toolbar with icons for saving, refreshing, and other functions. The main area is a table with the following columns: Process, PID, Protocol, Local Address, Local Port, and Remote Address. The table lists various system processes and user applications like chrome.exe, remoting_host.exe, putty.exe, and firefox.exe, along with their active network connections.

Process	PID	Protocol	Local Address	Local Port	Remote Address
[System Process]	0	TCP	williamsmith-pc.loc...	8832	204.79.197.222
[System Process]	0	TCP	williamsmith-pc.loc...	9045	13.107.42.254
[System Process]	0	TCP	williamsmith-pc.loc...	9696	165.254.40.138
[System Process]	0	TCP	williamsmith-pc.loc...	9697	165.254.40.138
[System Process]	0	TCP	williamsmith-pc.loc...	9698	165.254.40.138
[System Process]	0	TCP	williamsmith-pc.loc...	9699	165.254.40.138
[System Process]	0	TCP	williamsmith-pc.loc...	9855	10.13.71.49
[System Process]	0	TCP	williamsmith-pc.loc...	9865	10.13.65.127
[System Process]	0	TCP	williamsmith-pc.loc...	9996	10.13.66.183
[System Process]	0	TCP	williamsmith-pc.loc...	10027	10.13.71.49
chrome.exe	4552	TCP	williamsmith-pc.loc...	9525	10.13.77.38
chrome.exe	4552	TCP	williamsmith-pc.loc...	1194	ec2-34-226-99-108.compute-1.amazonaws.com
chrome.exe	4552	TCP	williamsmith-pc.loc...	1418	10.13.65.127
chrome.exe	4552	TCP	williamsmith-pc.loc...	1422	10.13.71.214
remoting_host.exe	4500	TCP	williamsmith-pc.loc...	1789	173.194.175.125
putty.exe	11256	TCP	williamsmith-pc.loc...	1977	72.229.156.57
firefox.exe	7964	TCP	WilliamSmith-PC	2077	localhost
firefox.exe	7964	TCP	WilliamSmith-PC	2078	localhost

Event Viewer

All of the events that a windows machine generates* are able to be viewed in the event viewer.



*Not all logs. Remember how the Firewall logs are in a different space

Event Logs

1	Powershell Remoting	4624,4672,4103, 4104, 53504, 400, 403, 800, 91, 198
	4624 Logon Type 3 Source IP/Logon User Name 4672 Logon User Name Logon by an a user with administrative rights Microsoft-WindowsPowerShell%4Operational.evtx 4103, 4104 – Script Block logging Logs suspicious scripts by default in PS v5 Logs all scripts if configured 53504 Records the authenticating user Windows PowerShell.evtx 400/403 "ServerRemoteHost" indicates start/end of Remoting session 800 Includes partial script code Microsoft-WindowsWinRM%4Operational.evtx 91 Session creation	

	168 Records the authenticating user	
2	WMI WMIC	4624,4672, 5857,5860, 5861
	security.evtx 4624 Logon Type 3 Source IP/Logon User Name 4672 Logon User Name Logon by an a user with administrative rights Microsoft-Windows-WMIActivity%4Operational.evtx 5857 Indicates time of wmioprse execution and path to provider DLL – attackers sometimes install malicious WMI provider DLLs 5860, 5861 Registration of Temporary (5860) and Permanent (5861) Event Consumers. Typically used for persistence, but can be used for remote execution.	
3	Services	4624,4697,7034,7035,7036,7040,7045
	security.evtx 4624 Logon Type 3 Source IP/Logon User Name 4697 Security records service install, if enabled Enabling non-default Security events such as ID 4697 are particularly useful if only the Security logs are forwarded to a centralized log server system.evtx 7034 – Service crashed unexpectedly 7035 – Service sent a Start/Stop control 7036 – Service started or stopped 7040 – Start type changed (Boot On Request Disabled) 7045 – A service was installed on the system	
4	Scheduled Tasks	4624,4672,4698,4702,4699,4700,4701,106,140,141,200,201
	security.evtx 4624 Logon Type 3 Source IP/Logon User Name 4672 Logon User Name Logon by a user with administrative rights Requirement for accessing default shares such as C\$ and ADMIN\$ 4698 – Scheduled task created 4702 – Scheduled task updated 4699 – Scheduled task deleted 4700/4701 – Scheduled task enabled/disabled Microsoft-Windows-Task Scheduler%4Maintenance.evtx 106 – Scheduled task created 140 – Scheduled task updated 141 – Scheduled task deleted 200/201 – Scheduled task executed/completed	
5	Psexec	4624,4672,5140,7045
	security.evtx 4624 Logon Type 3 (and Type 2 if “-u” Alternate Credentials are used) Source IP/Logon User Name 4672 Logon User Name Logon by a user with administrative rights Requirement for access default shares such as C\$ and ADMIN\$ 5140 – Share Access ADMIN\$ share used by PsExec system.evtx	

	7045 Service Install	
6	Map Network Shares	4624, 4672, 4776, 4768, 4769, 5140, 5145
	Security Event Log – security.evtx 4624 Logon Type 3 Source IP/Logon User Name 4672 Logon User Name Logon by user with administrative rights Requirement for accessing default shares such as C\$ and ADMIN\$ 4776 – NTLM if authenticating to Local System Source Host 4768 – TGT Granted Source Host Name/Logon User Name Available only on domain controller 4769 – Service Ticket Granted if authenticating to Domain Controller Destination Host Name/Logon User Name Source IP Available only on domain controller 5140 Share Access 5145 Auditing of shared files – NOISY!	
7	Remote Desktop	4624,4778,4779,131,98,1149,21,22,25,41
	Security Event Log – security.evtx 4624 Logon Type 10 Source IP/Logon User Name 4778/4779 IP Address of Source/Source System Name Logon User Name Microsoft-WindowsRemoteDesktopServicesRdpCoreTS%4Operational.evtx 131 – Connection Attempts Source IP/Logon User Name 98 – Successful Connections Microsoft-Windows-Terminal Services-RemoteConnection Manager%4Operational.evtx 1149 Source IP/Logon User Name • Blank user name may indicate use of Sticky Keys Microsoft-Windows-Terminal Services-LocalSession Manager%4Operational.evtx 21, 22, 25 Source IP/Logon User Name 41 Logon User Name	

Firewall Through Command Line

If you have gotten this far awesome! One of the most important things to learn / play with (other than maybe understanding administering services) is the Firewall.

The **netsh** suite is the toolset to do this. I encourage you do play with / understand it. Thank you to Ally who compiled these commands below.

Networking and Firewall

Task	Command
Configure your server to use a proxy server	netsh Winhttp set proxy <servername>:<port number> <i>Note: Server Core installations can't access the Internet through a proxy that requires a password to allow connections.</i>
Configure your server to bypass the proxy for internet addresses	netsh winhttp set proxy <servername>:<port number> bypass-list="<local>"
Display or modify IPSEC configuration	netsh ipsec
Display or modify NAP configuration	netsh nap
Display or modify IP to physical address translation	arp
Display or configure the local routing table	route
View or configure DNS server settings	nslookup
Display protocol statistics and current TCP/IP network connections	netstat
Display TCP/UDP connections	netstat /t Netstat /i
Display protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP (NBT)	nbtstat
Display hops for network connections	pathping
Trace hops for network connections	tracert
Display to configuration of the multicast router	mrinfo
Enable/Disable remote administration of the firewall	netsh advfirewall firewall set rule group="Windows Firewall Remote Management" new enable=yes

Get a new DHCP lease	ipconfig /release
	ipconfig /renew