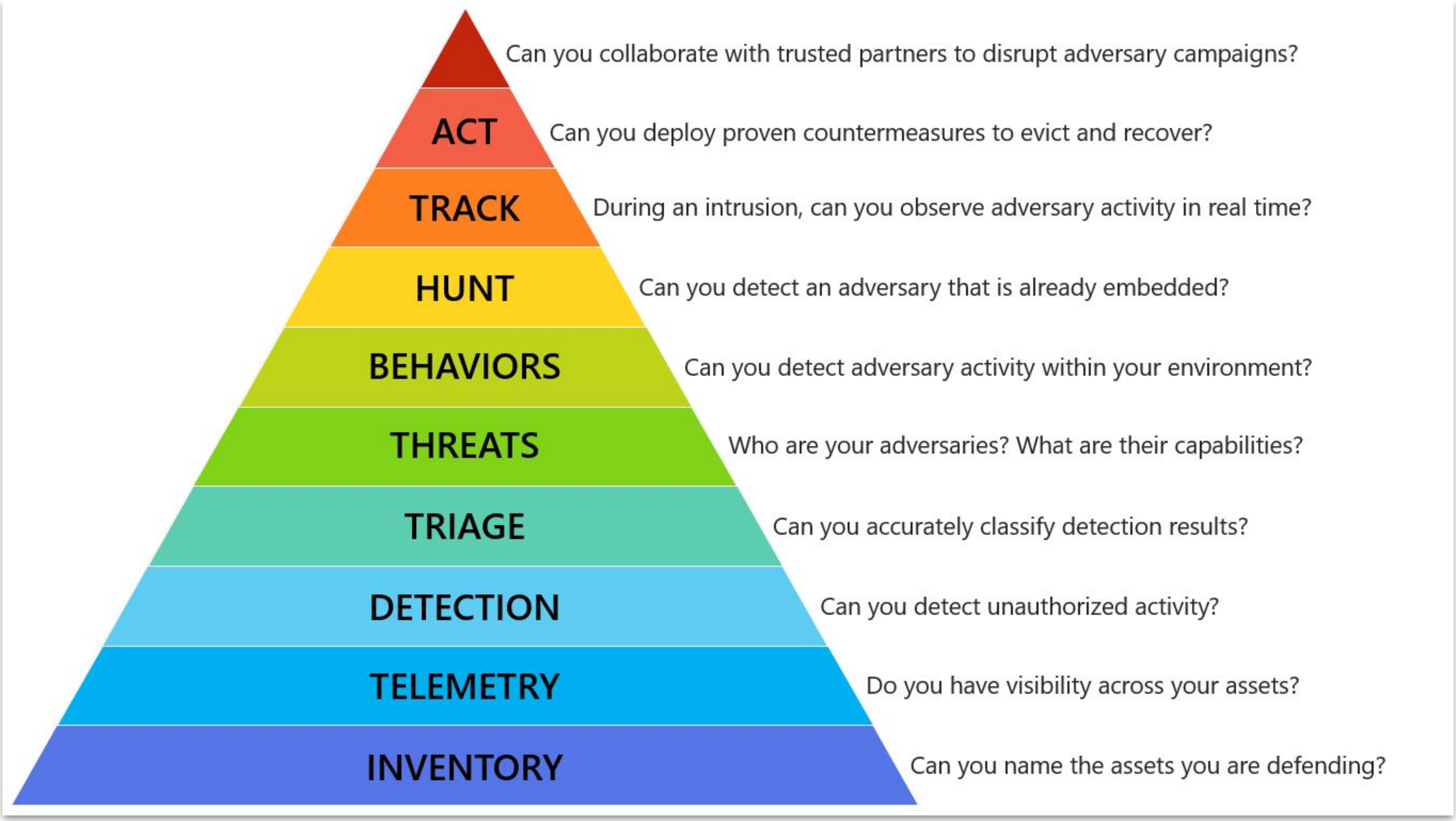
Intro to Windows Threat Hunting

With a focus on Red vs Blue Competitions
Liam Smith / Johnny Thunder 🌩

Threat Hunting 101



Can you collaborate with trusted partners to disrupt adversary campaigns?

ACT — Can you deploy proven countermeasures to evict and recover?

TRACK — During an intrusion, can you observe adversary activity in real time?

HUNT — Can you detect an adversary that is already embedded?

BEHAVIORS — Can you detect adversary activity within your environment?

THREATS — Who are your adversaries? What are their capabilities?

TRIAGE — Can you accurately classify detection results?

DETECTION — Can you detect unauthorized activity?

TELEMETRY — Do you have visibility across your assets?

INVENTORY — Can you name the assets you are defending?

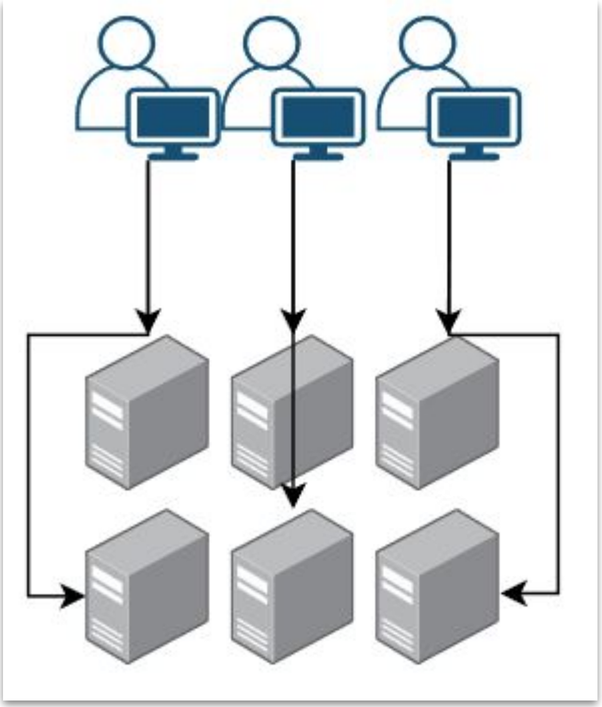
The Incident Response Hierarchy of Needs

CCDC “Threat Hunting” Collection

- Collecting Data one machine at a time.
- Each person tries to look at the same stuff on each machine.
- Viewing Data on Local Server / Machine you are investigating.

Leads to?

- Context of data (processes, autoruns, traffic) in the domain? **Nah.**
- Viewing data in uniform way? **Nah.**
- Looking at a live process list going *“hmm yup those are processes”* not knowing what even is the purpose as the ticking clock of death relentlessly moves as you stare at the list hoping something happens. **Yes.**



Scalable Threat Hunting Collection

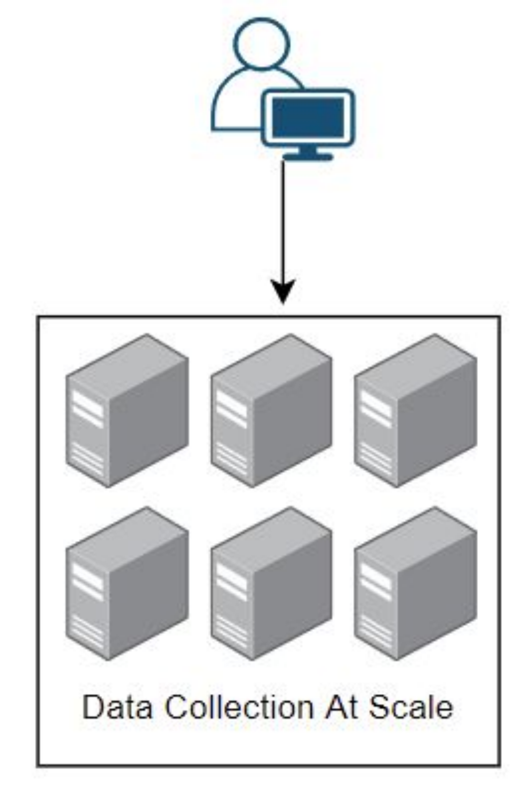
- **Our goal: Proactively searching on endpoints for evidence of compromise, and then querying those IOCs against all hosts.**

Advantages:

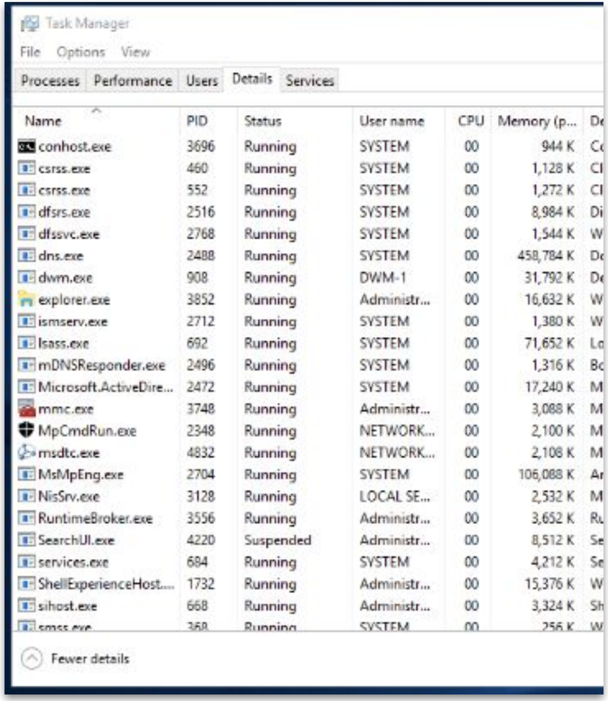
- Pulling the same data from all hosts in the environment.
- Get that IR data into a form you can actually review. IE Spreadsheets/CSVs you can grep, open in excel, and stack.
- Gets the context of the full domain. IE Is this process strange? It's on all the hosts so probably not.
- Ephemeral data (ie exists for a limited time) can be pulled an preserved.

What does this actually mean?

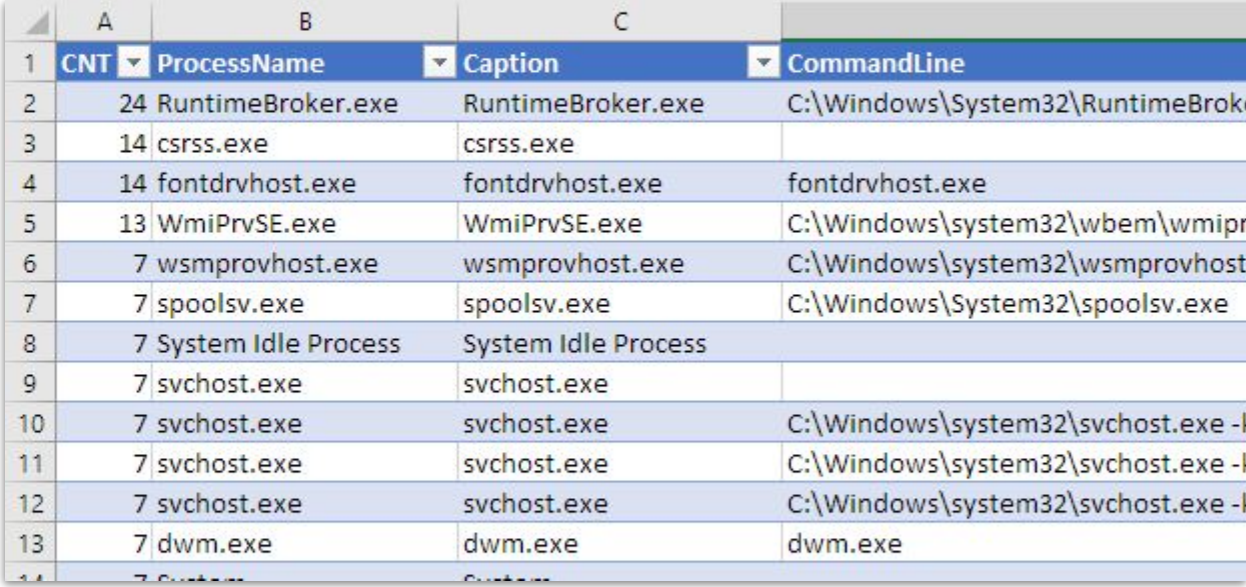
- Get process lists, persistence data, query event logs, etc. against all hosts and get the results to you in an easy to work with format.



Forgive the simple diagram.



Name	PID	Status	User name	CPU	Memory (p...	De
conhost.exe	3696	Running	SYSTEM	00	944 K	Cc
csrss.exe	460	Running	SYSTEM	00	1,128 K	Cl
csrss.exe	552	Running	SYSTEM	00	1,272 K	Cl
dfsrs.exe	2516	Running	SYSTEM	00	8,984 K	Di
dfssvc.exe	2768	Running	SYSTEM	00	1,544 K	W
dns.exe	2488	Running	SYSTEM	00	458,784 K	Dc
dwm.exe	908	Running	DWM-1	00	31,792 K	De
explorer.exe	3852	Running	Administr...	00	16,632 K	W
ismserv.exe	2712	Running	SYSTEM	00	1,380 K	W
lsass.exe	692	Running	SYSTEM	00	71,652 K	Lc
mDNSResponder.exe	2496	Running	SYSTEM	00	1,316 K	Bc
Microsoft.ActiveDire...	2472	Running	SYSTEM	00	17,240 K	M
mmc.exe	3748	Running	Administr...	00	3,088 K	M
MpCmdRun.exe	2348	Running	NETWORK...	00	2,100 K	M
msdtc.exe	4832	Running	NETWORK...	00	2,108 K	M
MsMpEng.exe	2704	Running	SYSTEM	00	106,088 K	Ar
NisSrv.exe	3128	Running	LOCAL SE...	00	2,532 K	M
RuntimeBroker.exe	3556	Running	Administr...	00	3,652 K	Ru
SearchUI.exe	4220	Suspended	Administr...	00	8,512 K	Se
services.exe	684	Running	SYSTEM	00	4,212 K	Se
ShellExperienceHost....	1732	Running	Administr...	00	15,376 K	W
sihost.exe	668	Running	Administr...	00	3,324 K	Sh
smss.exe	368	Running	SYSTEM	00	256 K	W



	A	B	C	
1	CNT	ProcessName	Caption	CommandLine
2	24	RuntimeBroker.exe	RuntimeBroker.exe	C:\Windows\System32\RuntimeBrok
3	14	csrss.exe	csrss.exe	
4	14	fontdrvhost.exe	fontdrvhost.exe	fontdrvhost.exe
5	13	WmiPrvSE.exe	WmiPrvSE.exe	C:\Windows\system32\wbem\wmipr
6	7	wsmprovhost.exe	wsmprovhost.exe	C:\Windows\system32\wsmprovhost
7	7	spoolsv.exe	spoolsv.exe	C:\Windows\System32\spoolsv.exe
8	7	System Idle Process	System Idle Process	
9	7	svchost.exe	svchost.exe	
10	7	svchost.exe	svchost.exe	C:\Windows\system32\svchost.exe -l
11	7	svchost.exe	svchost.exe	C:\Windows\system32\svchost.exe -l
12	7	svchost.exe	svchost.exe	C:\Windows\system32\svchost.exe -l
13	7	dwm.exe	dwm.exe	dwm.exe
14	7	System	System	

This vs That.

Types of Indicators

Name	Definition	Example
Atomic	These are elements or fragments of data that cannot be broken down any further.	Example.com 1.1.1.1 evil.exe
Computed	These are fragments of data computed in a specific fashion to attack the system or perform the breach.	d41d8cd98f00b204e9800998ecf8427e
Behavioral	These are basically a combination of Atomic and computed IoC's.	Evil.exe (MD5) is a sample of BEACON malware used by the attacker to exfiltrate data to example.com.

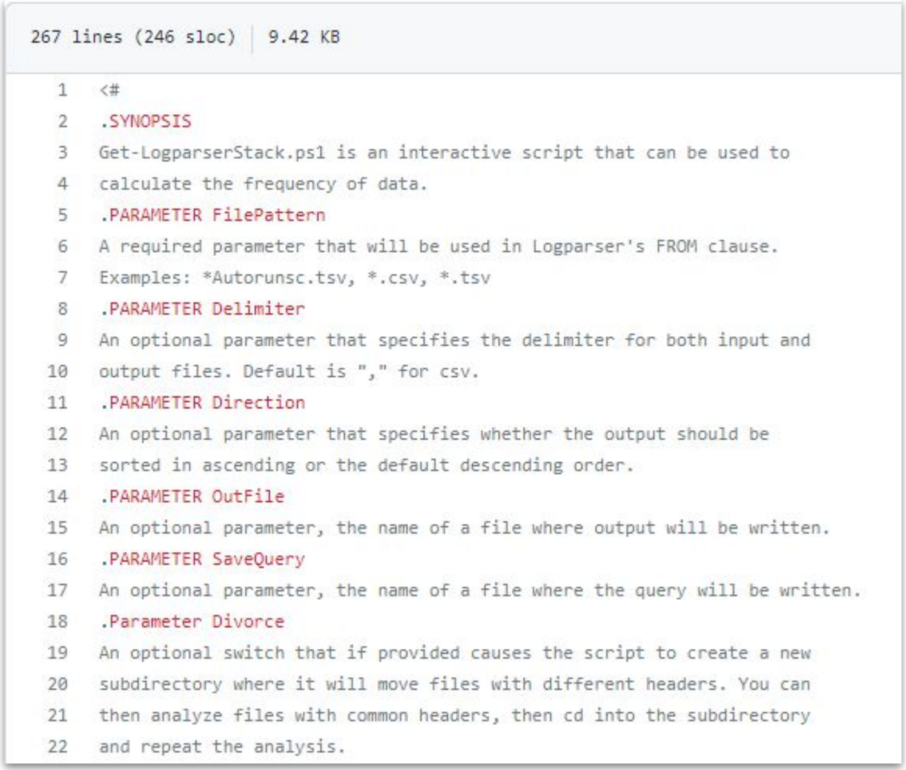
https://lifars.com/2020/05/what-are-indicators-of-compromise-iocs-used-for/

Defender Principles

Principle	Blue Team Advantage
Malware can hide but it must run.	Process listing analysis, memory forensics. - Difficulty: lots of data, and process injection.
Malware must persist.	Review of methods of persisting across a reboot. - Difficulty: is there are a lot of ways.
Malware is uncommon.	Comparison against clean machines. Frequency analysis (“stacking”) of data across multiple hosts. - Difficulty: CCDC most of those hosts are compromised.
Backdoors must communicate out, or be talked to.	What processes are talking on the network and why? Lock it down. - Difficulty: Noise.

Stacking Data

- Bedrock of Threat hunting.
- Malware is uncommon by its nature. At all times we can use stacking or frequency analysis to ask the following question:
    - Is this process, FQDN, IP, Service common in my environment.
- Thus we want current and historical data in a uniform format to facilitate stacking.
- [Get-LogparserStack.ps1]



267 lines (246 sloc) | 9.42 KB

```
<#
.SYNOPSIS
Get-LogparserStack.ps1 is an interactive script that can be used to
calculate the frequency of data.
.PARAMETER FilePattern
A required parameter that will be used in Logparser's FROM clause.
Examples: *Autorunsc.tsv, *.csv, *.tsv
.PARAMETER Delimiter
An optional parameter that specifies the delimiter for both input and
output files. Default is "," for csv.
.PARAMETER Direction
An optional parameter that specifies whether the output should be
sorted in ascending or the default descending order.
.PARAMETER OutFile
An optional parameter, the name of a file where output will be written.
.PARAMETER SaveQuery
An optional parameter, the name of a file where the query will be written.
.Parameter Divorce
An optional switch that if provided causes the script to create a new
subdirectory where it will move files with different headers. You can
then analyze files with common headers, then cd into the subdirectory
and repeat the analysis.
```

WTF am I looking for?

Stories for another time

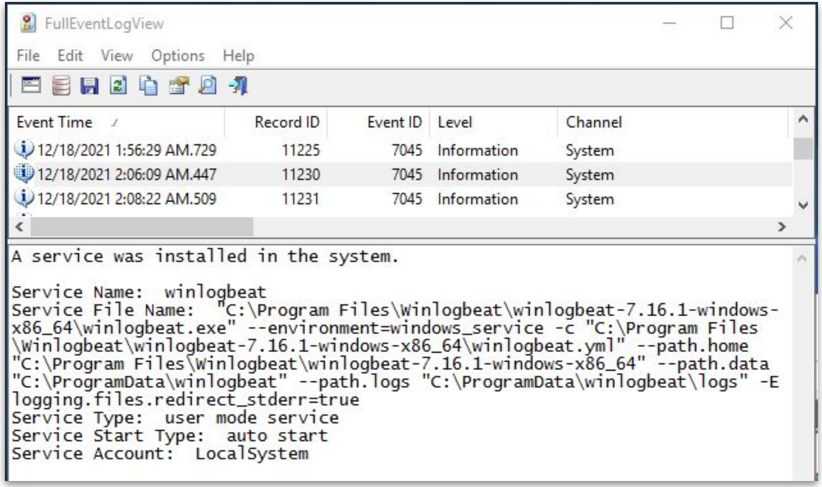
- Artifacts of execution hunting (Appcompat / Amcache / UserAssist)
- Searching for atomic indicators
- Network Hunting (DNS / process connections)

Persistence and Execution

Service Installs

Services are abused by threat actors at all points of a compromise. They can facilitate lateral movement, persistence, and execution. And, as a bonus, 7045s are low in frequency.

- 7040 – Start type changed (Boot | On Request | Disabled)
- 7045 – A service was installed on the system



Event Time	Record ID	Event ID	Level	Channel
12/18/2021 1:56:29 AM.729	11225	7045	Information	System
12/18/2021 2:06:09 AM.447	11230	7045	Information	System
12/18/2021 2:08:22 AM.509	11231	7045	Information	System

```
A service was installed in the system.

Service Name:  winlogbeat
Service File Name:  "C:\Program Files\Winlogbeat\winlogbeat-7.16.1-windows-
x86_64\winlogbeat.exe" --environment=windows_service -c "C:\Program Files
\Winlogbeat\winlogbeat-7.16.1-windows-x86_64\winlogbeat.yml" --path.home
"C:\Program Files\Winlogbeat\winlogbeat-7.16.1-windows-x86_64" --path.data
"C:\ProgramData\winlogbeat" --path.logs "C:\ProgramData\winlogbeat\logs" -E
logging.files.redirect_stderr=true
Service Type:  user mode service
Service Start Type:  auto start
Service Account:  LocalSystem
```

Scheduled Tasks

All scheduled tasks historically in the environment are suspect. They can facilitate lateral movement, persistence, and execution.

Microsoft-Windows-Task Scheduler%4Maintenance.evtx

- 106 – Scheduled task created
- 140 – Scheduled task updated
- 141 – Scheduled task deleted
- 200/201 – Scheduled task executed/completed

schtasks /Delete /TN [taskname] /F

WMI Persistence

WMI allows for the creation of “Filter” to “Consumer” “bindings”.

- Basically a “if this then that” triggering of VBS scripts, or arbitrary command.
- These are not widely used for legitimate purposes* so all are suspect.
- **Event ID 5861** is logged on Windows 10 systems when new EventFilterToConsumerBinding events are created.

```
Get-WmiObject -Namespace root\Default -Class __EventFilter

Get-WmiObject -Namespace root\Default -Class __EventConsumer

Get-WmiObject -Namespace root\Default -Class __FilterToConsumerBinding
```

Name	Definition
WMI Filters	These are trigger conditions. Think time of day, service start, file created etc.
WMI Consumers	Event to perform. Ultra sus are - ActiveScriptEventConsumer (VB or JScript Launch) and CommandLineEventConsumer
WMI Binding	Glues the Filter to the Consumer

DLL Persistence Attacks

DLL Search Order Hijacking

- Abuses the fact that when an EXE needs to load a function from a DLL, windows searches for that DLL in a predictable way. Place a malicious DLL ahead of the order to load code.
- If you ever see a legit signed EXE in a folder with a sus DLL, this is likely this attack.

Phantom DLL Hijacking

- Find DLLs an EXE wants to load but the DLL does not exist legitimately anymore. Often the case with legacy code

DLL Side-Loading

- Abuses the windows Side-by-Side (WinSxS) service that supports legacy code.
- The evil DLL is a new version of legacy code so I must run it!

These attacks are hard to find. Review systems for DLLs with no or invalid signatures. Keep in mind that legit processes / EXEs can be running evil code.

DLL Persistence Attacks - PT2

DLL Search Order Hijacking Search

```
reg query "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\KnownDLLs"
gci -path C:\Windows\* -include *.dll | Get-AuthenticodeSignature | Where-Object Status
-NE "Valid"
gci -path C:\Windows\System32\* -include *.dll | Get-AuthenticodeSignature | Where-Object
Status -NE "Valid"
gps | FL ProcessName, @{l="Modules";e={$_.Modules|Out-String}}
gps | ? {$_.Modules -like '*{DLLNAME}*'} | FL ProcessName,
@{l="Modules";e={$_.Modules|Out-String}}
$dll = gps | Where {$_.Modules -like '*{DLLNAME}*' } | Select Modules;$dll.Modules;
(gps).Modules.FileName
(gps).Modules | FL FileName,FileVersionInfo
(gps).Modules.FileName | get-authenticodesignature | ? Status -NE "Valid"
```

https://www.jaiminton.com/cheatsheet/DFIR/#t1038-dll-search-order-hijacking

DLL Persistence Attacks - PT3

DLL Side-Loading Search

```
gci -path C:\Windows\WinSxS -recurse -include *.dll | Get-AuthenticodeSignature |
Where-Object Status -E "NotSigned"
gci -path C:\Windows\WinSxS -recurse -include *.ocx | Get-AuthenticodeSignature |
Where-Object Status -NE "Valid"
```

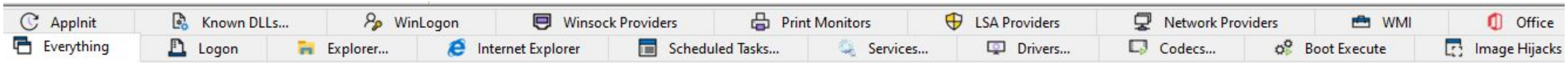
https://www.jaiminton.com/cheatsheet/DFIR/#locate-possible-dll-side-loading

Use Autoruns and Stay Humble

As of Jan 2022, Mitre ATT&CK has 19 core persistence techniques and plenty of of sub techniques. Hexacorn is on part 135 of the “Beyond good ol’ Run key”

- Be on the lookout for the new hotness, whatever that may be, but first know the core persistence mechanisms.
- “It aint stupid if it works” applies generally. And if you cant find basic persistence dont spend time sweating the esoteric stuff.

Autoruns Coverage	Notes
Registry + Other Autostart Location	Covers most registry run keys, user startup folders.
Services	Covers current service installs. (Not historical).
Scheduled Task	Covers currently scheduled scheduled tasks. (Not historical).
WMI Events	Current WMI filter to consumer bindings



Live Process

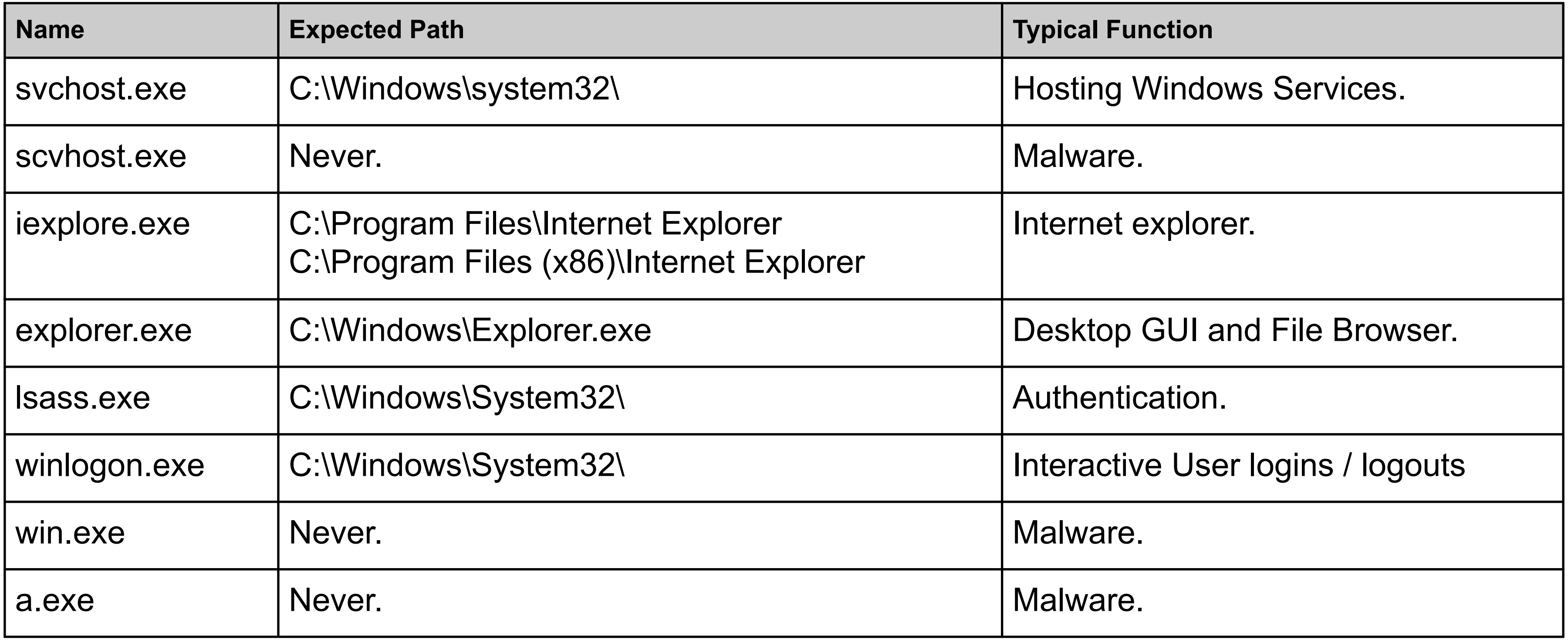
Process Analysis

Review processes for:

- Low frequency in the environment
- Misspelled binaries that are masquerading as legit
- Running out of common attacker directories
- Processes Out of the Wrong Directory
- Commonly Abused binaries - regsvr32.exe/mshta.exe/wscript.exe/cscript.exe

Data Sources to Help

- 4688 - Security - A process was created
- 1 - Sysmon - A process was created
- Live process listing with Kansa



Name	Expected Path	Typical Function
svchost.exe	C:\Windows\system32\	Hosting Windows Services.
scvhost.exe	Never.	Malware.
iexplore.exe	C:\Program Files\Internet Explorer C:\Program Files (x86)\Internet Explorer	Internet explorer.
explorer.exe	C:\Windows\Explorer.exe	Desktop GUI and File Browser.
lsass.exe	C:\Windows\System32\	Authentication.
winlogon.exe	C:\Windows\System32\	Interactive User logins / logouts
win.exe	Never.	Malware.
a.exe	Never.	Malware.

Resources -

https://www.echotrail.io/insights/search/svchost.exe

https://www.sans.org/posters/hunt-evil/

Common Malware Locations/Staging Directory	Notes
C:\Windows\System32	Abusing malware with the same name as legit windows binaries but in C:\Windows vs C:\Windows\System32
C:\Windows	
C:\Temp C:\Windows\Temp C:\Users\<USER>\AppData\Local\Temp	Temp directories are plentiful in Windows and are often writable by any user.
C:\PerfLogs	Default root folder that often has little contents.
C:\Users\Public	Default Public user folder and sub folders.
C:\Users\<USER>\AppData	User AppData Local, Roaming, and LocalLow subdirs.
C:\Windows\WinSxS	Windows Side-By-Side service.
C:\System Volume Information	Volume Shadow Copies folder.
C:\$Recycle Bin	Hidden recycle bin folder.
C:\Program Files	Installed Programs

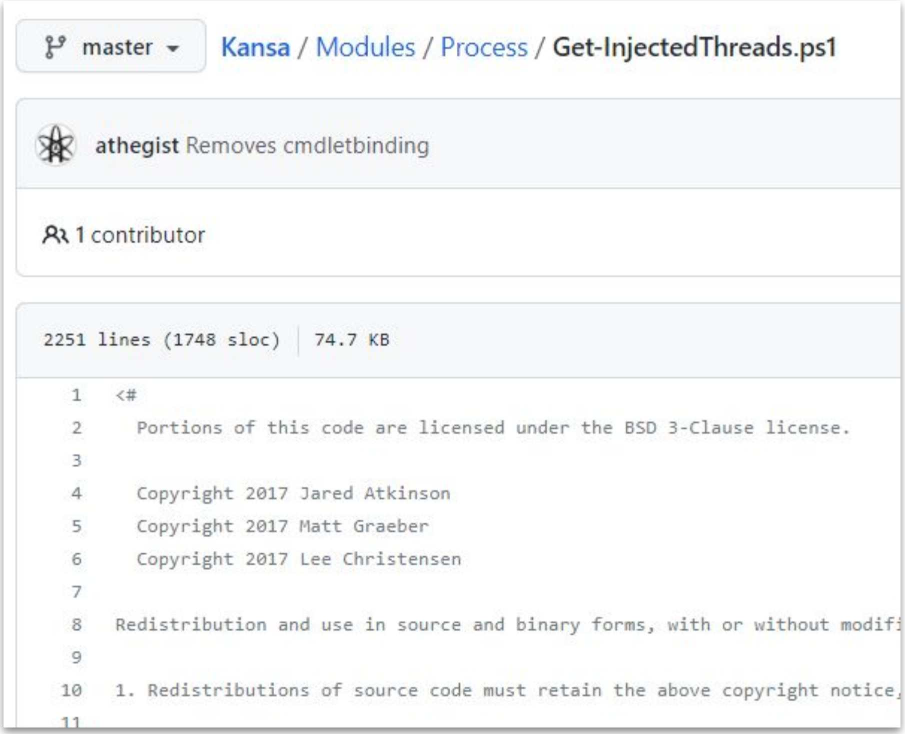
Process Injection

Processes that Contain Injected Threads.

- Process injection is a method of executing arbitrary code in the address space of a separate live process. The best way to find this is via [Get-InjectedThreads.ps1]()

```
Import-Module .\Get-InjectedThreads.ps1

Get-InjectedThreads
```



master
Kansa / Modules / Process / Get-InjectedThreads.ps1
athegist Removes cmdletbinding
1 contributor
2251 lines (1748 sloc) | 74.7 KB

```
<#
  Portions of this code are licensed under the BSD 3-Clause license.

  Copyright 2017 Jared Atkinson
  Copyright 2017 Matt Graeber
  Copyright 2017 Lee Christensen

Redistribution and use in source and binary forms, with or without modifi

1. Redistributions of source code must retain the above copyright notice,
```

Better Logging

TL;DR - Windows Logging Needs Help

- Default Windows logging for what we want is lacking.
- Supplemental
  - Sysmon
- Built in logging we need to configure:
  - By Default Windows Logging can be very helpful, but we need to configure it.
  - Audit logging
    - Process Events
    - User Authentication
  - Powershell Logging

Sysinternals Sysmon - PT1

- Sysmon is a free sensor/agent that can be installed on systems to generate logs for important events on systems
- Two Parts
  - Sysmon.exe binary
  - A config file
    - https://github.com/SwiftOnSecurity/sysmon-config
    - https://github.com/ion-storm/sysmon-config
- Not to be confused with:
  - Procmon - live monitoring of Network, Reg, Filesystem changes.
  - Process Explorer - Basically a better task manager. (It can do so much more but for now that's what matters)
- Install:
  - Choco install sysinternals
  - Get your config on disk or an SMB share.
  - sysmon.exe -accepteula -i sysmonconfig-export.xml

Sysinternals Sysmon - PT2

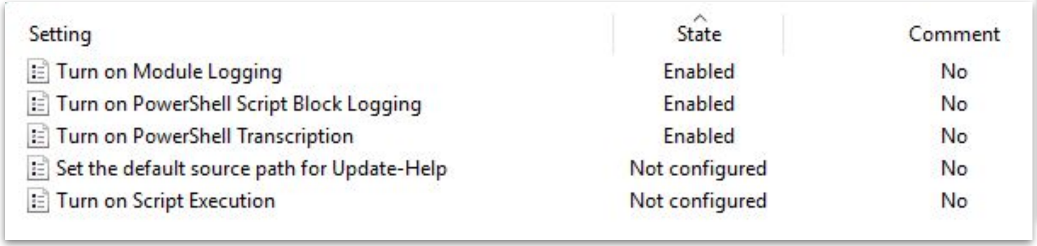
1	Process Created	11	FileCreate
2	process changed a file creation time	12	Registry Event (Object Create / Deleted)
3	Network Connection	13	Registry Event Value Set
4	Sysmon Service Changed	14	Registry Event (Key and value Rename)
5	Process Terminated	15	FileCreateStreamHash
6	Driver Loaded	17	PipeEvent (Pipe Created)
7	Image Loaded	18	PipeEvent (Pipe Connected)
8	CreateRemote Thread	19	WMI Event (WmiEventFilter activity detected)
9	Raw Access Read	20	WmiEvent (WmiEventConsumer activity detected)
10	Process Access	21	WmiEvent (WmiEventConsumerToFilter activity detected)
		22	DNS

Enable Powershell Script Block Logging -PT1

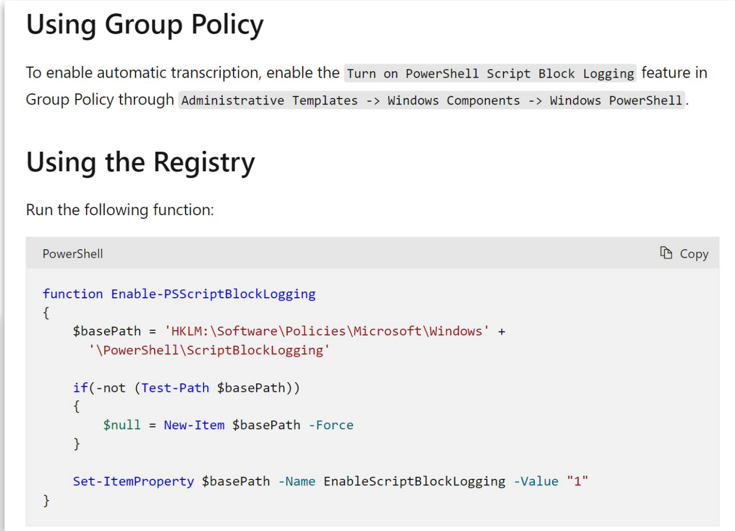
- One of the most valuable logs you can have, shows attacker activity
- Default: powershell v4+ logs warning level script block logs (not good enough)
- Use Winrm to configure it with powershell script or use GPO

GPO:

Administrative Templates → Windows Components → Windows PowerShell
Turn on Module - > Set *
Scripting Block -> Log Script Block checked
Transcript -> Include Invo Checked



Setting	State	Comment
Turn on Module Logging	Enabled	No
Turn on PowerShell Script Block Logging	Enabled	No
Turn on PowerShell Transcription	Enabled	No
Set the default source path for Update-Help	Not configured	No
Turn on Script Execution	Not configured	No



Using Group Policy

To enable automatic transcription, enable the `Turn on PowerShell Script Block Logging` feature in Group Policy through `Administrative Templates -> Windows Components -> Windows PowerShell`.

Using the Registry

Run the following function:

```powershell
function Enable-PSScriptBlockLogging
{
    $basePath = 'HKLM:\Software\Policies\Microsoft\Windows' +
      '\PowerShell\ScriptBlockLogging'

    if(-not (Test-Path $basePath))
    {
        $null = New-Item $basePath -Force
    }

    Set-ItemProperty $basePath -Name EnableScriptBlockLogging -Value "1"
}
```

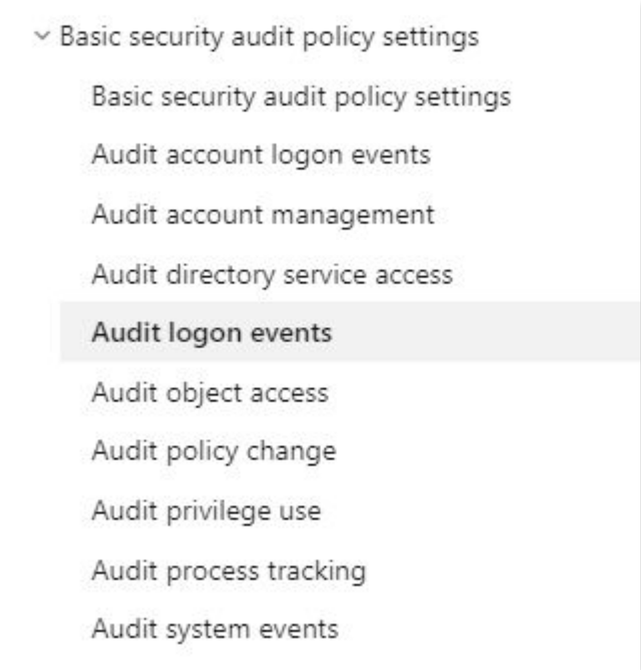
Enable Powershell Script Block Logging -PT2

Powershell Logging	Notes
Scripting Block -> Log Script Block checked	Script block logging records blocks of code as they are executed by the PowerShell engine, thereby capturing the full contents of code executed by an attacker, including scripts and commands. Gets you the amazing 4104 Event logs. - Basically EZ mode what is happening with powershell in my environment. Collect them and look at them. Fun read here - https://www.splunk.com/en_us/blog/security/hunting-for-malicious-powershell-using-script-block-logging.html
Transcript -> Include Invo Checked	Stores a history (input and output) of powershell to - `$Home\My Documents\PowerShell_transcript.<time-stamp>.txt` - Good for single system analysis but hard to collect
Turn on Module - > Set *	Module logging records pipeline execution details as PowerShell executes, including variable initialization and command invocations. Module logging will record portions of scripts, some de-obfuscated code, and some data formatted for output. Gets you 4103 events. - Valuable but lot of events. 4104 events are preferred IMHO.

https://www.mandiant.com/resources/greater-visibilityt

Enable Audit Logging - PT1

- CC -> Policies -> Windows Settings -> Security Settings -> Advanced Audit



Basic security audit policy settings

Basic security audit policy settings

Audit account logon events

Audit account management

Audit directory service access

Audit logon events

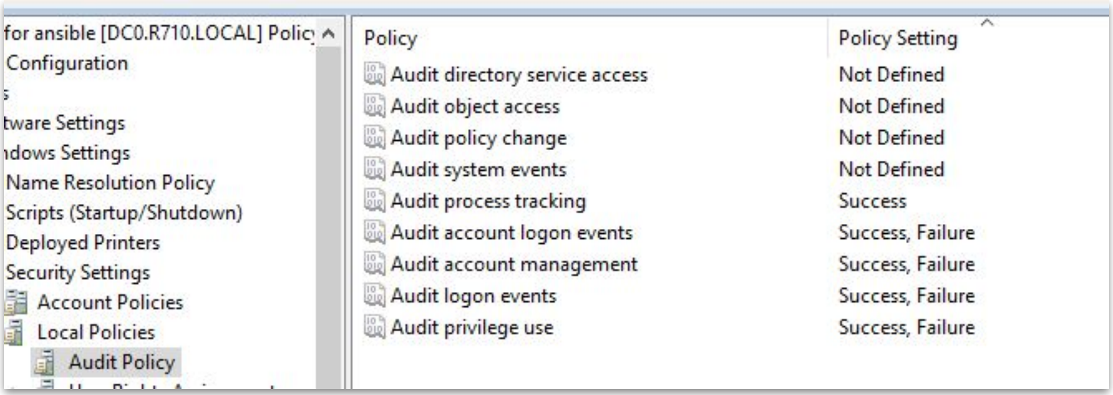
Audit object access

Audit policy change

Audit privilege use

Audit process tracking

Audit system events



for ansible [DC0.R710.LOCAL] Polic
Configuration
s
tware Settings
ndows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy

Policy	Policy Setting
Audit directory service access	Not Defined
Audit object access	Not Defined
Audit policy change	Not Defined
Audit system events	Not Defined
Audit process tracking	Success
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit logon events	Success, Failure
Audit privilege use	Success, Failure

https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-security-audit-policy-settings

Enable Audit Logging - PT2

Audit Logging	**Notes**
Audit Process Tracking	Success - Stored Per Machine - **4688 Event ID in Security** - Imho - dont bother with failures.
Audit Account Management	S&F - Lots of logs - Stored on Domain Controller Examples of account management events include: 1. A user account or group is created, changed, or deleted. 2. A user account is renamed, disabled, or enabled. 3. A password is set or changed. 4720 A user account was created.
Audit Privilege Use	S&F - Noisy may want to skip if you dont have a SIEM 1. Bypass traverse checking 2. Debug programs 3. Create a token object 4. Replace process level token

Enable Audit Logging - PT3

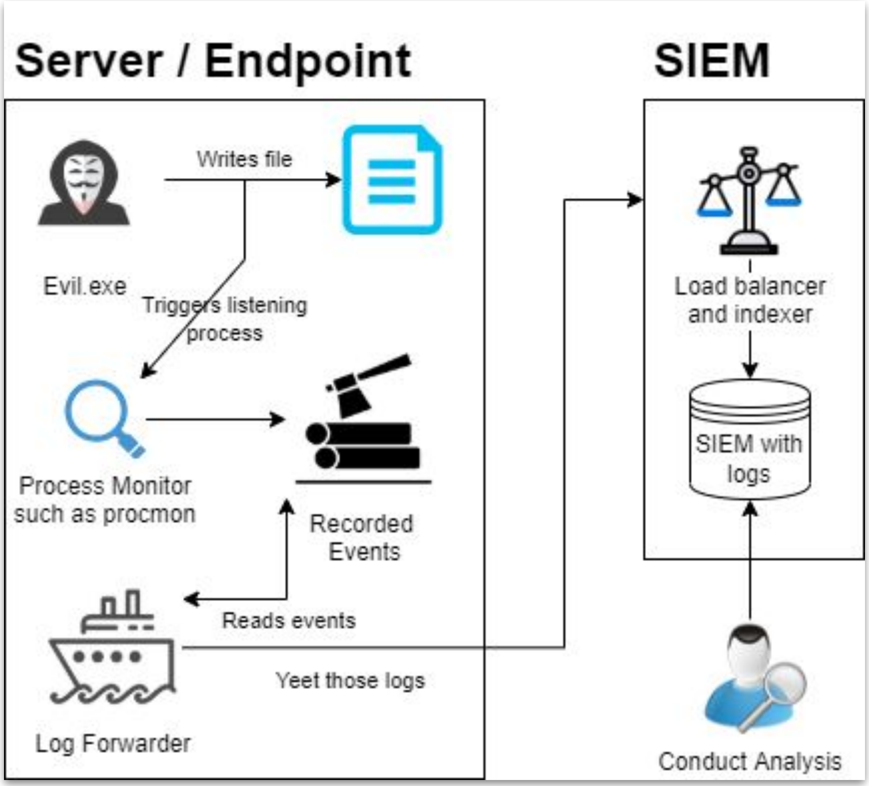
Audit Logging	**Notes**
Audit ***account*** logon events	Determines whether to audit each instance of a user logging on to or logging off from another device in which this device is used to validate the account. - Aka - I am a Domain Controller and User1 auths to Machine2 using me. Do ***I*** log the event? - S&F - to get domain controller presence.
Audit Logon Events	Determines whether to audit each instance of a user logging on to or logging off from a device. - AKA - I am Machine2 and User1 is logging on to me. Do I log the event? - S&F - Bread and butter IR/Threathunting - 4624/4625 Account Logon/Logon failure - 4634 Account Logoff

Review MS docs for more info, but if you do nothing else do the two green ones pls.

SIEM Threat Hunting

SIEM Basics

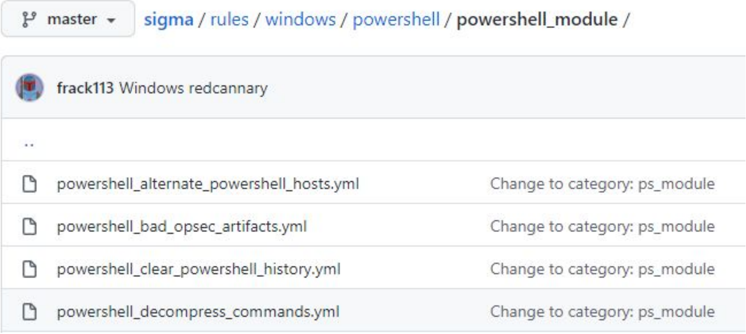
1. Something happens
2. Some process monitoring the API calls records that thing to an event log
3. Log forwarder notices the new log, parses it, and sends to indexer
4. Indexer looks at log and parses it into standard format
5. Throws into ‘data lake’
6. You look at that lake



Yes I made this.

SIGMA - Using Community detections

- Use opensource detections to get a head start.
- Sigma is a project with a lot of premade detections and can output to multiple SIEM search formats.
- https://github.com/SigmaHQ/sigma



sigma / rules / windows / powershell / powershell_module /

frack113 Windows redcannary

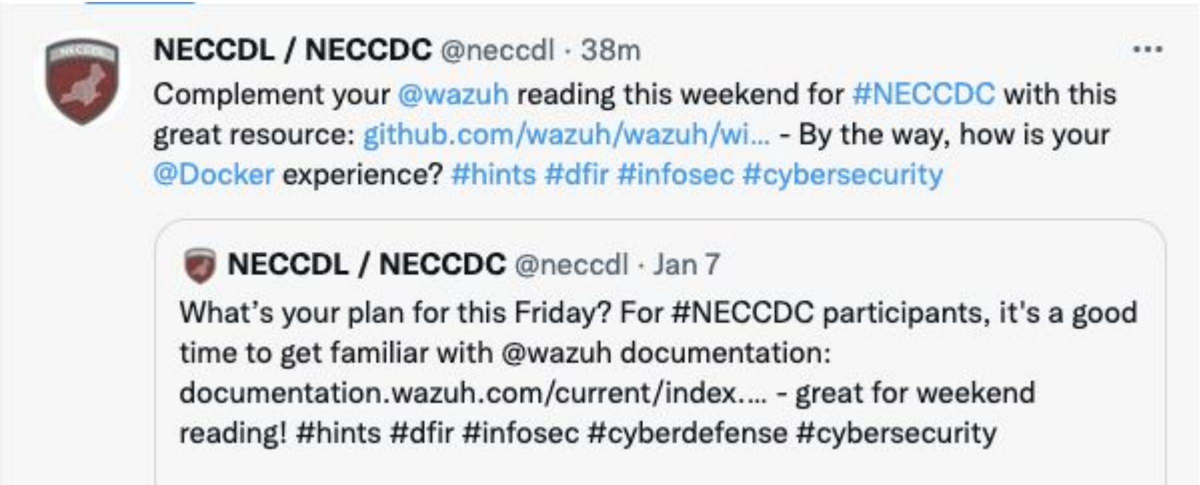
..

powershell_alternate_powershell_hosts.yml	Change to category: ps_module
powershell_bad_opsec_artifacts.yml	Change to category: ps_module
powershell_clear_powershell_history.yml	Change to category: ps_module
powershell_decompress_commands.yml	Change to category: ps_module

```
tools/sigmac -t splunk -c splunk-windows rules/windows/sysmon/sysmon_susp_image_load.yml
```

SIEM Requirement =)

- Only if they do not give you a SIEM
- Wazuh: https://github.com/wazuh/wazuh
  - Easy installation
  - Powerful detection features and log forwarding out of the box



NECCDL / NECCDC @neccdl · 38m

Complement your @wazuh reading this weekend for #NECCDC with this great resource: github.com/wazuh/wazuh/wi... - By the way, how is your @Docker experience? #hints #dfir #infosec #cybersecurity

> **NECCDL / NECCDC** @neccdl · Jan 7
>
> What's your plan for this Friday? For #NECCDC participants, it's a good time to get familiar with @wazuh documentation: documentation.wazuh.com/current/index.... - great for weekend reading! #hints #dfir #infosec #cyberdefense #cybersecurity

Kansa

What is Kansa?

- **Powershell based Incident Response collection and analysis platform.**
- Basically a bunch of powershell scripts do collect and process data.
- Why use it?
  - Is it the best framework out there? No.
  - Does it have the fastest, most comprehensive, best collection? No.
  - Is it maintained? Not from what I can tell.
- **So Why?**
  - **Agentless. IE no server you need to set up and an msi/exe to install.**
  - **Gets 90% of the data you can actually use in a Red vs Blue competition.**
  - **Only requires you set up WinRM. (10 minutes max via a GPO).**
  - **Run on one system get every system's data.**
  - **Built-in processing/stacking of data***

Requirements

- Enable WinRM via GPO - How to enable WinRM with domain controller Group Policy for WMI monitoring – Auvik Support
- Clone the Kansa repo
  - Get SysInternals AutoRunsc.exe to get that data.
  - Get LogParser.exe to stack data - https://www.microsoft.com/en-us/download/details.aspx?id=24659

Quick Static Reverse Engineering

Value of Static Reverse Engineering

- Quick, and without risk of
- Spot NBIs you could block on the firewall side
- Spot HBIs you could add to the report
- Spot Malware functionality to add to the incident report
- This will not catch everything

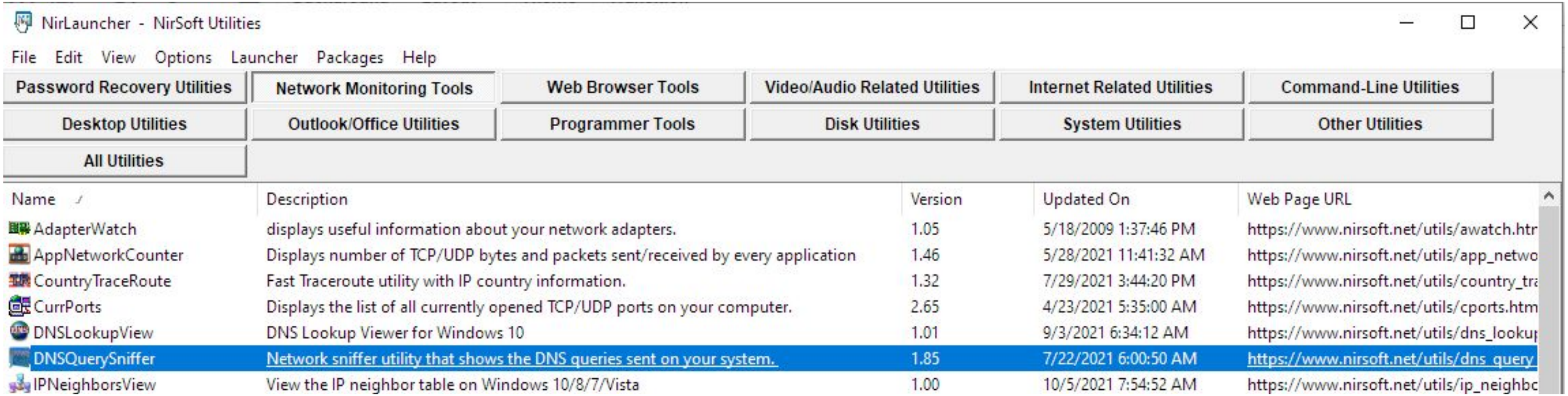
CCDC Past TTPs

Persistence

- Userinit keys on all of the boxes with a .scr extension, was a cobalt beacon
    - Windows will run some extensions as .exe: .scr, .ttf - https://www.howtogeek.com/137270/50-file-extensions-that-are-potentially-dangerous-on-windows
- Scheduled tasks, lots of them
- Services with powershell running on them
- Openssh Service installation
- Persistence through Powershell profiles
- Running scripts in powershell example
    - C:\Windows\System32\WindowsPowerShell\v1.0\Examples
    - C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Examples
- GPO installation of services
- Cred stealing with what we think is LSASS patch (detection: is lsass beaconing out)

Wrapping up

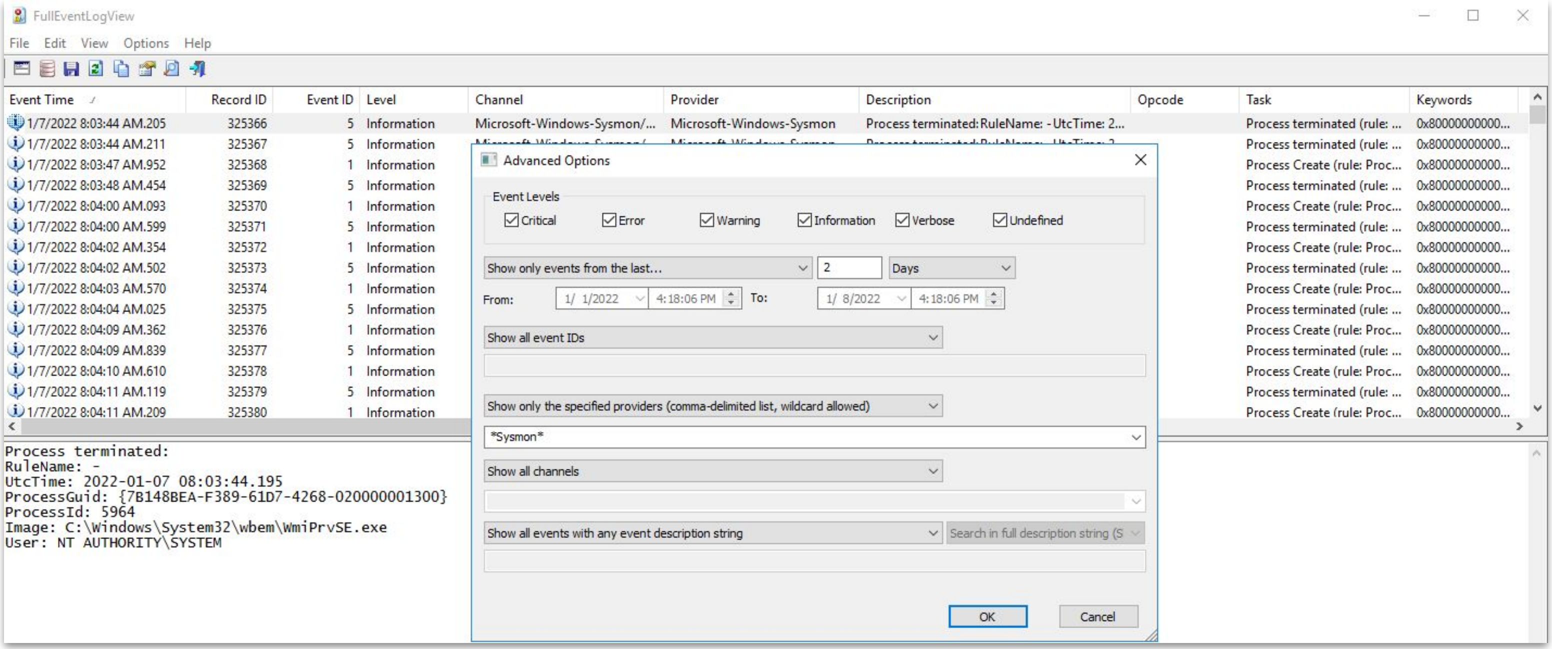
One off - NirSoft



Name	Description	Version	Updated On	Web Page URL
AdapterWatch	displays useful information about your network adapters.	1.05	5/18/2009 1:37:46 PM	https://www.nirsoft.net/utils/awatch.htr
AppNetworkCounter	Displays number of TCP/UDP bytes and packets sent/received by every application	1.46	5/28/2021 11:41:32 AM	https://www.nirsoft.net/utils/app_netwo
CountryTraceRoute	Fast Traceroute utility with IP country information.	1.32	7/29/2021 3:44:20 PM	https://www.nirsoft.net/utils/country_tra
CurrPorts	Displays the list of all currently opened TCP/UDP ports on your computer.	2.65	4/23/2021 5:35:00 AM	https://www.nirsoft.net/utils/cports.htm
DNSLookupView	DNS Lookup Viewer for Windows 10	1.01	9/3/2021 6:34:12 AM	https://www.nirsoft.net/utils/dns_lookup
DNSQuerySniffer	Network sniffer utility that shows the DNS queries sent on your system.	1.85	7/22/2021 6:00:50 AM	https://www.nirsoft.net/utils/dns_query
IPNeighborsView	View the IP neighbor table on Windows 10/8/7/Vista	1.00	10/5/2021 7:54:52 AM	https://www.nirsoft.net/utils/ip_neighbo

- Don't sleep on the nirsoft tools suite.
- choco install nirlauncher
- Don't forget Defender will go crazy on the password recovery tools

One off - Sysmon + FullEventLogView



Event Time	Record ID	Event ID	Level	Channel	Provider	Description	Opcode	Task	Keywords
1/7/2022 8:03:44 AM.205	325366	5	Information	Microsoft-Windows-Sysmon/...	Microsoft-Windows-Sysmon	Process terminated: RuleName: - UtcTime: 2...		Process terminated (rule: ...	0x80000000000...
1/7/2022 8:03:44 AM.211	325367	5	Information					Process terminated (rule: ...	0x80000000000...
1/7/2022 8:03:47 AM.952	325368	1	Information					Process Create (rule: Proc...	0x80000000000...
1/7/2022 8:03:48 AM.454	325369	5	Information					Process terminated (rule: ...	0x80000000000...
1/7/2022 8:04:00 AM.093	325370	1	Information					Process Create (rule: Proc...	0x80000000000...
1/7/2022 8:04:00 AM.599	325371	5	Information					Process terminated (rule: ...	0x80000000000...
1/7/2022 8:04:02 AM.354	325372	1	Information					Process Create (rule: Proc...	0x80000000000...
1/7/2022 8:04:02 AM.502	325373	5	Information					Process terminated (rule: ...	0x80000000000...
1/7/2022 8:04:03 AM.570	325374	1	Information					Process Create (rule: Proc...	0x80000000000...
1/7/2022 8:04:04 AM.025	325375	5	Information					Process terminated (rule: ...	0x80000000000...
1/7/2022 8:04:09 AM.362	325376	1	Information					Process Create (rule: Proc...	0x80000000000...
1/7/2022 8:04:09 AM.839	325377	5	Information					Process terminated (rule: ...	0x80000000000...
1/7/2022 8:04:10 AM.610	325378	1	Information					Process Create (rule: Proc...	0x80000000000...
1/7/2022 8:04:11 AM.119	325379	5	Information					Process terminated (rule: ...	0x80000000000...
1/7/2022 8:04:11 AM.209	325380	1	Information					Process Create (rule: Proc...	0x80000000000...

```
Process terminated:
RuleName: -
UtcTime: 2022-01-07 08:03:44.195
ProcessGuid: {7B148BEA-F389-61D7-4268-020000001300}
ProcessId: 5964
Image: C:\Windows\System32\wbem\WmiPrvSE.exe
User: NT AUTHORITY\SYSTEM
```

Advanced Options

Event Levels
☑ Critical ☑ Error ☑ Warning ☑ Information ☑ Verbose ☑ Undefined

Show only events from the last... 2 Days

From: 1/ 1/2022 4:18:06 PM To: 1/ 8/2022 4:18:06 PM

Show all event IDs

Show only the specified providers (comma-delimited list, wildcard allowed)

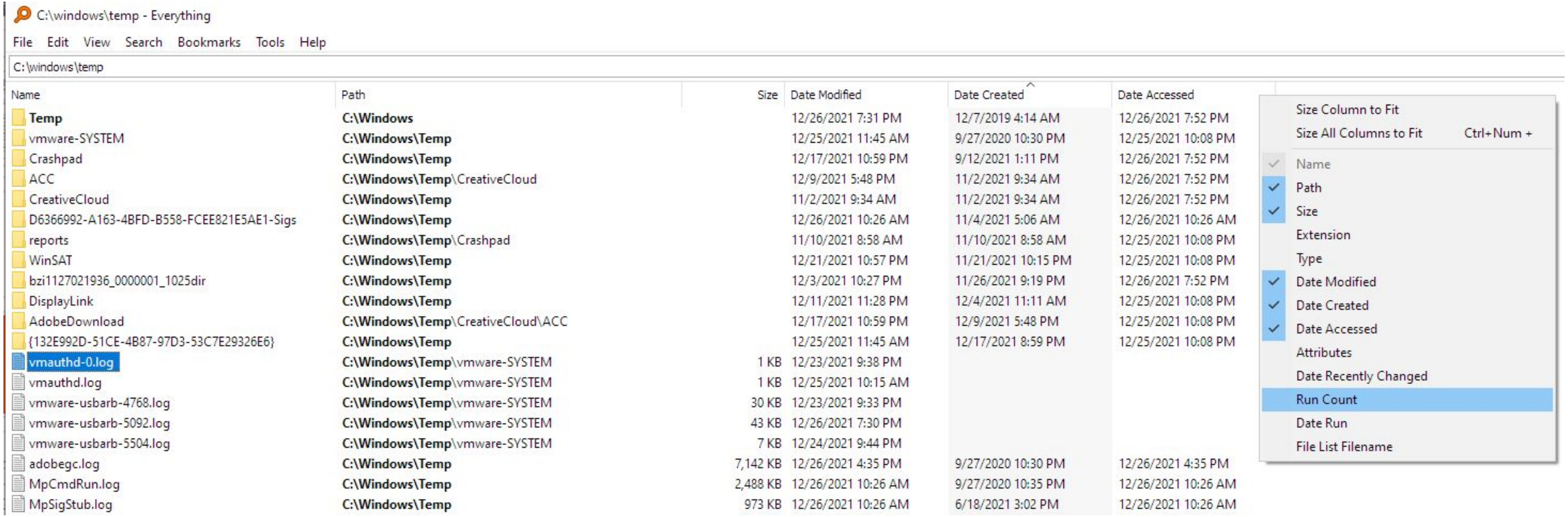
Sysmon

Show all channels

Show all events with any event description string | Search in full description string (S

- Event Viewer makes me hate myself.
- Sysmon + FullEventLogView allows you to spotcheck IOCs on a specific host, then do some quick timeline analysis (event directly before and after) you can get a quick picture
- Just make sure to filter by something its slow - Options - Advanced Options.

One off - Everything



C:\windows\temp

Name	Path	Size	Date Modified	Date Created	Date Accessed
Temp	C:\Windows		12/26/2021 7:31 PM	12/7/2019 4:14 AM	12/26/2021 7:52 PM
vmware-SYSTEM	C:\Windows\Temp		12/25/2021 11:45 AM	9/27/2020 10:30 PM	12/25/2021 10:08 PM
Crashpad	C:\Windows\Temp		12/17/2021 10:59 PM	9/12/2021 1:11 PM	12/26/2021 7:52 PM
ACC	C:\Windows\Temp\CreativeCloud		12/9/2021 5:48 PM	11/2/2021 9:34 AM	12/26/2021 7:52 PM
CreativeCloud	C:\Windows\Temp		11/2/2021 9:34 AM	11/2/2021 9:34 AM	12/26/2021 7:52 PM
D6366992-A163-4BFD-B558-FCEE821E5AE1-Sigs	C:\Windows\Temp		12/26/2021 10:26 AM	11/4/2021 5:06 AM	12/26/2021 10:26 AM
reports	C:\Windows\Temp\Crashpad		11/10/2021 8:58 AM	11/10/2021 8:58 AM	12/25/2021 10:08 PM
WinSAT	C:\Windows\Temp		12/21/2021 10:57 PM	11/21/2021 10:15 PM	12/25/2021 10:08 PM
bzi1127021936_0000001_1025dir	C:\Windows\Temp		12/3/2021 10:27 PM	11/26/2021 9:19 PM	12/26/2021 7:52 PM
DisplayLink	C:\Windows\Temp		12/11/2021 11:28 PM	12/4/2021 11:11 AM	12/25/2021 10:08 PM
AdobeDownload	C:\Windows\Temp\CreativeCloud\ACC		12/17/2021 10:59 PM	12/9/2021 5:48 PM	12/25/2021 10:08 PM
{132E992D-51CE-4B87-97D3-53C7E29326E6}	C:\Windows\Temp		12/25/2021 11:45 AM	12/17/2021 8:59 PM	12/25/2021 10:08 PM
vmauthd-0.log	C:\Windows\Temp\vmware-SYSTEM	1 KB	12/23/2021 9:38 PM		
vmauthd.log	C:\Windows\Temp\vmware-SYSTEM	1 KB	12/25/2021 10:15 AM		
vmware-usbarb-4768.log	C:\Windows\Temp\vmware-SYSTEM	30 KB	12/23/2021 9:33 PM		
vmware-usbarb-5092.log	C:\Windows\Temp\vmware-SYSTEM	43 KB	12/26/2021 7:30 PM		
vmware-usbarb-5504.log	C:\Windows\Temp\vmware-SYSTEM	7 KB	12/24/2021 9:44 PM		
adobegc.log	C:\Windows\Temp	7,142 KB	12/26/2021 4:35 PM	9/27/2020 10:30 PM	12/26/2021 4:35 PM
MpCmdRun.log	C:\Windows\Temp	2,488 KB	12/26/2021 10:26 AM	9/27/2020 10:35 PM	12/26/2021 10:26 AM
MpSigStub.log	C:\Windows\Temp	973 KB	12/26/2021 10:26 AM	6/18/2021 3:02 PM	12/26/2021 10:26 AM

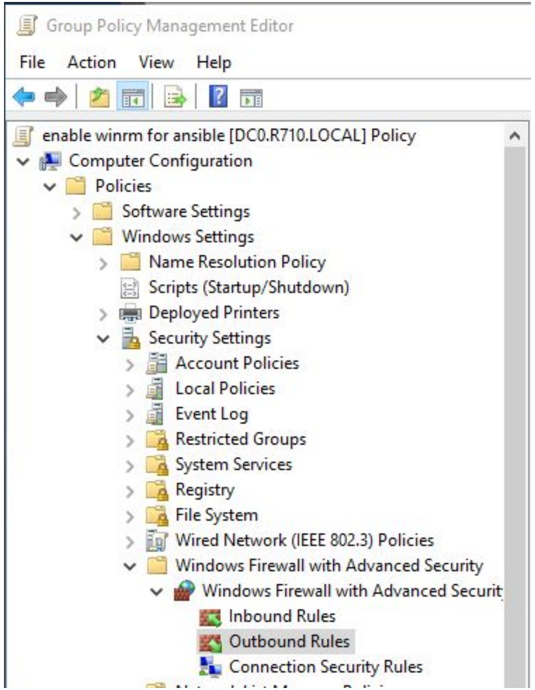
- choco install everything
- https://www.voidtools.com/
- Looks like Standard Information Timestamps but still lit. Most filesystem searching

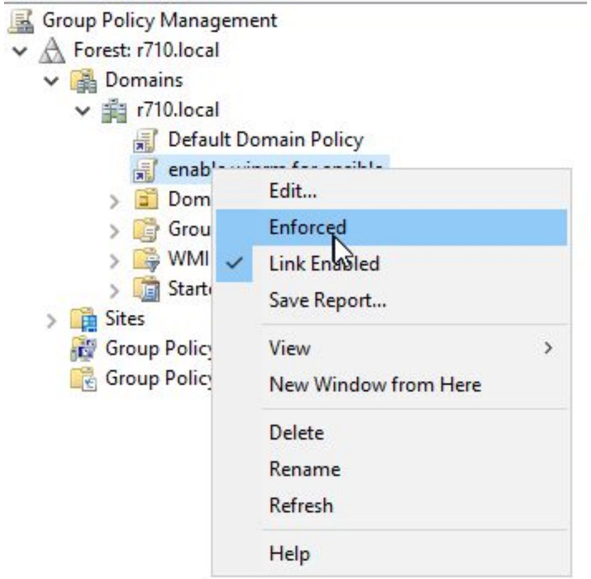
One off - Firewall Config with GPO

- Dont forget about doing bulk firewall rules with GPO!
- And dont forget you can enforce a GPO to override local settings.

CC -> Windows Setting -> Security Settings -> Windows Defender Firewall -> Windows Defender Firewall

Block Out TCP
notepad.exe
regsvr32.exe
calc.exe
mshta.exe
wscript.exe
cscript.exe
runscripthelper.exe



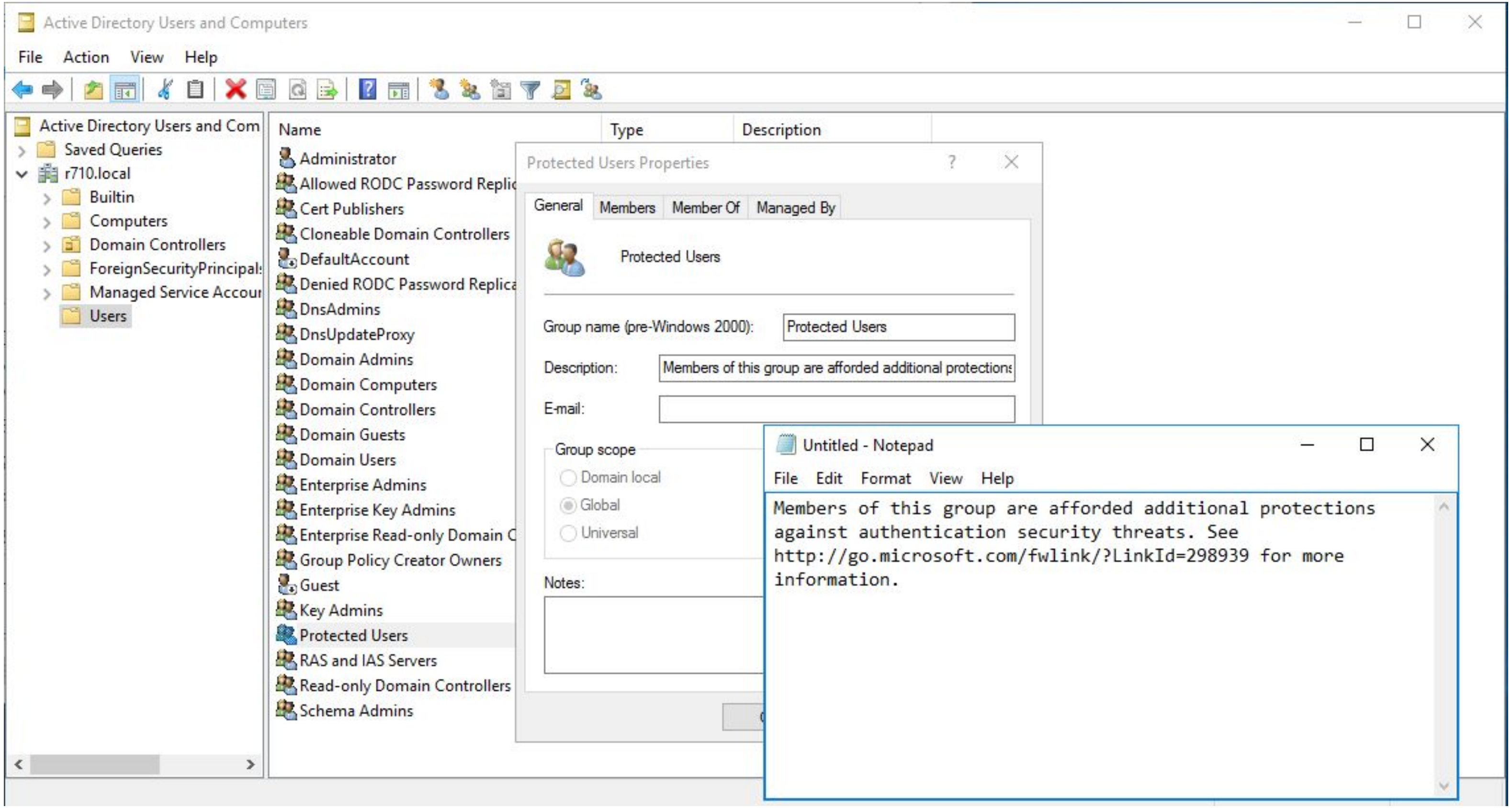


One off - Protect your Credentials

Action	Logon Type	Creds on Target?	Mitigation
Console Login	2	Y*	Unless Credential Guard is enabled
RunAs	2	Y*	Unless Credential Guard is enabled
Remote Desktop	10	Y*	Unless Remote Cred. Guard is enabled
Net Use	3	No	
Powershell remoting	3	No	
PsExec alternate creds	3 + 2	Yes	
Psexec w/o explicit creds	3	No	
Remote Scheduled Task	4	Yes	
Run as a service	5	Yes	
Remote Registry	3	No	

https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group

One off - Protected Users Security Group



Group name (pre-Windows 2000): Protected Users

Description: Members of this group are afforded additional protections

E-mail:

Group scope

○ Domain local

● Global

○ Universal

Notes:

```
Members of this group are afforded additional protections
against authentication security threats. See
http://go.microsoft.com/fwlink/?LinkId=298939 for more
information.
```

- Protected Users group - EZ mode protection from creds/tokens/hashes from being everywhere
- Use with caution, if you do not know the impact you can accidentally lock yourself out

One Off - Powershell Downgrade Attacks

- With the release of Powershell v5, v2 is unnecessary and dangerous
  - Wouldn’t be surprised if this is an inject since it is a popular way to bypass threat hunters
- Couldn’t find GPO method but here’s how to disable it with PS: https://superuser.com/questions/1690388/disable-powershell-v2-via-gpo

One off - Floss & Stringsifter

- Floss is Mandiant's enhanced strings
  - Able to decode strings such as base64 automatically (might have issues with larger samples, use -- nodecoded-strings if you run into an error like this)
  - Installation: choco install floss
  - Usage: floss.exe <filepath> > strings.txt
  - Tooltip: use grep on the output with a regex for IP addresses and URLs to search for NBIs
- Stringsifter is Mandiant's method of sorting strings based on perceived relevance: GitHub - mandiant/stringsifter
  - Takes input from stdin (command line)
  - Install with pip. NOTE: I was having difficulty installing it, stringsifter may not work for you
  - Installs flarestrings (lesser version of floss) and rank_strings
  - Usage: floss.exe -q <filepath> | rank_strings **OR** flarestrings <filepath> | rank_strings
- Use this to add more detail to your IR reports and get additional NBIs/HBIs

One off - How to Write an IR Event Summary

Bad -

- At 5pm we had a bunch of bananas start appearing on the machine.
- Here is photo of bananas.
- Pls help.

Include - Executive Summary, Remediation Actions Taken, Earliest evidence, Timeline of evidence, Host Based Indicators (MD5s, filenames), Network Indicators (FQDN / IPS), compromised accounts.

Doesnt need to be fancy. Content matters.

Better -

Executive Summary: At 5pm ET on Jan 6, 2022 the internal security team noticed attacker activity on host DC-1. The internal team is continuing to investigate the root cause of the incident, below are details.

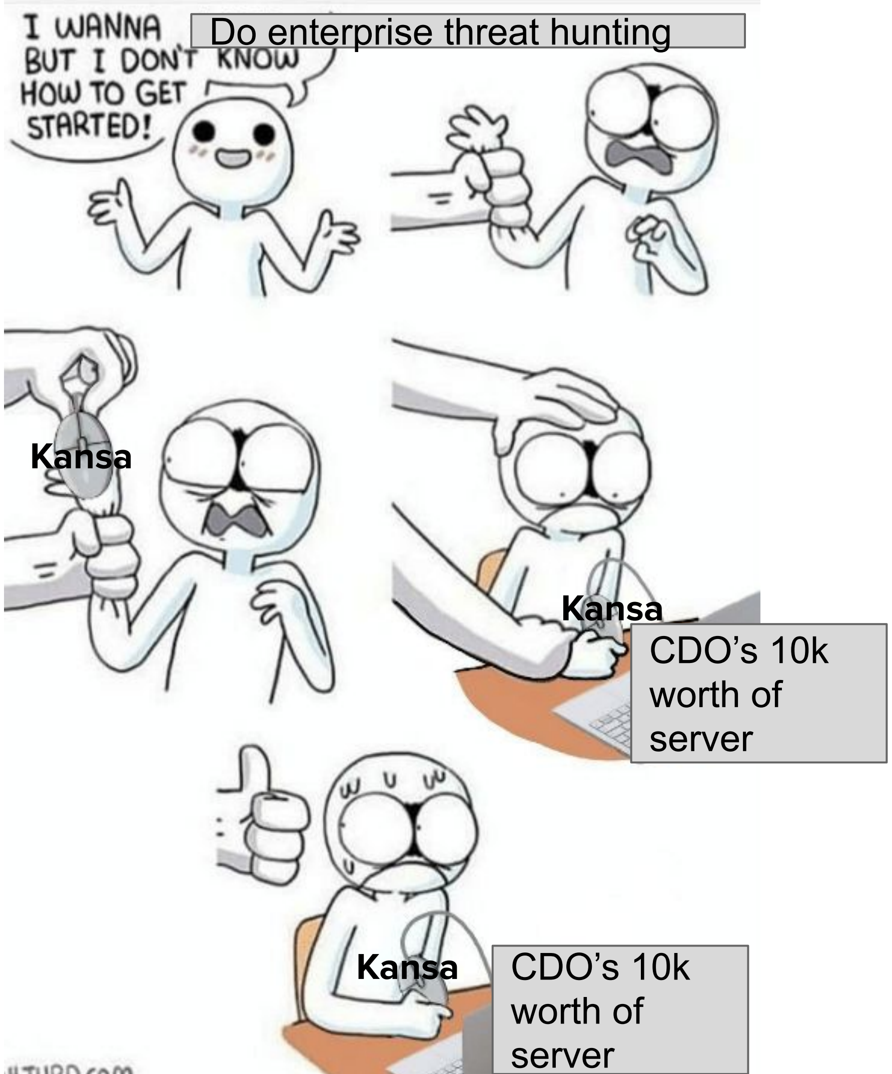
Earliest Evidence: 2022-01-06 10:00:00 UTC - File time Stamp of Bananas.exe

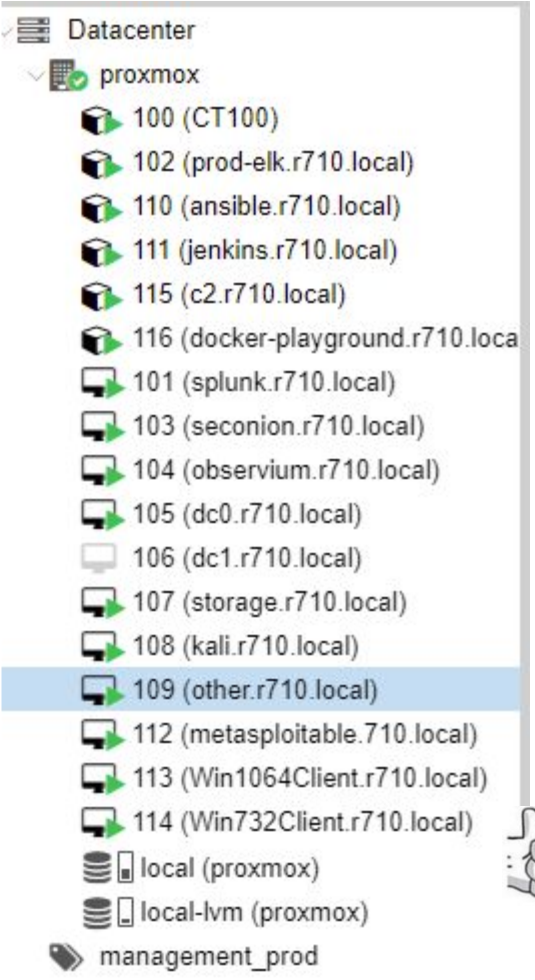
HBIs:

C:\Users\Username\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\bananas.exe

afd6528b1ed8af8bdf7116f26dab69a1 (bananas.exe)

NBIs:

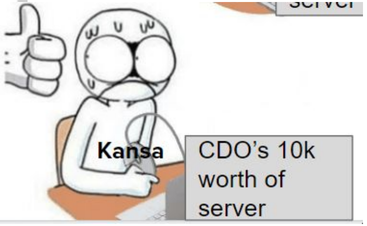

I WANNA
Do enterprise threat hunting
BUT I DON'T KNOW HOW TO GET STARTED!
Kansa
Kansa
CDO's 10k worth of server
Kansa
CDO's 10k worth of server



Datacenter
proxmox
100 (CT100)
102 (prod-elk.r710.local)
110 (ansible.r710.local)
111 (jenkins.r710.local)
115 (c2.r710.local)
116 (docker-playground.r710.loca
101 (splunk.r710.local)
103 (seconion.r710.local)
104 (observium.r710.local)
105 (dc0.r710.local)
106 (dc1.r710.local)
107 (storage.r710.local)
108 (kali.r710.local)
109 (other.r710.local)
112 (metasploitable.710.local)
113 (Win1064Client.r710.local)
114 (Win732Client.r710.local)
local (proxmox)
local-lvm (proxmox)
management_prod

This is overkill. You can practice threat hunting with even less.

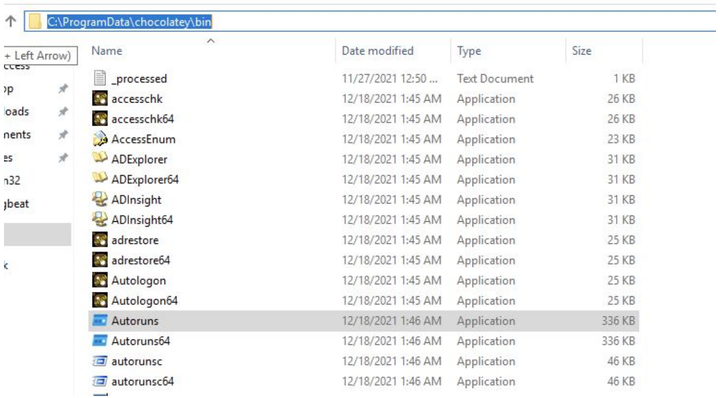
1. Set up a Kali Machine and get some beacon working. PoshC2, meterpreter, MerlinC2, anything.
2. Have the beacons persist in random ways on random hosts. EX mode - [GitHub - mandiant/SharPersist]
3. Purple team this. Have the blue team try to find all the hosts.
    - Practice blind searching - Use Kansa to find live processes and persistence with autoruns. Stack the data see what you can find.
    - Practice hunting with Limited knowledge - Gather all the filenames, IPs, hashes, and IOCs - search in Sysmon event logs.
    - Practice Remediation - Practice blocking IPs on all hosts and firewall. Remove the persistence mechanisms.
    - Practice Reporting - how can I communicate these IOCs to the white team?
        - Easy question - If I were given your report, could I search for this activity on my network?
            - Oh I got some bananas on my screen? No.
            - I have bananas.exe (MD5 Here) in C:\windows\temp. Yes.



Kansa Appendix

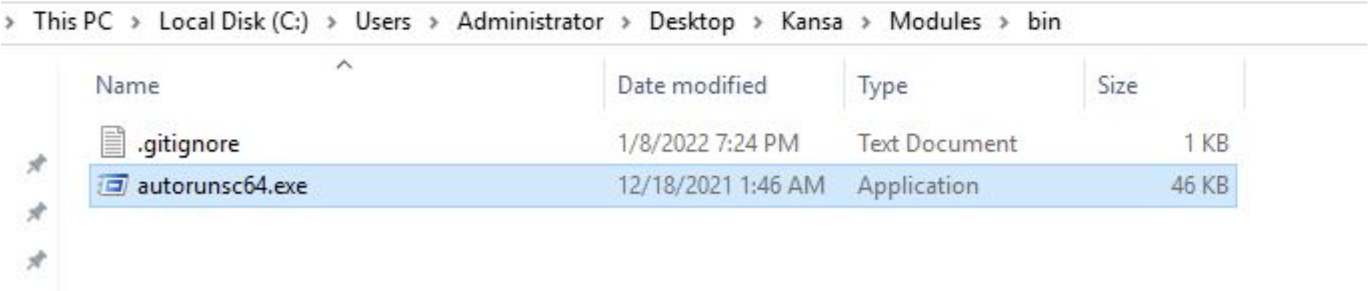
System Prerequisite

- Chocolatey
- Choco install sysinternals git everything -y
- Clone the [Kansa repo]
- Get Autorunsc64.exe and move to Kansa/Modules/Bin
- Get [LogParser.exe]



C:\ProgramData\chocolatey\bin

Name	Date modified	Type	Size
_processed	11/27/2021 12:50 ...	Text Document	1 KB
accesschk	12/18/2021 1:45 AM	Application	26 KB
accesschk64	12/18/2021 1:45 AM	Application	26 KB
AccessEnum	12/18/2021 1:45 AM	Application	23 KB
ADExplorer	12/18/2021 1:45 AM	Application	31 KB
ADExplorer64	12/18/2021 1:45 AM	Application	31 KB
ADInsight	12/18/2021 1:45 AM	Application	31 KB
ADInsight64	12/18/2021 1:45 AM	Application	31 KB
adrestore	12/18/2021 1:45 AM	Application	25 KB
adrestore64	12/18/2021 1:45 AM	Application	25 KB
Autologon	12/18/2021 1:45 AM	Application	25 KB
Autologon64	12/18/2021 1:45 AM	Application	25 KB
Autoruns	12/18/2021 1:46 AM	Application	336 KB
Autoruns64	12/18/2021 1:46 AM	Application	336 KB
autorunsc	12/18/2021 1:46 AM	Application	46 KB
autorunsc64	12/18/2021 1:46 AM	Application	46 KB

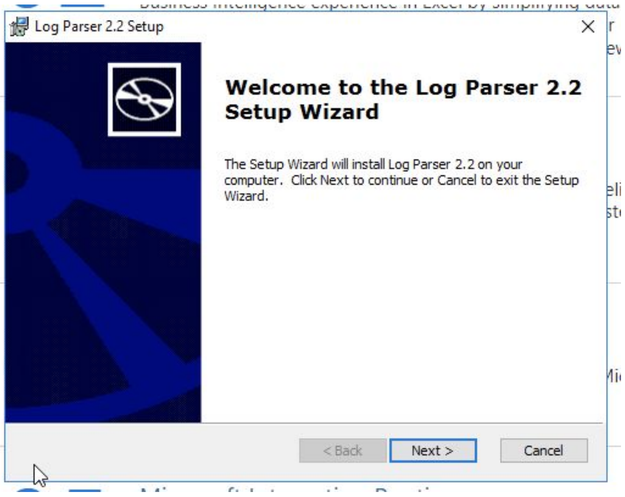


› This PC › Local Disk (C:) › Users › Administrator › Desktop › Kansa › Modules › bin

Name	Date modified	Type	Size
.gitignore	1/8/2022 7:24 PM	Text Document	1 KB
autorunsc64.exe	12/18/2021 1:46 AM	Application	46 KB

System Prerequisite - PT2

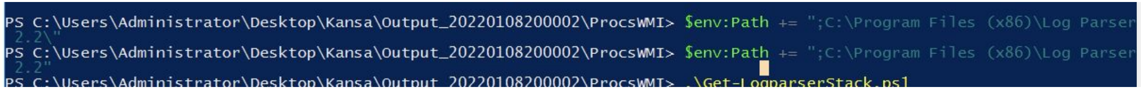
- Get LogParser.exe into the system environment vars
- $env:Path += “;<path>”



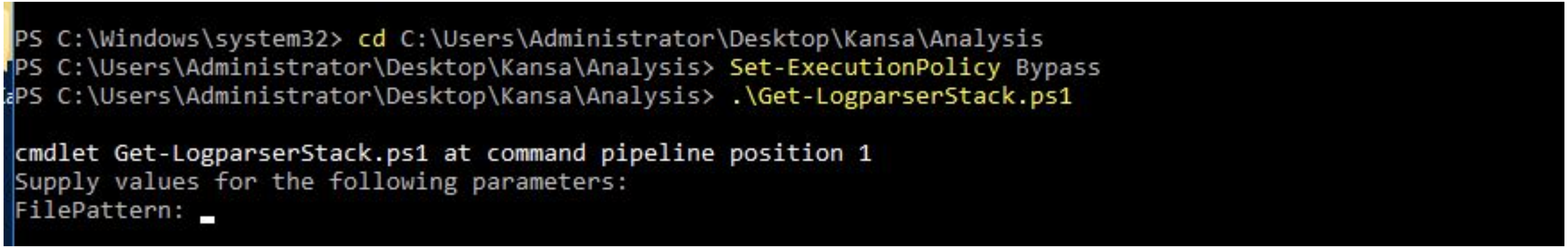
Log Parser 2.2 Setup

Welcome to the Log Parser 2.2 Setup Wizard

The Setup Wizard will install Log Parser 2.2 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.



```
PS C:\Users\Administrator\Desktop\Kansa\Output_20220108200002\ProcsWMI> $env:Path += ";C:\Program Files (x86)\Log Parser
 2.2\"
PS C:\Users\Administrator\Desktop\Kansa\Output_20220108200002\ProcsWMI> $env:Path += ";C:\Program Files (x86)\Log Parser
 2.2"
PS C:\Users\Administrator\Desktop\Kansa\Output_20220108200002\ProcsWMI> .\Get-LogparserStack.ps1
```

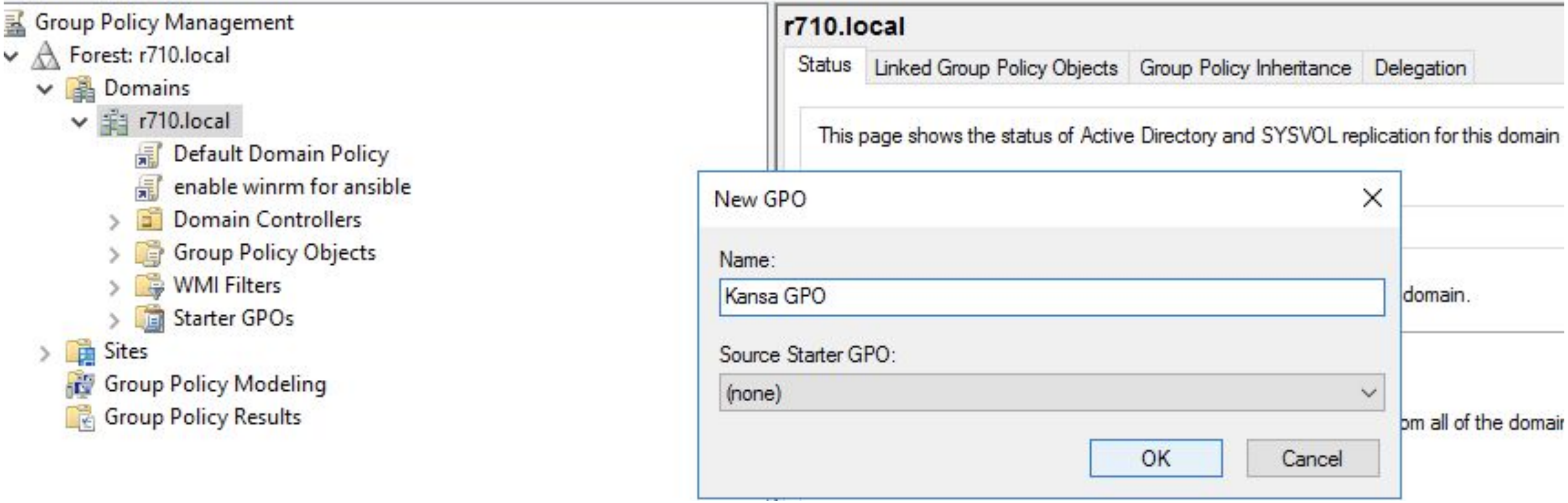


```
PS C:\Windows\system32> cd C:\Users\Administrator\Desktop\Kansa\Analysis
PS C:\Users\Administrator\Desktop\Kansa\Analysis> Set-ExecutionPolicy Bypass
PS C:\Users\Administrator\Desktop\Kansa\Analysis> .\Get-LogparserStack.ps1

cmdlet Get-LogparserStack.ps1 at command pipeline position 1
Supply values for the following parameters:
FilePattern: _
```

GPO to Allow WinRM

- Enable WinRM via GPO - [PowerShell Remoting and Incident Response - Matt's DFIR Blog]



This page shows the status of Active Directory and SYSVOL replication for this domain

domain.

om all of the domain

Name: Kansa GPO

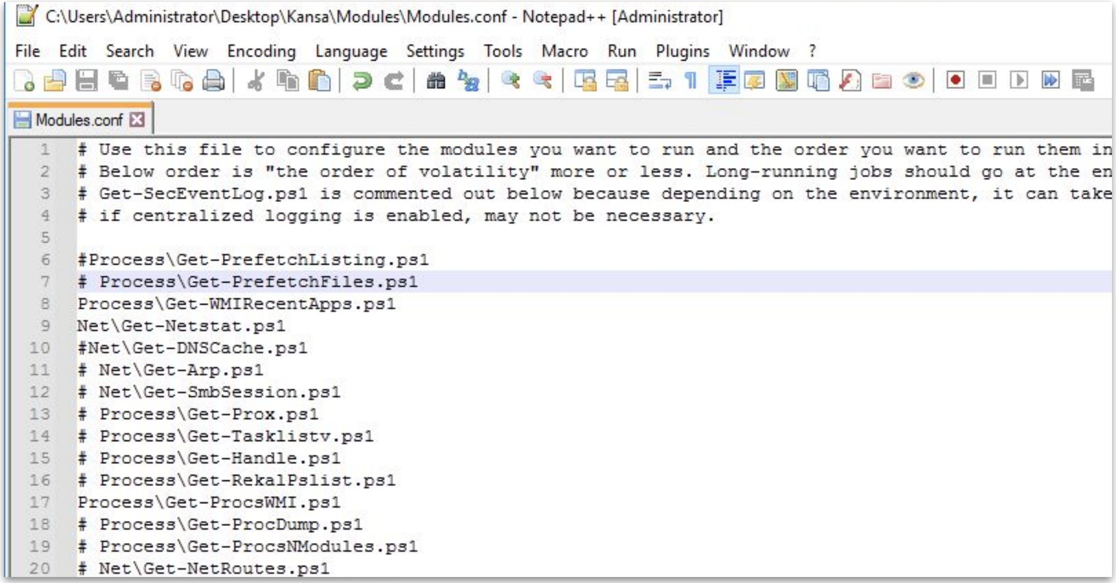
Source Starter GPO: (none)

Run Kansa

Edit the Modules/Modules.conf to contain modules you want to run

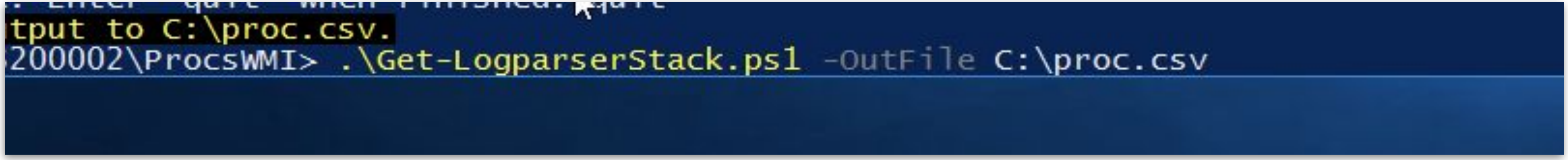
.\kansa.ps1 -PushBin -ModulePath .\Modules -Verbose

Stack the results!


C:\Users\Administrator\Desktop\Kansa\Modules\Modules.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Modules.conf

```
# Use this file to configure the modules you want to run and the order you want to run them in
# Below order is "the order of volatility" more or less. Long-running jobs should go at the en
# Get-SecEventLog.ps1 is commented out below because depending on the environment, it can take
# if centralized logging is enabled, may not be necessary.

#Process\Get-PrefetchListing.ps1
# Process\Get-PrefetchFiles.ps1
Process\Get-WMIRecentApps.ps1
Net\Get-Netstat.ps1
#Net\Get-DNSCache.ps1
# Net\Get-Arp.ps1
# Net\Get-SmbSession.ps1
# Process\Get-Prox.ps1
# Process\Get-Tasklistv.ps1
# Process\Get-Handle.ps1
# Process\Get-RekalPslist.ps1
Process\Get-ProcsWMI.ps1
# Process\Get-ProcDump.ps1
# Process\Get-ProcsNModules.ps1
# Net\Get-NetRoutes.ps1
```



```
: Enter  quit  when finished: quit
tput to C:\proc.csv.
200002\ProcsWMI> .\Get-LogparserStack.ps1 -OutFile C:\proc.csv
```