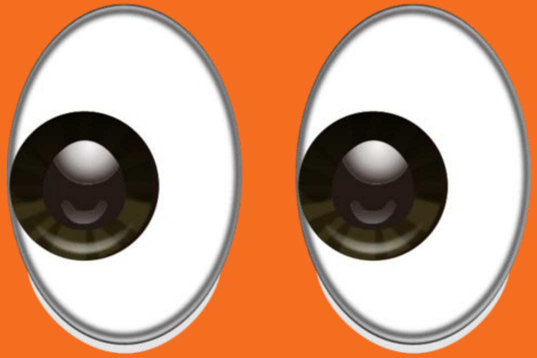
Welcome to RC3

RIT Competitive Cybersecurity Club

"Security Through Community"

Today's meeting brought to you in part by…



Platinum

GRIMM

IOMAXIS

Gold

hackerone

SIG® SUSQUEHANNA

Educational Supporter

Malshare

Trello

http://signin.rc3.club

RC3 Sign-in

Important dates & times

- The Incident Response Security Competition is **April 21st**
  - **White Team Signups:** https://tinyurl.com/irsec2018-whiteteam
  - Come volunteer and help us <3
- BSides Roc is **April 13-14th**
  - Buy tickets here: https://www.eventbrite.com/e/bsides-rochester-2018-tickets-43047674754
  - It’s a great first conference.
    - 13th is Training day, 14th is the conference
  - If you cannot afford tickets to go, come talk to an RC3 E-board member
    - No one should be excluded from going to security events

HackerOne x RC3 Bug Bounty Competition

- Get money
- Get RC3 points
- Get exclusive HackerOne swag
- When you submit a bug bounty report to HackerOne, once the report has been resolved, you can submit it to @joel for even more points for even more prizes! Woo!

Oh, the places you’ll go

- Mailing List: Go to the website, scroll down!
  - Weekly announcements, hints for the Hard challenge, past week’s challenge guide
- Facebook: RITC3
  - Announcements, random postings,
- Twitter: @RC3_Official
  - Just a lot of memes and retweets
- Youtube: RC3club RIT
  - SMASH THAT SUBSCRIBE BUTTON
- Instagram: @rc3.club
  - Please, we have 0 followers
- Slack: https://ritc3.slack.com
  - It’s where work doesn’t happen
- ANSR: listen.rc3.club

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.

Without further ado…

9. Intro to Windows Blue Teaming

Professor Russell pt 2

echo %username%

- 3rd year Comp Sec
- Windows Clients on CCDC
- Co-Captain of CPTC
- I know how to configure an A record
- Outside of Security:
  - Outdoors
  - Baseball
  - Football
  - Movies

Write-Host $env:UserName
Aka Scuzz3y

- 3rd year CSEC - In BS/MS
- 3rd year on CCDC Team
  - Co-Captain
  - DNS is EZ
- 2nd year on ISTS Black Team
  - Team Lead
- “The Windows Guy”
- “The VMware Guy”

Windows Firewall

- Meet your new best friend
- Can be managed from a GUI or command prompt
- Two Different types:
    - “Basic Firewall” - Windows XP SP2 - Windows 2003
    - “Advanced Firewall” - Windows Vista onwards
- Features:
    - Logging
    - Ability to create rules around programs
    - Fine grained control
- When blue teaming, create your firewall settings in a script!

Basic Firewall

- Still powerful but lacks a few of the fine grained controls
  - cannot specify if port is local or remote
  - cannot specify direction
  - logging settings are limited
- Basic Example:

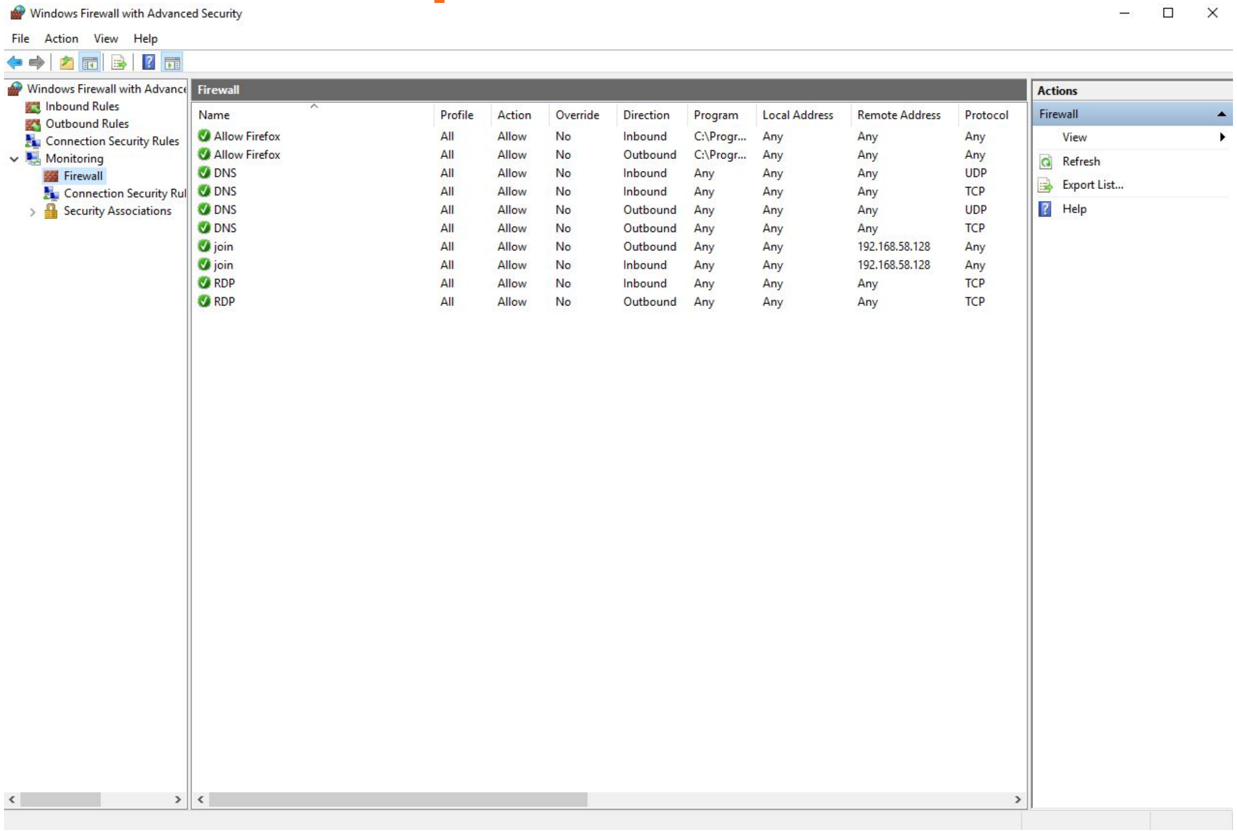
```
netsh firewall set opmode mode=ENABLE exceptions=ENABLE profile=ALL
netsh firewall add portopening protocol=ALL port=389 "LDAP" mode=ENABLE profile=ALL
netsh firewall add portopening protocol=TCP port=686 "LDAP SSL" mode=ENABLE profile=ALL
```

Advanced Firewall

- Allows for more fine grained control of rules
- Basic Example:

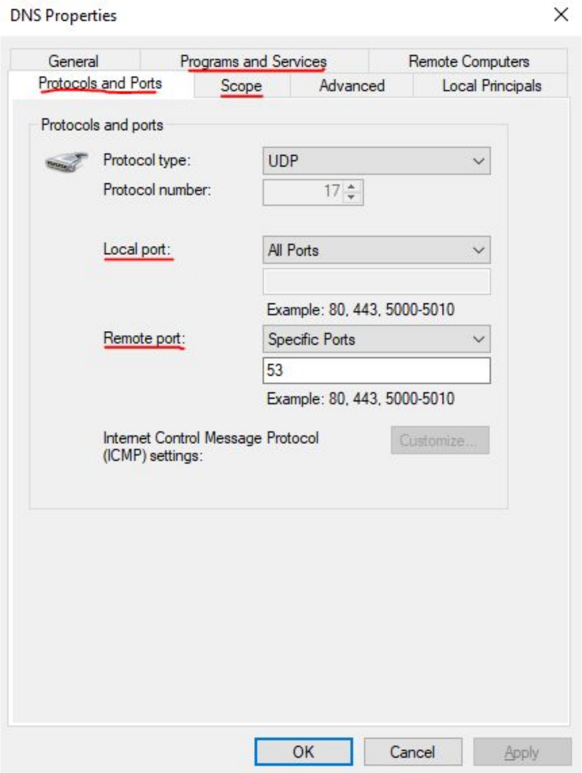
```
netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound

netsh advfirewall firewall add rule name="Allow Firefox" dir=in action=allow program="C:\Program Files\Mozilla Firefox\firefox.exe"
enable=yes profile=any
netsh advfirewall firewall add rule name="Allow Firefox" dir=out action=allow program="C:\Program Files\Mozilla Firefox\firefox.exe"
enable=yes profile=any
netsh advfirewall firewall add rule name=AdClient dir=out protocol=tcp remoteport=53 action=allow
netsh advfirewall firewall add rule name=AdClinet dir=in protocol=tcp remoteport=53 action=allow
```

GUI Example



Firewall

Name	Profile	Action	Override	Direction	Program	Local Address	Remote Address	Protocol
Allow Firefox	All	Allow	No	Inbound	C:\Progr...	Any	Any	Any
Allow Firefox	All	Allow	No	Outbound	C:\Progr...	Any	Any	Any
DNS	All	Allow	No	Inbound	Any	Any	Any	UDP
DNS	All	Allow	No	Inbound	Any	Any	Any	TCP
DNS	All	Allow	No	Outbound	Any	Any	Any	UDP
DNS	All	Allow	No	Outbound	Any	Any	Any	TCP
join	All	Allow	No	Outbound	Any	Any	192.168.58.128	Any
join	All	Allow	No	Inbound	Any	Any	192.168.58.128	Any
RDP	All	Allow	No	Inbound	Any	Any	Any	TCP
RDP	All	Allow	No	Outbound	Any	Any	Any	TCP



Protocols and ports

Protocol type: UDP

Protocol number: 17

Local port: All Ports

Example: 80, 443, 5000-5010

Remote port: Specific Ports

53

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

CMD

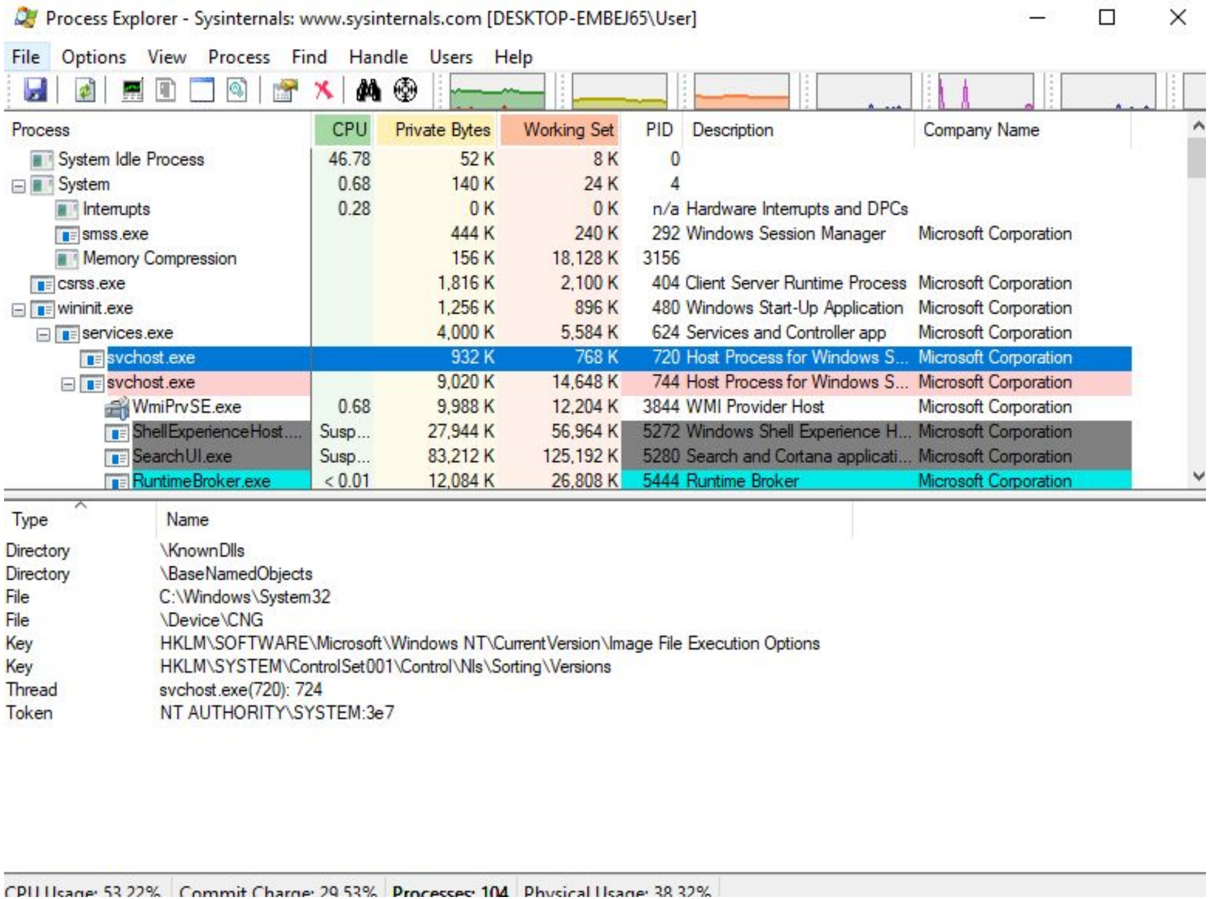
- netstat - similar to unix command: displays connections
- tasklist - display processes on a host
- taskkill - kill a specified task
- net user - audit local users
- net localgroup - audit local computer groups
- net group - audit domain groups
- schtasks - interface with scheduled tasks
- systeminfo - provides high level overview of the system

Sysinternals Suite

- A set of powerful tools to help system administrators
- Also useful for incident response
- Four essential tools:
  - Process Explorer
  - Autoruns
  - Process Monitor
  - TCP View

Process Explorer

- Task manager on steroids
- Gives detailed information on every process running on the system
  - Threads
  - TCP connections
  - Environment
  - Privileges
  - Strings
- You can also grab important information such as handles and loaded DLLs


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-EMBEJ65\User]
File
Options
View
Process
Find
Handle
Users
Help

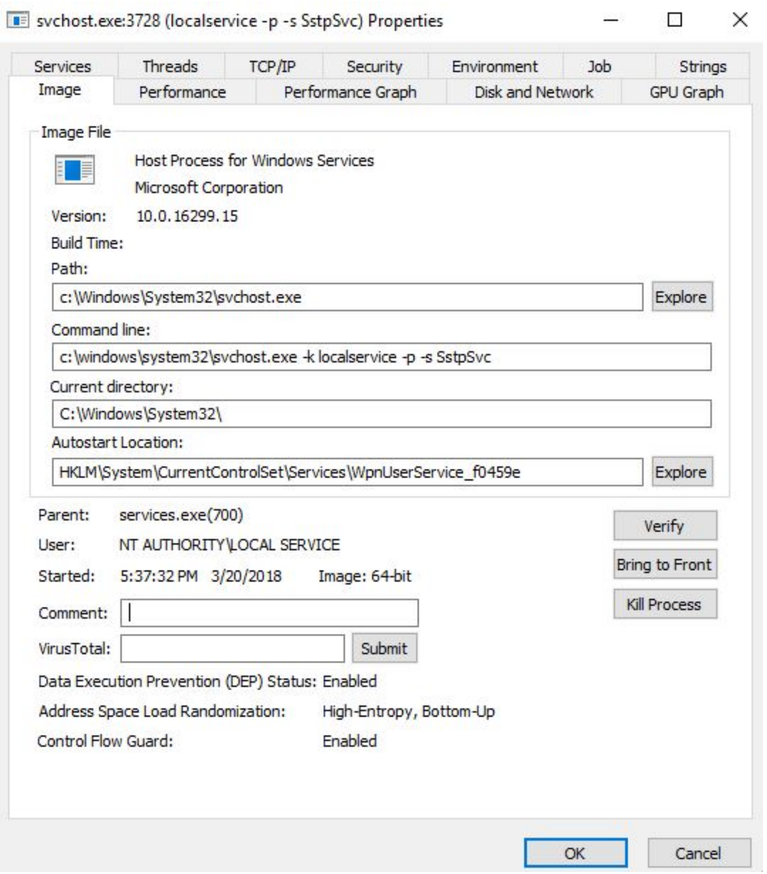
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	46.78	52 K	8 K	0		
System	0.68	140 K	24 K	4		
Interrupts	0.28	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		444 K	240 K	292	Windows Session Manager	Microsoft Corporation
Memory Compression		156 K	18,128 K	3156		
csrss.exe		1,816 K	2,100 K	404	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,256 K	896 K	480	Windows Start-Up Application	Microsoft Corporation
services.exe		4,000 K	5,584 K	624	Services and Controller app	Microsoft Corporation
svchost.exe		932 K	768 K	720	Host Process for Windows S...	Microsoft Corporation
svchost.exe		9,020 K	14,648 K	744	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe	0.68	9,988 K	12,204 K	3844	WMI Provider Host	Microsoft Corporation
ShellExperienceHost....	Susp...	27,944 K	56,964 K	5272	Windows Shell Experience H...	Microsoft Corporation
SearchUI.exe	Susp...	83,212 K	125,192 K	5280	Search and Cortana applicati...	Microsoft Corporation
RuntimeBroker.exe	< 0.01	12,084 K	26,808 K	5444	Runtime Broker	Microsoft Corporation

Type	Name
Directory	\KnownDlls
Directory	\BaseNamedObjects
File	C:\Windows\System32
File	\Device\CNG
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Thread	svchost.exe(720): 724
Token	NT AUTHORITY\SYSTEM:3e7

CPU Usage: 53.22% | Commit Charge: 29.53% | Processes: 104 | Physical Usage: 38.32%

Process Explorer

- First enable sig verification
  - options->verify signature
- Check for sigs that are invalid or processes that have none
- Suspend processes in case of **bad watchdogs**
- Keep an eye on that network graph
  - Beacons will be "constant"



Host Process for Windows Services
Microsoft Corporation

Version: 10.0.16299.15

Build Time:

Path: c:\Windows\System32\svchost.exe

Command line: c:\windows\system32\svchost.exe -k localservice -p -s SstpSvc

Current directory: C:\Windows\System32\

Autostart Location: HKLM\System\CurrentControlSet\Services\WpnUserService_f0459e

Parent: services.exe(700)

User: NT AUTHORITY\LOCAL SERVICE

Started: 5:37:32 PM 3/20/2018 Image: 64-bit

Comment:

VirusTotal:

Data Execution Prevention (DEP) Status: Enabled

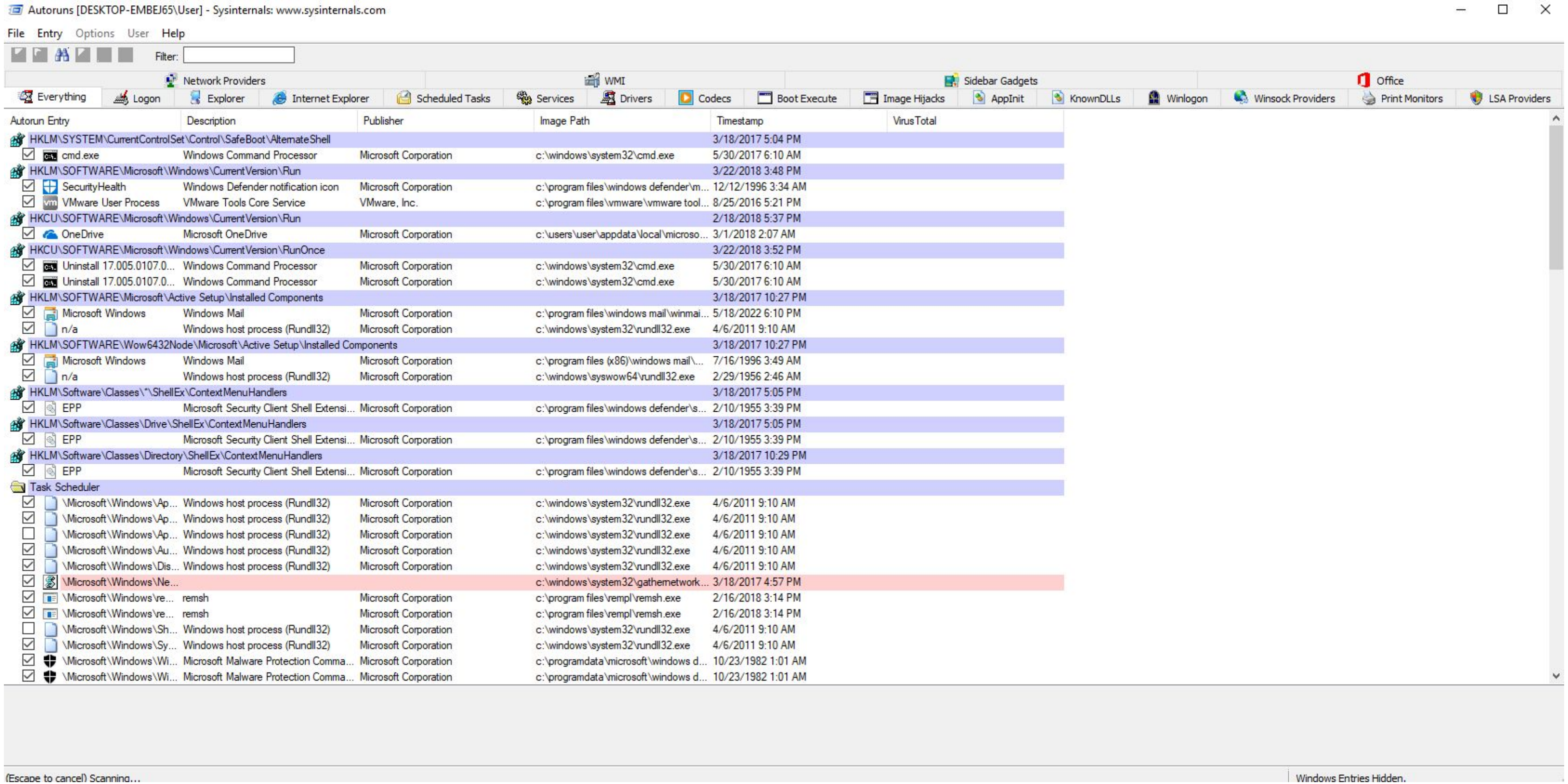
Address Space Load Randomization: High-Entropy, Bottom-Up

Control Flow Guard: Enabled

Autoruns

- Detects most well-known registry attacks
- Monitor:
  - WMI
  - Scheduled Tasks
  - Services
  - etc etc…
- Does miss quite a few important registry keys

Autoruns



	Autorun Entry	Description	Publisher	Image Path	Timestamp	Virus Total
	HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				3/18/2017 5:04 PM	
☑	cmd.exe	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	5/30/2017 6:10 AM	
	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				3/22/2018 3:48 PM	
☑	SecurityHealth	Windows Defender notification icon	Microsoft Corporation	c:\program files\windows defender\m...	12/12/1996 3:34 AM	
☑	VMware User Process	VMware Tools Core Service	VMware, Inc.	c:\program files\vmware\vmware tool...	8/25/2016 5:21 PM	
	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2/18/2018 5:37 PM	
☑	OneDrive	Microsoft OneDrive	Microsoft Corporation	c:\users\user\appdata\local\microso...	3/1/2018 2:07 AM	
	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce				3/22/2018 3:52 PM	
☑	Uninstall 17.005.0107.0...	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	5/30/2017 6:10 AM	
☑	Uninstall 17.005.0107.0...	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	5/30/2017 6:10 AM	
	HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				3/18/2017 10:27 PM	
☑	Microsoft Windows	Windows Mail	Microsoft Corporation	c:\program files\windows mail\winmai...	5/18/2022 6:10 PM	
☑	n/a	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	4/6/2011 9:10 AM	
	HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				3/18/2017 10:27 PM	
☑	Microsoft Windows	Windows Mail	Microsoft Corporation	c:\program files (x86)\windows mail\...	7/16/1996 3:49 AM	
☑	n/a	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\syswow64\rundll32.exe	2/29/1956 2:46 AM	
	HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers				3/18/2017 5:05 PM	
☑	EPP	Microsoft Security Client Shell Extensi...	Microsoft Corporation	c:\program files\windows defender\s...	2/10/1955 3:39 PM	
	HKLM\Software\Classes\Drive\ShellEx\ContextMenuHandlers				3/18/2017 5:05 PM	
☑	EPP	Microsoft Security Client Shell Extensi...	Microsoft Corporation	c:\program files\windows defender\s...	2/10/1955 3:39 PM	
	HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers				3/18/2017 10:29 PM	
☑	EPP	Microsoft Security Client Shell Extensi...	Microsoft Corporation	c:\program files\windows defender\s...	2/10/1955 3:39 PM	
	Task Scheduler					
☑	\Microsoft\Windows\Ap...	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	4/6/2011 9:10 AM	
☑	\Microsoft\Windows\Ap...	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	4/6/2011 9:10 AM	
☐	\Microsoft\Windows\Ap...	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	4/6/2011 9:10 AM	
☑	\Microsoft\Windows\Au...	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	4/6/2011 9:10 AM	
☑	\Microsoft\Windows\Dis...	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	4/6/2011 9:10 AM	
☑	\Microsoft\Windows\Ne...			c:\windows\system32\gathernetwork...	3/18/2017 4:57 PM	
☑	\Microsoft\Windows\re...	remsh	Microsoft Corporation	c:\program files\rempl\remsh.exe	2/16/2018 3:14 PM	
☑	\Microsoft\Windows\re...	remsh	Microsoft Corporation	c:\program files\rempl\remsh.exe	2/16/2018 3:14 PM	
☐	\Microsoft\Windows\Sh...	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	4/6/2011 9:10 AM	
☑	\Microsoft\Windows\Sy...	Windows host process (Rundll32)	Microsoft Corporation	c:\windows\system32\rundll32.exe	4/6/2011 9:10 AM	
☑	\Microsoft\Windows\Wi...	Microsoft Malware Protection Comma...	Microsoft Corporation	c:\programdata\microsoft\windows d...	10/23/1982 1:01 AM	
☑	\Microsoft\Windows\Wi...	Microsoft Malware Protection Comma...	Microsoft Corporation	c:\programdata\microsoft\windows d...	10/23/1982 1:01 AM	

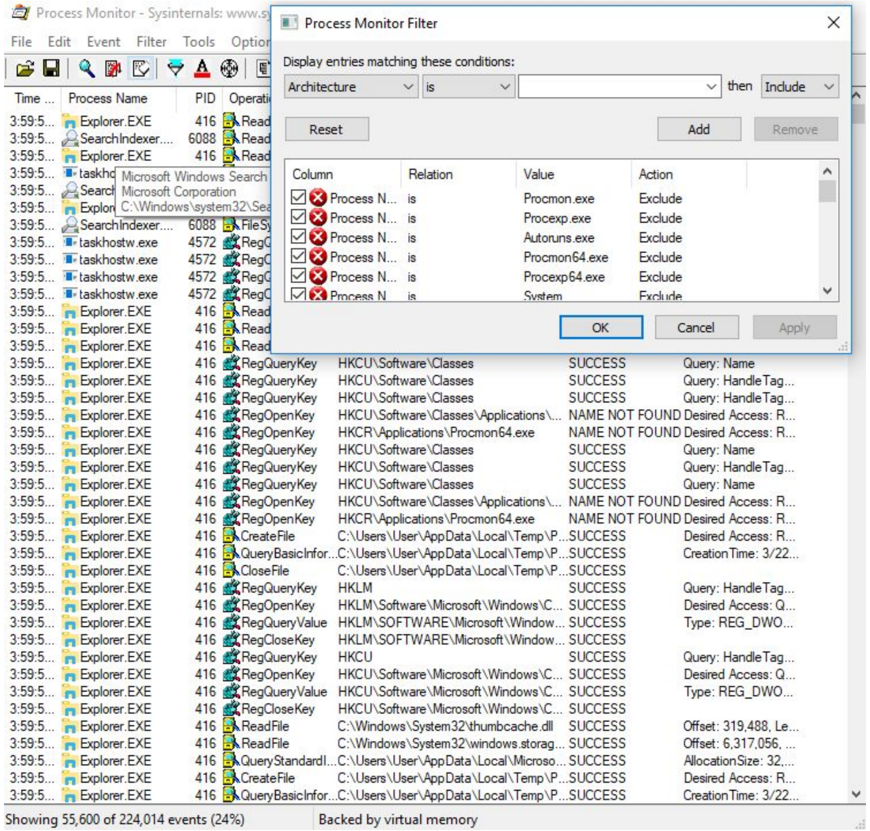
(Escape to cancel) Scanning...

Windows Entries Hidden.

Process Monitor

- Monitors registry, file system, and process activity
- Fine grained filtering control
- Example use case:

Registry key or file is constantly being added. You can use procmon to find what process is performing this action



Display entries matching these conditions:

Architecture | is | | then | Include

Column	Relation	Value	Action
☑ ☒ Process N...	is	Procmon.exe	Exclude
☑ ☒ Process N...	is	Procexp.exe	Exclude
☑ ☒ Process N...	is	Autoruns.exe	Exclude
☑ ☒ Process N...	is	Procmon64.exe	Exclude
☑ ☒ Process N...	is	Procexp64.exe	Exclude
☑ ☒ Process N	is	System	Exclude

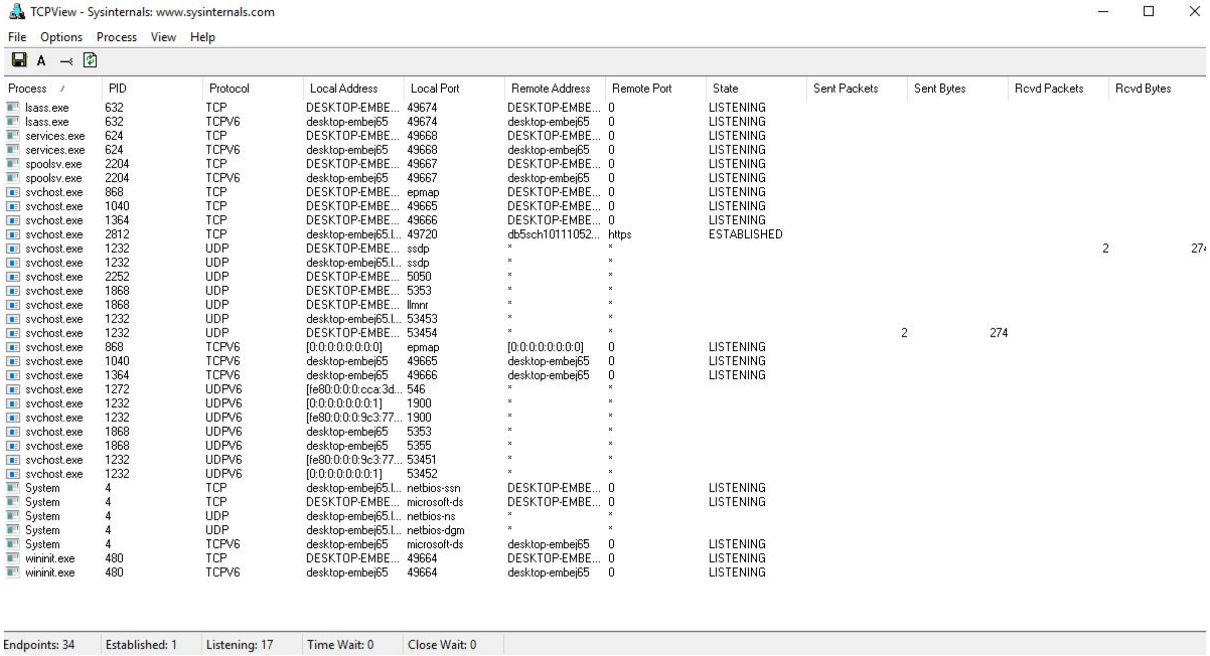
Microsoft Windows Search
Microsoft Corporation
C:\Windows\system32\Sea

Time ...	Process Name	PID	Operati			
3:59:5...	Explorer.EXE	416	Read			
3:59:5...	SearchIndexer....	6088	Read			
3:59:5...	Explorer.EXE	416	Read			
3:59:5...	taskhc					
3:59:5...	Searcl					
3:59:5...	Explor					
3:59:5...	SearchIndexer....	6088	FileSy			
3:59:5...	taskhostw.exe	4572	RegC			
3:59:5...	taskhostw.exe	4572	RegC			
3:59:5...	taskhostw.exe	4572	RegC			
3:59:5...	taskhostw.exe	4572	RegC			
3:59:5...	Explorer.EXE	416	Read			
3:59:5...	Explorer.EXE	416	Read			
3:59:5...	Explorer.EXE	416	Read			
3:59:5...	Explorer.EXE	416	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
3:59:5...	Explorer.EXE	416	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
3:59:5...	Explorer.EXE	416	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
3:59:5...	Explorer.EXE	416	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
3:59:5...	Explorer.EXE	416	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
3:59:5...	Explorer.EXE	416	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
3:59:5...	Explorer.EXE	416	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
3:59:5...	Explorer.EXE	416	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
3:59:5...	Explorer.EXE	416	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
3:59:5...	Explorer.EXE	416	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
3:59:5...	Explorer.EXE	416	CreateFile	C:\Users\User\AppData\Local\Temp\P...	SUCCESS	Desired Access: R...
3:59:5...	Explorer.EXE	416	QueryBasicInfor...	C:\Users\User\AppData\Local\Temp\P...	SUCCESS	CreationTime: 3/22...
3:59:5...	Explorer.EXE	416	CloseFile	C:\Users\User\AppData\Local\Temp\P...	SUCCESS	
3:59:5...	Explorer.EXE	416	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
3:59:5...	Explorer.EXE	416	RegOpenKey	HKLM\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: Q...
3:59:5...	Explorer.EXE	416	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_DWO...
3:59:5...	Explorer.EXE	416	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
3:59:5...	Explorer.EXE	416	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
3:59:5...	Explorer.EXE	416	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: Q...
3:59:5...	Explorer.EXE	416	RegQueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_DWO...
3:59:5...	Explorer.EXE	416	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	
3:59:5...	Explorer.EXE	416	ReadFile	C:\Windows\System32\thumbcache.dll	SUCCESS	Offset: 319,488, Le...
3:59:5...	Explorer.EXE	416	ReadFile	C:\Windows\System32\windows.storag...	SUCCESS	Offset: 6,317,056, ...
3:59:5...	Explorer.EXE	416	QueryStandardI...	C:\Users\User\AppData\Local\Microso...	SUCCESS	AllocationSize: 32,...
3:59:5...	Explorer.EXE	416	CreateFile	C:\Users\User\AppData\Local\Temp\P...	SUCCESS	Desired Access: R...
3:59:5...	Explorer.EXE	416	QueryBasicInfor...	C:\Users\User\AppData\Local\Temp\P...	SUCCESS	CreationTime: 3/22...

Showing 55,600 of 224,014 events (24%) | Backed by virtual memory

Tcp View

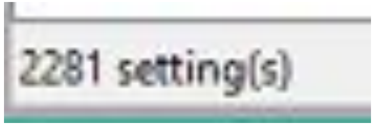
- Very similar to netstat
  - provides a bit more info
  - runs in a loop
- Useful for finding beacons or injected processes calling out



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
lsass.exe	632	TCP	DESKTOP-EMBE...	49674	DESKTOP-EMBE...	0	LISTENING				
lsass.exe	632	TCPV6	desktop-embej65	49674	desktop-embej65	0	LISTENING				
services.exe	624	TCP	DESKTOP-EMBE...	49668	DESKTOP-EMBE...	0	LISTENING				
services.exe	624	TCPV6	desktop-embej65	49668	desktop-embej65	0	LISTENING				
spoolsv.exe	2204	TCP	DESKTOP-EMBE...	49667	DESKTOP-EMBE...	0	LISTENING				
spoolsv.exe	2204	TCPV6	desktop-embej65	49667	desktop-embej65	0	LISTENING				
svchost.exe	868	TCP	DESKTOP-EMBE...	epmap	DESKTOP-EMBE...	0	LISTENING				
svchost.exe	1040	TCP	DESKTOP-EMBE...	49665	DESKTOP-EMBE...	0	LISTENING				
svchost.exe	1364	TCP	DESKTOP-EMBE...	49666	DESKTOP-EMBE...	0	LISTENING				
svchost.exe	2812	TCP	desktop-embej65.l...	49720	db5sch10111052...	https	ESTABLISHED				
svchost.exe	1232	UDP	DESKTOP-EMBE...	ssdp	*	*				2	27
svchost.exe	1232	UDP	desktop-embej65.l...	ssdp	*	*					
svchost.exe	2252	UDP	DESKTOP-EMBE...	5050	*	*					
svchost.exe	1868	UDP	DESKTOP-EMBE...	5353	*	*					
svchost.exe	1868	UDP	DESKTOP-EMBE...	llmnr	*	*					
svchost.exe	1232	UDP	desktop-embej65.l...	53453	*	*					
svchost.exe	1232	UDP	DESKTOP-EMBE...	53454	*	*		2	274		
svchost.exe	868	TCPV6	[0:0:0:0:0:0:0:0]	epmap	[0:0:0:0:0:0:0:0]	0	LISTENING				
svchost.exe	1040	TCPV6	desktop-embej65	49665	desktop-embej65	0	LISTENING				
svchost.exe	1364	TCPV6	desktop-embej65	49666	desktop-embej65	0	LISTENING				
svchost.exe	1272	UDPV6	[fe80:0:0:0:cca:3d...	546	*	*					
svchost.exe	1232	UDPV6	[0:0:0:0:0:0:0:1]	1900	*	*					
svchost.exe	1232	UDPV6	[fe80:0:0:0:9c3:77...	1900	*	*					
svchost.exe	1868	UDPV6	desktop-embej65	5353	*	*					
svchost.exe	1868	UDPV6	desktop-embej65	5355	*	*					
svchost.exe	1232	UDPV6	[fe80:0:0:0:9c3:77...	53451	*	*					
svchost.exe	1232	UDPV6	[0:0:0:0:0:0:0:1]	53452	*	*					
System	4	TCP	desktop-embej65.l...	netbios-ssn	DESKTOP-EMBE...	0	LISTENING				
System	4	TCP	DESKTOP-EMBE...	microsoft-ds	DESKTOP-EMBE...	0	LISTENING				
System	4	UDP	desktop-embej65.l...	netbios-ns	*	*					
System	4	UDP	desktop-embej65.l...	netbios-dgm	*	*					
System	4	TCPV6	desktop-embej65	microsoft-ds	desktop-embej65	0	LISTENING				
wininit.exe	480	TCP	DESKTOP-EMBE...	49664	DESKTOP-EMBE...	0	LISTENING				
wininit.exe	480	TCPV6	desktop-embej65	49664	desktop-embej65	0	LISTENING				

Endpoints: 34 | Established: 1 | Listening: 17 | Time Wait: 0 | Close Wait: 0

Group Policy



2281 setting(s)

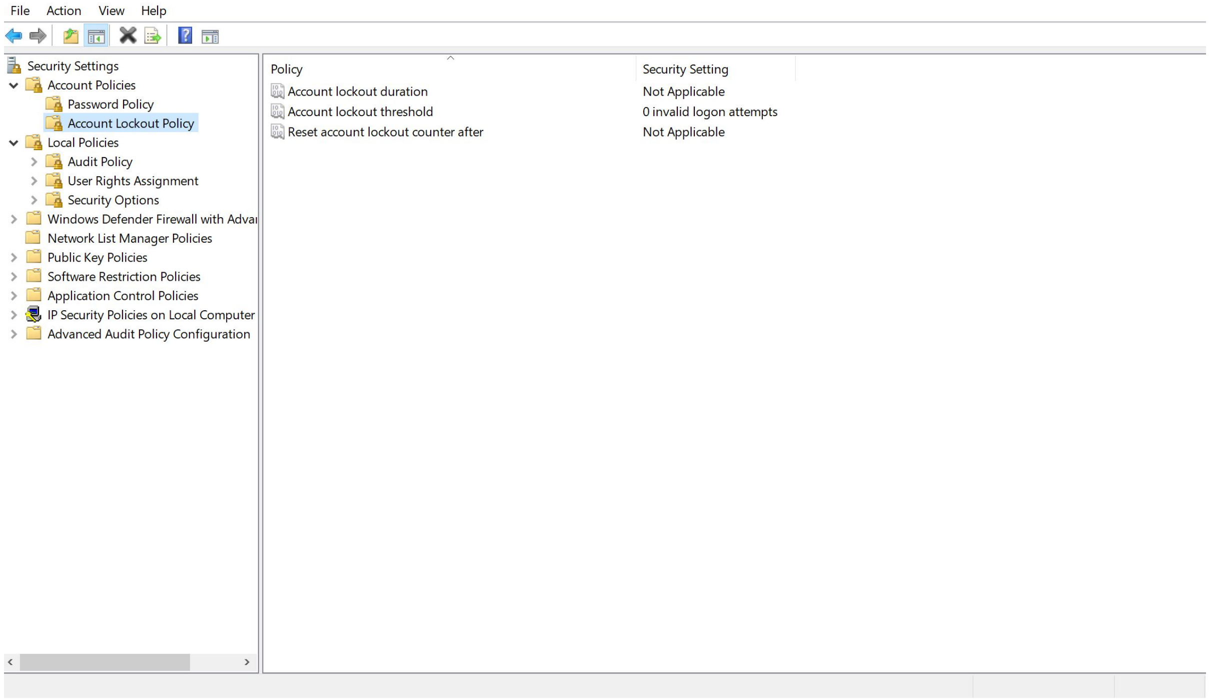
Yes, that’s 2281 different settings

- This can be your best friend if you know what settings to change
  - Deny users right to logon to your computer
- Can create policies that deploy to every computer on the domain
- Main settings you want to look at
  - Computer Config -> Windows Settings -> Security Settings
    - Account Policies
      - Password requirements (length, complexity, age)
      - Account Lockout Policy
    - Local Policies
      - Deny user/group logon rights
      - Enable logging of important events
      - Most security based things

Group Policy cont.

- Be careful with some settings ----------------------------------> you might lock yourself out if threshold and stuff is set to high numbers

- Group Policy is important to implement since it overrides the Local Security Policy



- Security Settings
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Windows Defender Firewall with Advai
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Computer
  - Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	Not Applicable
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Applicable

Process Injection

- Attackers will often times attempt to hollow out space in other processes
- Almost impossible to see unless looking at individual threads
- Ways to defeat & detect Process Injection:
  - Restart your computer!
    - Injected processes aren't persistent (a persistent process must inject them)
  - Find bad threads and suspend them
    - Can be done using netstat and looking for callbacks
    - Use Process Explorer to look at running threads

Questions?

Demo info:

<info here>

Thank you

Feedback: https://rc3club.typeform.com/to/JdS2lV