

Windows Defense

Welcome to the black box

Disclaimer

The information contained in this presentation is for educational purposes ONLY! RC3 nor its members hold any responsibility for any misuse of the information provided in any slides, discussions, activities, or exercises.

...You have been warned.

Then you learn the black box

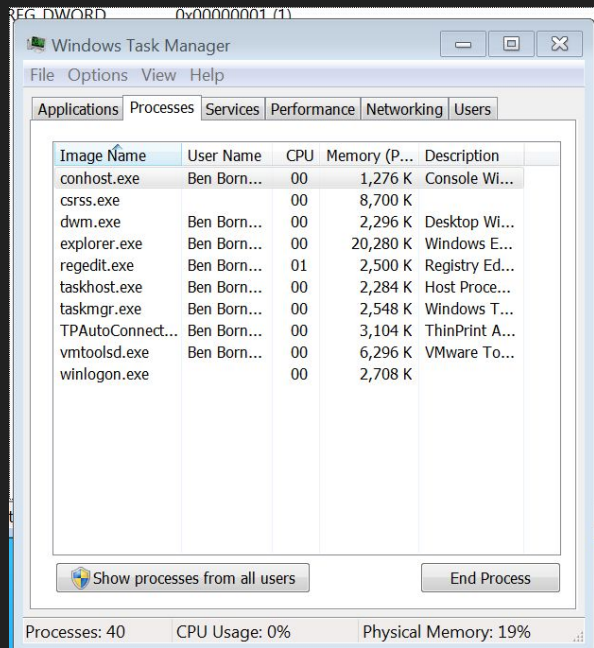


Windows Terms and such

- Windows is **HARD**
 - Closed source black box
 - 70% of all client computers are Windows...so what you gonna make malware for...
- WinNT/ME/2000 -> XP/2003 -> 7/2k8 -> 8/2k12
- Ghetto firewall -> netsh firewall -> advfirewall
 - Ghetto firewall
 - Ingress filtering - Traffic coming into the box.
 - Egress filtering - Traffic leaving the box. (**No egress** filtering so malware is happy :))
- SMB - file share and remote admin port 445
 - Important
- Pro tip: Learn some CMD :) (and some PowerShell)

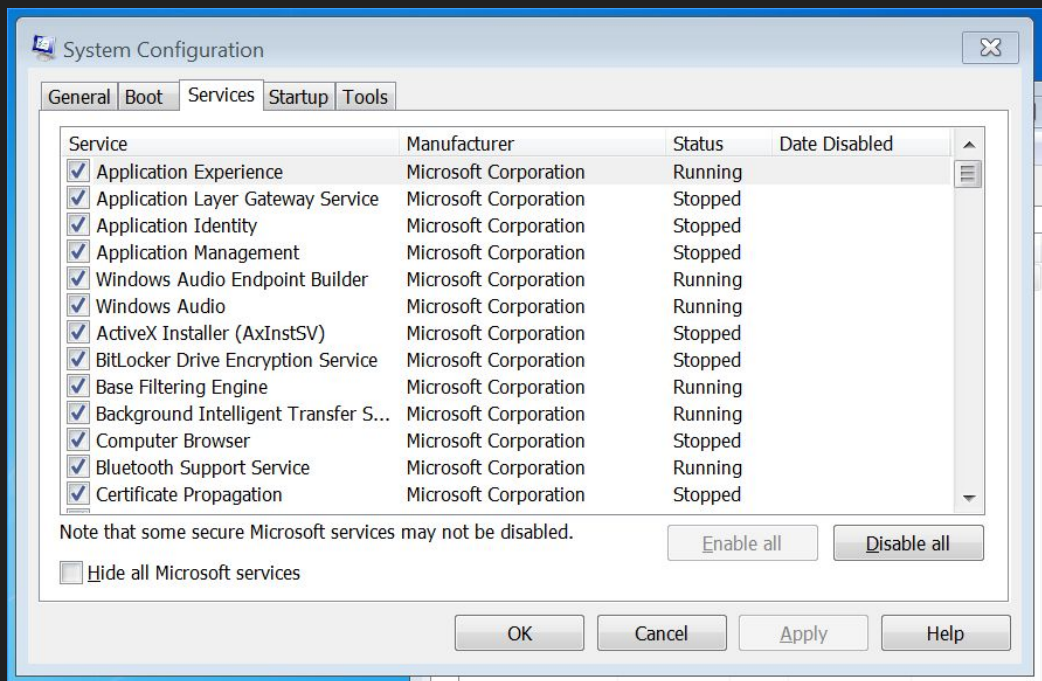
Windows Processes

- Instance of a program running.
- Processes run under a user, so a user has to be **logged in**.



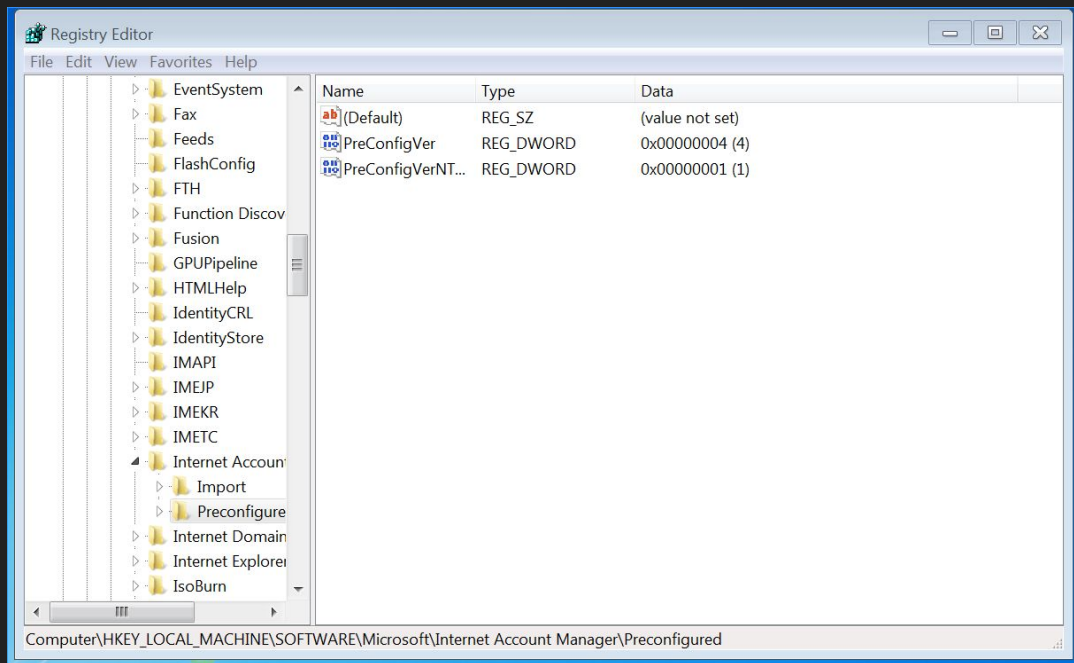
Windows Services

- Like a linux daemon.
- Windows background processes that run whether a **user is logged on or not**.



Windows Registry

- The Windows Registry is a hierarchical database structure that contains all the settings and preferences for the operating system.



Window Registry Locations

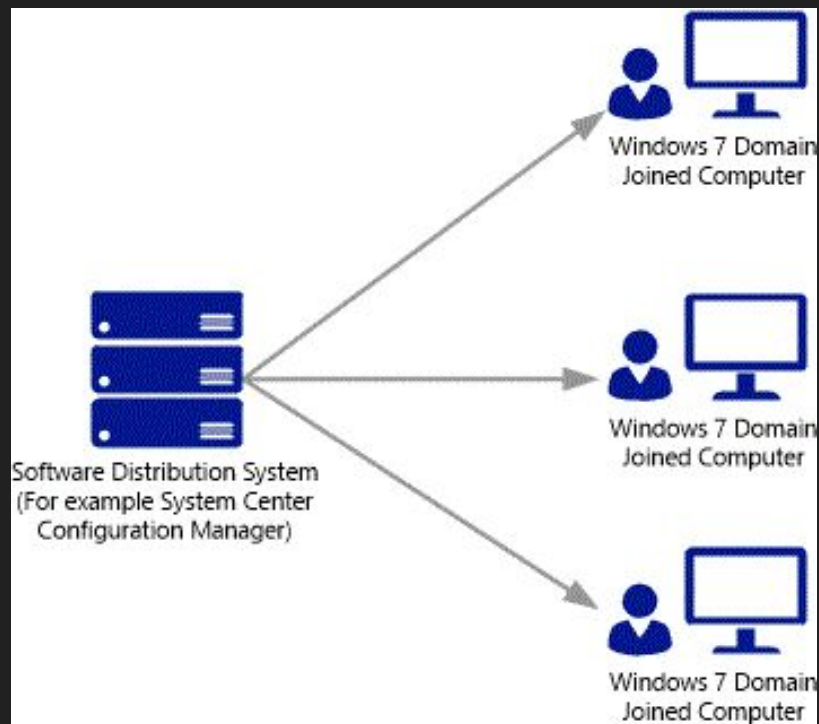
- Startup
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
 - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
 - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
 - There are MANY MORE locations these are just the common locations.
 - Each user has a startup location
- Windows Firewall
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules
 - Location of rules for the Windows firewall.

Windows Domain Controller

Windows Active Directory and DNS

- Active Directory - A database service that provides storage of username and passwords for all users in a network. This database allows for one central location for authentication for all devices in the network within a specific domain.
 - User storage, User printers, User authentication, Remote Administration (Group Policy)
- Domain - [Windows domains](#) provide network administrators with a way to manage a large number of PCs and control them from one place.
- Active Directory is DNS based
 - Therefore each network is given a domain name (malwarelove.xyz/rit.edu) and you join the domain.
 - Login: [abc123@rit.edu](#), xyz789@student.rit.edu
- Group Policy - A single set of rules to apply to multiple users/computers.

Domain



DOS Shell

- So imagine a terminal...but worse
- Some commands are the same (ie cd)
- Some commands are different (ie ls == dir)

Terminal Commands

- ls
- clear
- rm
- cd
- mv
- ifconfig
- ifdown eth0

DOS shell commands

- dir
- cls
- del
- cd
- move
- ipconfig
- netsh interface set interface
name="Local Area Connection"
admin=disabled



Powershell

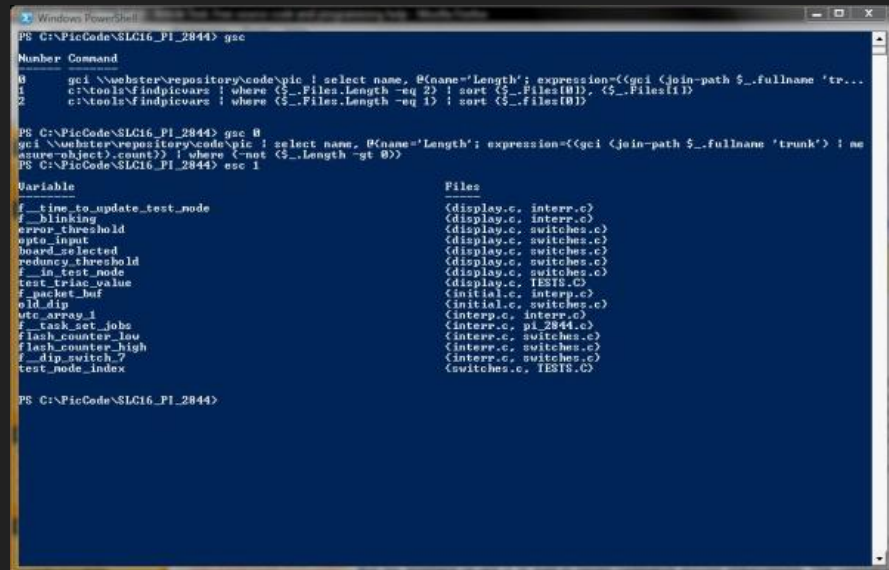
- Powershell v1.0 first available in 2006
- Currently on v4.0 as of April 2014
- It's like a dos shell, but on steroids
- It's also like....a real language
- Oh...and you can use nix cmds now!
- Runs on .NET
- Users “cmdlets”

- Crazy good documentation on technet

Example:

Select-String -Path c:\foo*.txt -pattern rc3

- search for the string “rc3” in any text file in C:\foo.txt



```
PS C:\PicCode\SLC16_PI_2844> gsc
Number Command
0 gci \\webster\repository\code\pic ! select name, @(<name>'Length'; expression=<{(gci <join-path $_.fullname 'tr...
1 c:\tools\findpicvars ! where ($_.Files.Length -eq 2) ! sort ($_.Files[0]), ($_.Files[1])
2 c:\tools\findpicvars ! where ($_.Files.Length -eq 1) ! sort ($_.Files[0])

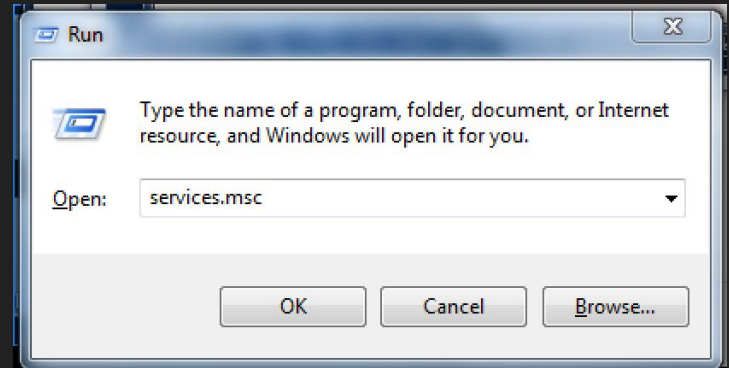
PS C:\PicCode\SLC16_PI_2844> gsc 0
gci \\webster\repository\code\pic ! select name, @(<name>'Length'; expression=<{(gci <join-path $_.fullname 'trunk') : ne
azure-object>.count)} ! where (<not ($_.Length -gt 0)})
PS C:\PicCode\SLC16_PI_2844> esc 1

Variable Files
-----
f_time_to_update_test_node <(display.c, interr.c)
f_blinking <(display.c, interr.c)
error_threshold <(display.c, switches.c)
gpio_input <(display.c, switches.c)
board_selected <(display.c, switches.c)
reduncy_threshold <(display.c, switches.c)
f_in_test_node <(display.c, switches.c)
test_triac_value <(display.c, TESTS.C)
f_packet_buf <(initial.c, interr.c)
old_dip <(initial.c, switches.c)
utc_array_1 <(interr.c, interr.c)
f_task_set_jobs <(interr.c, pi_2844.c)
flash_counter_low <(interr.c, switches.c)
flash_counter_high <(interr.c, switches.c)
f_dip_switch_7 <(interr.c, switches.c)
test_node_index <(switches.c, TESTS.C)

PS C:\PicCode\SLC16_PI_2844>
```

Run quick commands

- Run prompt: Windows key + R
- Services menu - services.msc
- System settings - sysctl.msc
- Registry - regedit
- Computer Management - compmgmt.msc
- Event Viewer - eventvwr.msc
- Remote Desktop - tsmmc.msc
- Windows Firewall - wf.msc



SO how does one break Windows???

- File and Printer Sharing
- Remote Desktop
- DNS Transfer
- LSASS
- Pass-the-hash
- Windows Shares
- Scheduled tasks
- Windows Logon

Defense Methodology Cont.

- Change password
- If you don't have a service scoring disconnect from internet
 - If you do, turn it off and turn it back on
- Uncheck file sharing/rdp
- Disable/delete unused accounts
- Change password/flicker NIC
- Audit processes/connections/network/services
- Firewall
- Don't use Internet Explorer

Change your password

- `net user <username> *`
- Ex: `net user administrator *`
- **JUST DO IT**. Default creds are the best way for red team to get in

Flick the NIC

1. Windows Key - R
2. ncpa.cpl
3. Right click on adapter
4. DISABLE THAT BAD BOY, THEN RE-ENABLE
5. (Re-enable if just flickering)
 - Flickering kills any established connections to your machine

Disable File/Print Sharing

1. Windows Key - R
2. ncpa.cpl
3. Double click or right click
4. Properties
5. Uncheck file and print sharing
 - Disables psexec (remote command execution) and common vulns (MS08_067, MS10_061)
 - Look at network shares when “File and Print Sharing” needs to be enabled.
 - **NOTE: Disabling File and Print Sharing on a domain controller WILL BREAK THINGS.**

Remote Desktop and Assistance

1. Windows Key - R
2. sysdm.cpl
3. Remote tab
4. Disallow remote connections & remote assistance
 - Also Select Users... and remove everyone
 - Sometimes RDP selection will be greyed out

Disable/Delete Unused Accounts

- `net user guest /active:no`
- `net user redteamhax /delete`
- Remove from admin group
 - `net (local)group Administrators (list)`
 - `net (local)group Administrators guest /delete`

Audit Processes

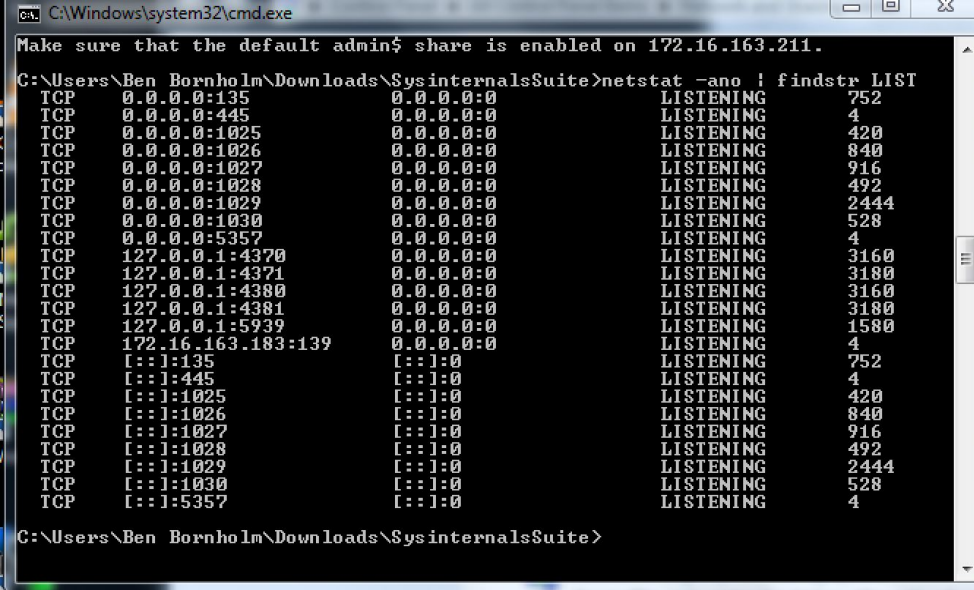
- Windows Key - R -> taskmgr
- USE PROCESS EXPLORER(more on this later)
- Kill notepad (unless you are using it :p)
- Kill exes called a bunch of random numbers and letters
 - sdDFjdfx.exe
- Office.Updater.A.exe (example)
- notmalware.pdf.exe is probably malware

CMD kill those processes

- Pskill works well (more on this later)
- cmd: taskkill
 - `taskkill /f /im malware.exe`
 - `taskkill /f /pid <processID>`
- Powershell: Stop-Process
 - `Stop-Process -Force -Name malware.exe`
 - `Stop-Process -Force <pid>`

Audit connections

- `netstat -ano | findstr LIST`
 - Show listening service
- `netstat -ano | findstr STAB`
 - Show established connections
- Flags will differ from Linux!!!



The screenshot shows a Windows command prompt window titled "C:\Windows\system32\cmd.exe". The prompt is at "C:\Users\Ben Bornholm\Downloads\SysinternalsSuite>". The command entered is `netstat -ano | findstr LIST`. The output lists several listening TCP services on the local machine (127.0.0.1 and 172.16.163.183).

```
Make sure that the default admin$ share is enabled on 172.16.163.211.

C:\Users\Ben Bornholm\Downloads\SysinternalsSuite>netstat -ano | findstr LIST
TCP        0.0.0.0:135           0.0.0.0:*             LISTENING   752
TCP        0.0.0.0:445           0.0.0.0:*             LISTENING    4
TCP        0.0.0.0:1025          0.0.0.0:*             LISTENING   420
TCP        0.0.0.0:1026          0.0.0.0:*             LISTENING   840
TCP        0.0.0.0:1027          0.0.0.0:*             LISTENING   916
TCP        0.0.0.0:1028          0.0.0.0:*             LISTENING   492
TCP        0.0.0.0:1029          0.0.0.0:*             LISTENING  2444
TCP        0.0.0.0:1030          0.0.0.0:*             LISTENING   528
TCP        0.0.0.0:5357          0.0.0.0:*             LISTENING    4
TCP        127.0.0.1:4370        0.0.0.0:*             LISTENING  3160
TCP        127.0.0.1:4371        0.0.0.0:*             LISTENING  3180
TCP        127.0.0.1:4380        0.0.0.0:*             LISTENING  3160
TCP        127.0.0.1:4381        0.0.0.0:*             LISTENING  3180
TCP        127.0.0.1:5939        0.0.0.0:*             LISTENING  1580
TCP        172.16.163.183:139    0.0.0.0:*             LISTENING    4
TCP        [::]:135             [::]:*                LISTENING   752
TCP        [::]:445             [::]:*                LISTENING    4
TCP        [::]:1025            [::]:*                LISTENING   420
TCP        [::]:1026            [::]:*                LISTENING   840
TCP        [::]:1027            [::]:*                LISTENING   916
TCP        [::]:1028            [::]:*                LISTENING   492
TCP        [::]:1029            [::]:*                LISTENING  2444
TCP        [::]:1030            [::]:*                LISTENING   528
TCP        [::]:5357            [::]:*                LISTENING    4

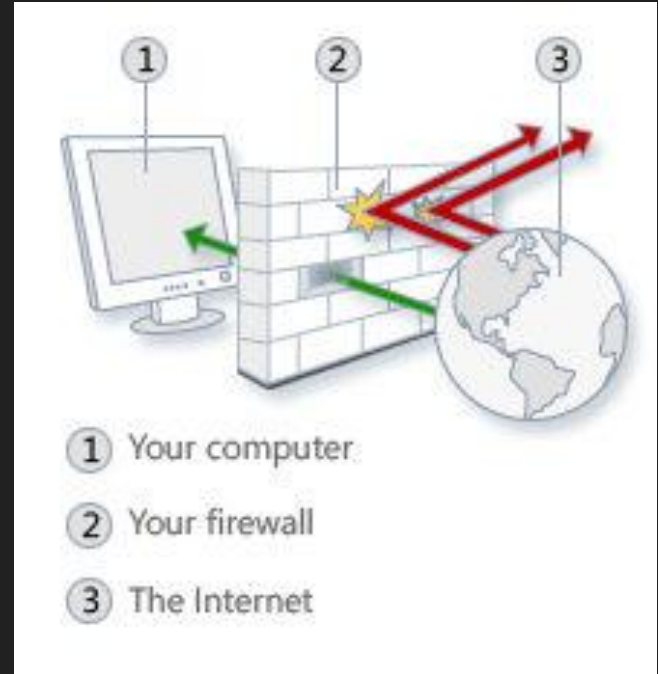
C:\Users\Ben Bornholm\Downloads\SysinternalsSuite>
```


Audit Services

- Windows Key - R -> services.msc
- Shut off unused services!
 - Telnet
 - IIS (web)
 - Terminal Services
 - DNS/DHCP if you aren't a scored server
 - Suspicious things
 - Look at service descriptions and executable paths!

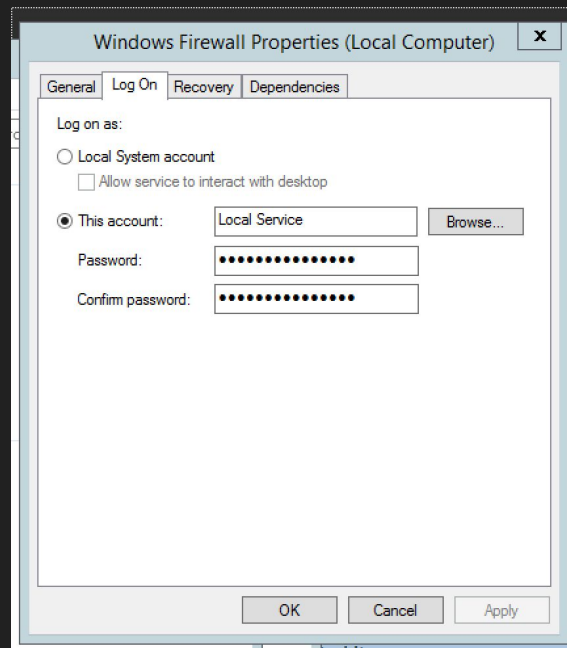
Firewalls

- Depending on your OS, there are two types of firewalls
 - Netsh Firewall (old)
 - Netsh AdvFirewall (new)
- What is a firewall?
 - A piece of software that filters inbound (or outbound) traffic
- GUI is available but should learn CLI



Pro tip

- The firewall account should be set to Local Service or NT_AUTHORITY\LocalService for servers.
- Firewall **won't** start unless it starts as the right user.
- This happened to me at ISTS and I was sad.



Windows Advfirewall Profiles

- Domain - Applied to a network adapter when it is connected to a network on which it **can detect a domain** controller of the domain to which the computer is joined.
- Public - Applied to a network adapter when it is connected to a network that is identified by the user or administrator as a **private network**. A private network is one that is not connected directly to the Internet, but is behind some kind of **security device, such as a network address translation (NAT) router or hardware firewall**.
 - Example: Home networks or office network
- Private - Applied to a network adapter when it is connected to a **public network** such as those available in airports and coffee shops. When the profile is **not set to Domain or Private**, the default profile is Public. The Public profile settings should be the most restrictive because the computer is connected to a public network where the security cannot be controlled.
 - Example: Airport networks, coffee shops, untrusted networks

Windows Advfirewall examples

1. `netsh advfirewall firewall show rule name=all`
 - a. Show all current firewall rules
2. `netsh advfirewall set allprofiles state on`
3. `netsh advfirewall firewall delete rule name=all`
 - a. Wipe all rules in case there was any shenanigans.
4. `netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound`
 - a. Set the profiles to block everything by default that isn't stated otherwise.
5. `netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes`
 - a. Allow File and Printer sharing services - don't have to define services.
6. `netsh advfirewall firewall add rule name="Allow HTTPS IN" dir=in action=allow protocol=TCP localport=443`
 - a. Allow HTTPS/443 in
7. `netsh advfirewall firewall add rule name="Allow HTTPS out" dir=out action=allow protocol=TCP localport=443`
 - a. Allow HTTPS/443 out

Task Scheduler

- Creating a task
 - `schtasks /Create /SC <schedule> /TN <task name> /TR <taskrun> /ST <start time>`
 - This task will run daily at 9 a.m. every day
 - `schtasks /Create /SC DAILY /TN "My Task" /TR "C:RunMe.bat" /ST 09:00`
- Changing a task
 - `schtasks /Change /TN "My Task" /ST 14:00`
 - Changed "My Task" to start at 2 p.m.
- Deleting a task
 - `schtasks /delete /TN "My Task"`
- Create scripts for bulk creation

Scripting with Windows

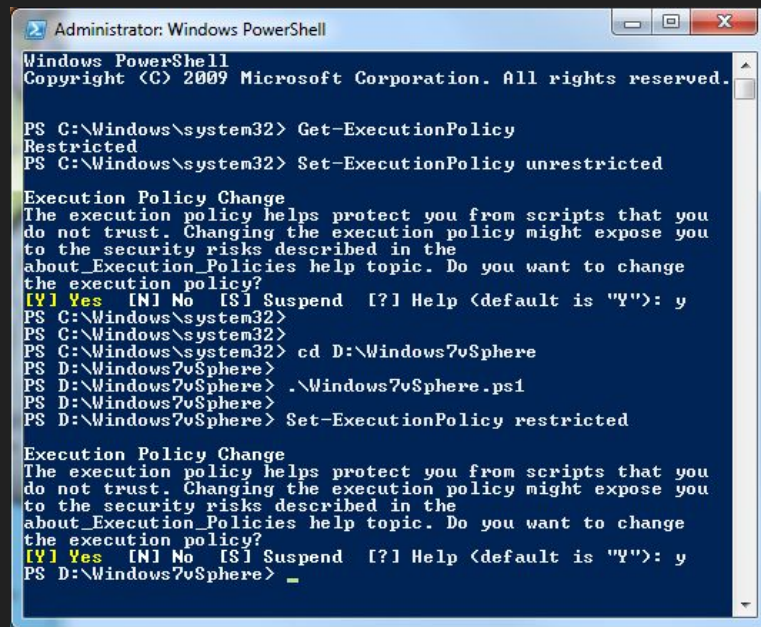
- We have two (native) options:
 - Batch (.bat)
 - Powershell (.ps)
- We have to Set-ExecutionPolicy

Restricted - No scripts can be run. Windows PowerShell can be used only in interactive mode.

AllSigned - Only scripts signed by a trusted publisher can be run.

RemoteSigned - Downloaded scripts must be signed by a trusted publisher before they can be run.

Unrestricted - No restrictions; all Windows PowerShell scripts can be run.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Get-ExecutionPolicy
Restricted
PS C:\Windows\system32> Set-ExecutionPolicy unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you
do not trust. Changing the execution policy might expose you
to the security risks described in the
about_Execution_Policies help topic. Do you want to change
the execution policy?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32> cd D:\Windows7vSphere
PS D:\Windows7vSphere>
PS D:\Windows7vSphere> .\Windows7vSphere.ps1
PS D:\Windows7vSphere>
PS D:\Windows7vSphere> Set-ExecutionPolicy restricted

Execution Policy Change
The execution policy helps protect you from scripts that you
do not trust. Changing the execution policy might expose you
to the security risks described in the
about_Execution_Policies help topic. Do you want to change
the execution policy?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y
PS D:\Windows7vSphere> _
```

Crash course on Sysinternals in 5mins

Sysinternals

- DON'T THINK ABOUT just DO IT!
 - Free
- Suite of Windows portable tools
- Lots of tools within one toolkit for windows sysadmin and incident response
- Samba share: [\\live.sysinternals.com\tools](https://live.sysinternals.com/tools)
- Autoruns
 - Shows you all of the things that start up when your computer starts or users login.
- Process Explorer
 - Task manager... on steroids.
- TCPView
 - Better netstat in GUI form

Process Explorer

- Upload processes to VirusTotal to verify them
 - Only works on Windows processes and some well known processes.
 - Allow you to narrow the scope of WHAT IS **NOT** malware.

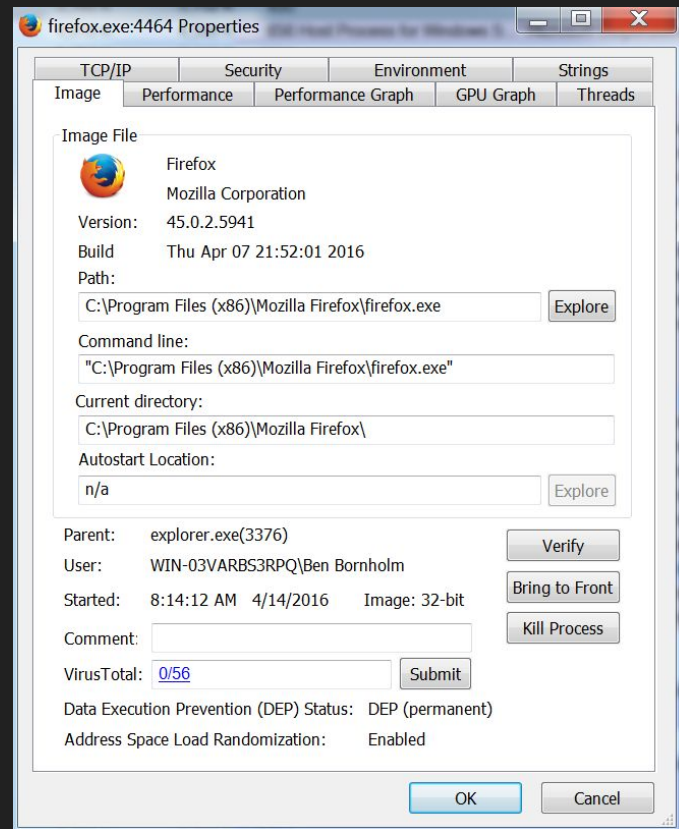
- **Pink** - Windows Service hosting processes
- **Blue** - Current user launched processes
- **Cyan** - Windows app store application
- **Purple** - Indicates a "packed" piece of software
- **Green** - Newly launched processes
- **Red** - Terminated process
- **Dark Gray** - Suspended process

Name	Private Bytes	Working Set	PID	Description	Company Name	Command Line	VirusTotal
System Idle Process	0 K	0 K	0				
System	12 K	64 K	4				
smss.exe	476 K	268 K	284				
svchost.exe	2,084 K	1,820 K	322				
lsass.exe	1,452 K	224 K	424				
services.exe	8,800 K	5,760 K	460				
smss.exe	4,988 K	4,056 K	688	Host Process for Windows S...	Microsoft Corporation	C:\Windows\system32\svchost.exe -k DismLaunch	Hash submitted
smss.exe	8,800 K	6,624 K	1084				
smss.exe	2,544 K	6,240 K	3720				
smss.exe	1,440 K	476 K	716	VMware Activation Helper	VMware, Inc.	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"	Hash submitted
smss.exe	5,880 K	8,110 K	760	Host Process for Windows S...	Microsoft Corporation	C:\Windows\system32\svchost.exe -k RPCSS	Hash submitted
smss.exe	26,492 K	14,572 K	820	Host Process for Windows S...	Microsoft Corporation	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted	Hash submitted
smss.exe	15,888 K	15,512 K	3428				
smss.exe	5,460 K	7,244 K	100	Host Process for Windows S...	Microsoft Corporation	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted	Hash submitted
smss.exe	5,23	314,236 K	238	Desktop Window Manager	Microsoft Corporation	"C:\Windows\system32\csrss.exe"	Hash submitted
smss.exe	1,07	31,620 K	30,520	644 Host Process for Windows S...	Microsoft Corporation	C:\Windows\system32\svchost.exe -k netbios	Hash submitted
smss.exe	+0.01	11,890 K	17,110 K	460 Host Process for Windows S...	Microsoft Corporation	C:\Windows\system32\svchost.exe -k LocalService	Hash submitted
smss.exe	0.03	31,388 K	18,552 K	1002 Host Process for Windows S...	Microsoft Corporation	C:\Windows\system32\svchost.exe -k NetworkService	Hash submitted
smss.exe	8,900 K	5,234 K	1392	Speaker Recognition App	Microsoft Corporation	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted	Hash submitted
smss.exe	13,800 K	9,524 K	1240	Host Process for Windows S...	Microsoft Corporation	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted	Hash submitted
smss.exe	0.19	10,560 K	6,620 K	1376 VMware Tools Core Service	VMware, Inc.	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"	Hash submitted
smss.exe	0.02	3,750 K	5,270 K	1008 ThreatNet AutoConnect printer	Corbis AG	"C:\Program Files\VMware\VMware Tools\AutoConnect.exe"	Hash submitted
smss.exe	0.01	3,816 K	8,456 K	6080 ThreatNet AutoConnect comp	ThreatNet GmbH	TFAutoConnect.exe -q -v mware -s COM1 F 30	Hash submitted
smss.exe	1.640 K	720 K	2044	Host Process for Windows S...	Microsoft Corporation	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted	Hash submitted
smss.exe	+0.01	33,958 K	10,024 K	2484 Microsoft Windows Search I...	Microsoft Corporation	C:\Windows\system32\SearchIndexer.exe	Hash submitted
smss.exe	3,076 K	4,584 K	2580	Host Process for Windows S...	Microsoft Corporation	C:\Windows\system32\svchost.exe -k LocalServiceAndAuthImpersonation	Hash submitted
smss.exe	7,822 K	2,984 K	2284	Microsoft Software Protection	Microsoft Corporation	C:\Windows\system32\svchost.exe -k LocalServiceAndAuthImpersonation	Hash submitted
smss.exe	68,120 K	33,408 K	2056	Host Process for Windows S...	Microsoft Corporation	C:\Windows\system32\svchost.exe -k LocalServiceAndAuthImpersonation	Hash submitted
smss.exe	8,144 K	6,524 K	3316	System activity monitor	Systemlabs - www.systemlabs.com	C:\Windows\System32\svchost.exe -k LocalServiceAndAuthImpersonation	Hash submitted
smss.exe	8,020 K	5,184 K	2012	Host Process for Windows S...	Microsoft Corporation	C:\Windows\system32\svchost.exe -k LocalServiceAndAuthImpersonation	Hash submitted
smss.exe	3,492 K	2,256 K	1920	Microsoft Distributed Transac...	Microsoft Corporation	C:\Windows\System32\svchost.exe	Hash submitted
smss.exe	4,648 K	5,900 K	540	Local Security Authority Proc...	Microsoft Corporation	C:\Windows\system32\svchost.exe	Hash submitted
smss.exe	0.02	2,816 K	1,884 K	548			
smss.exe	0.44	10,276 K	4,160 K	4084			
smss.exe	1,760 K	1,100 K	4084	Corbis Window Host	Microsoft Corporation	C:\Windows\system32\svchost.exe	Hash submitted
smss.exe	1,702 K	434 K	1888				
smss.exe	2,820 K	2,600 K	2324				
smss.exe	68,856 K	18,904 K	3376	Windows Explorer	Microsoft Corporation	C:\Windows\Explorer.exe	Hash submitted
smss.exe	0.10	14,448 K	11,500 K	3250 VMware Tools Core Service	VMware, Inc.	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n mware	Hash submitted
smss.exe	272	216,460 K	20,804 K	4660 Firefox	Mozilla Corporation	"C:\Program Files\Firefox\Firefox.exe"	Hash submitted
smss.exe	2,490 K	2,120 K	2786				
smss.exe	2,772 K	6,744 K	5820	Systemlabs Process Explorer	Systemlabs - www.systemlabs.com	"C:\Users\Ben Bonhardt\Desktop\SystemlabsProcessExp.exe"	Hash submitted
smss.exe	0.04	12,836 K	32,672 K	4660 Systemlabs Process Explorer	Systemlabs - www.systemlabs.com	"C:\Users\Ben Bonhardt\Desktop\SystemlabsProcessExp.exe"	Hash submitted

CPU Usage: 54.10% Commit Charge: 41.82% Processes: 43 Physical Usage: 67.30%

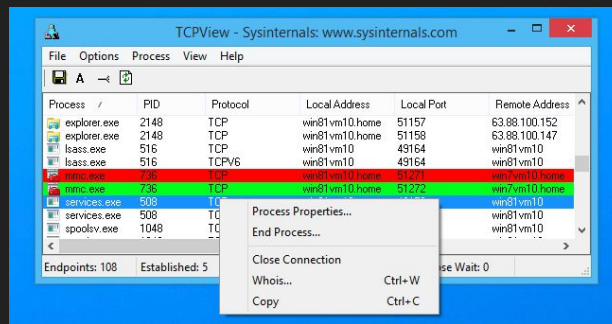
Process details

- Shows path of process
- Start time
- End time
- User who started it
- VirusTotal Signature
- Parent process ID(PPID)
- TCP/IP for network connections



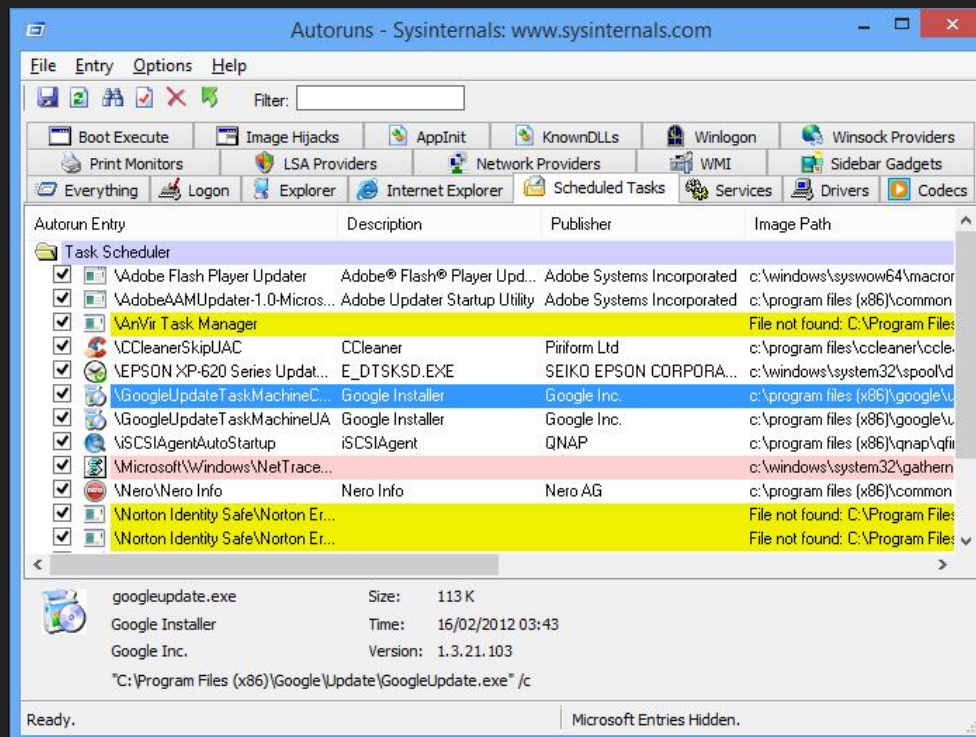
TCPviewer

- A prettier netstat for those who don't like the command line
- If you right-click a process you can run a WHOIS search on the IP.
- Color Scheme
 - Bright Green - Connection is being initiated
 - Bright Red - Connection is being terminated



Autoruns

- Shows all locations where processes/services are started.
- Verify drivers installed and running on boot.
- Programs run on user login
- Shows programs starting at boot
- Loaded DLLs by autostart applications.
- Services started by default



Demo Goal/Rules

1. NO DISABLING NIC
2. Must allow Active Directory and DNS traffic.
3. Must keep Active Directory and DNS services up.
4. Since your a domain controller “File and Printer Sharing” must be enabled.

Resources/Sources

- [Sysinternals](#) - Download
- [Malware Hunting with Mark Russinovich and the Sysinternals Tools](#) -Youtube
 - Mark Russinovich the CREATOR of sysinternals
 - Absolutely favorite resource for sysinternals!!!!!!!!!!!!!!

Questions

