

Windows Threat Hunting

UBNetDef, Spring 2024
Week 6

Presenter:
Anthony Magrene

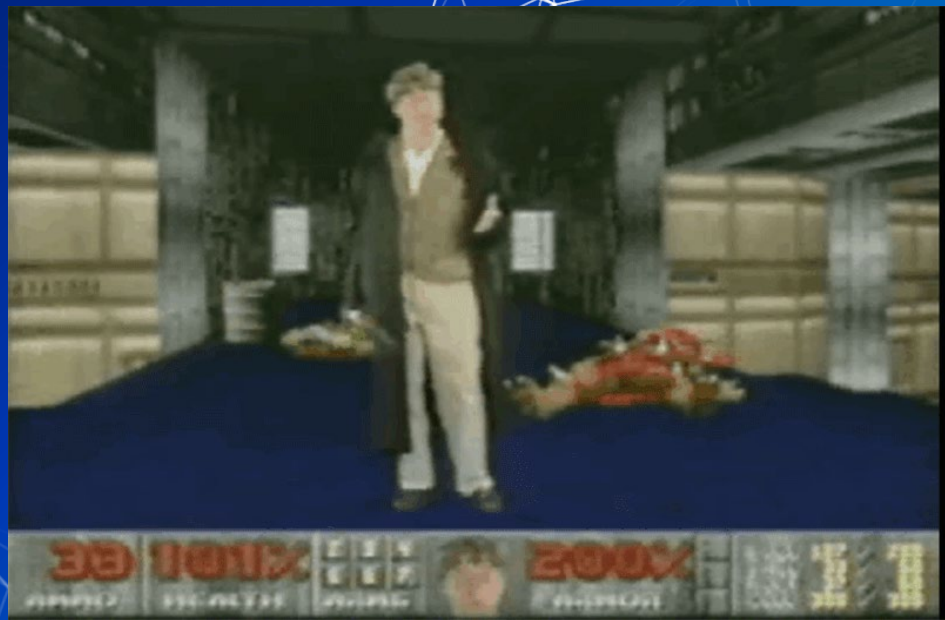
Microsoft®

Windows®

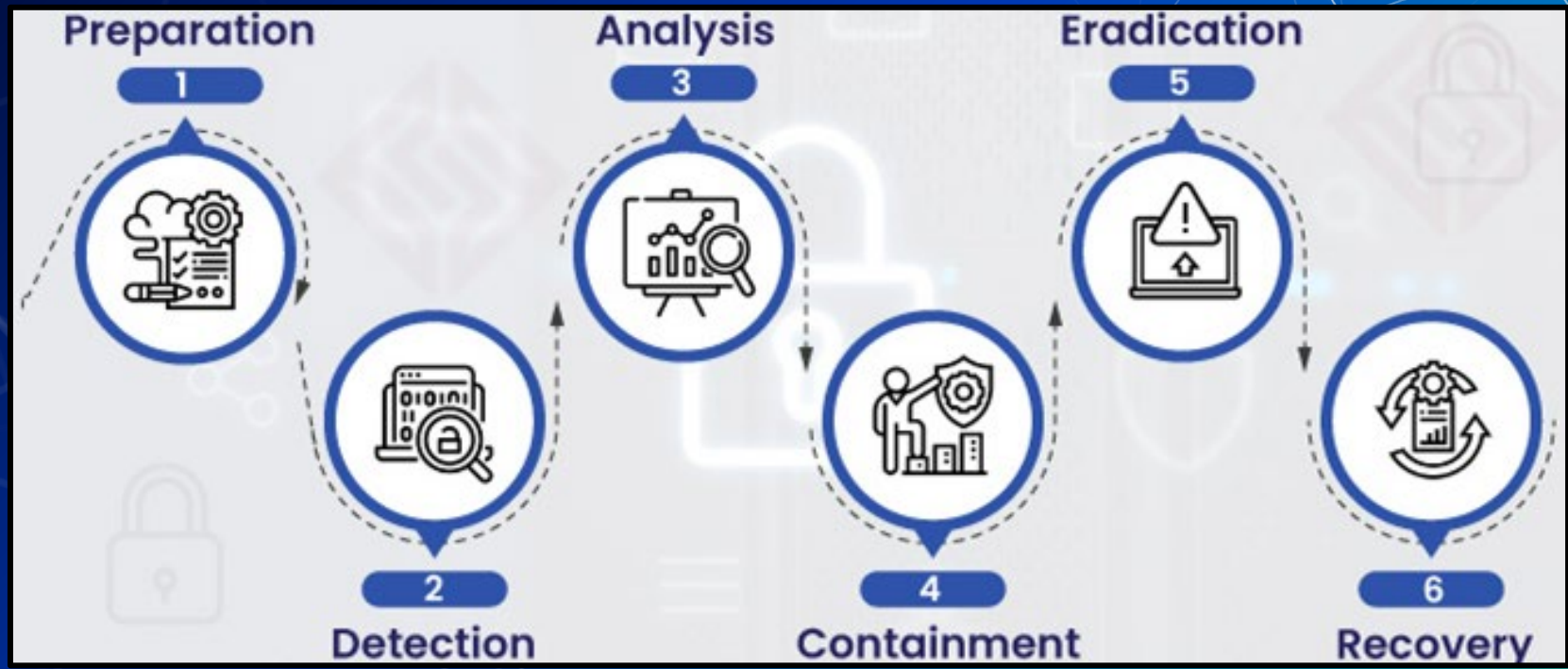


Agenda – Week 6

- Incident Response (IR) High Level
- Windows Concepts
- Network Forensics
- PowerShell for IR
- Hands-on Activity 1-2
- Windows Management Instrumentation (WMI) & Services
- Hands-on Activity 3
- Persistence
- Hands-on Activity 4



Incident Response



Windows Concepts

Notable File Types

Dynamic Link Library (.dll)

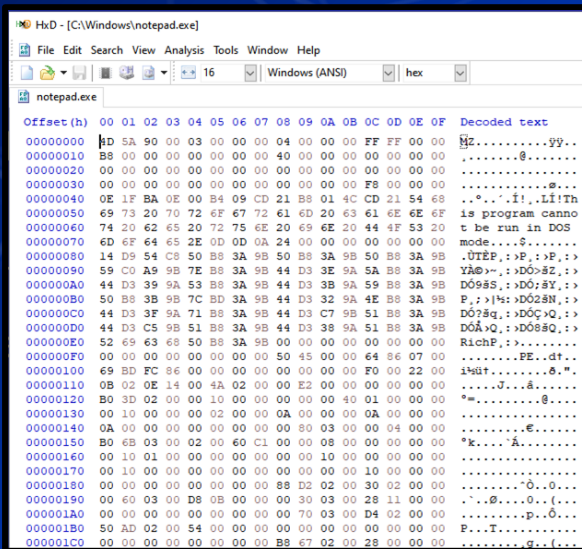
- Windows implementation of shared libraries
- Prevents redundant storage commonly used code

This PC > Local Disk (C:) > Windows > System32 >

Name	Date modified	Type	Size
aaauthhelper.dll	12/11/2020 6:13 PM	Application exten...	449 KB
aadcloudap.dll	12/11/2020 6:13 PM	Application exten...	970 KB
aadjcsp.dll	3/12/2021 10:15 PM	Application exten...	101 KB
aadtb.dll	1/12/2021 1:43 PM	Application exten...	1,383 KB
aadWamExtension.dll	1/12/2021 1:43 PM	Application exten...	150 KB
AarSvc.dll	3/12/2021 10:15 PM	Application exten...	434 KB
AboutSettingsHandlers.dll	1/12/2021 1:43 PM	Application exten...	431 KB
AboveLockAppHost.dll	3/12/2021 10:15 PM	Application exten...	410 KB
accessibilitycpl.dll	2/11/2021 3:15 PM	Application exten...	275 KB
accountaccessor.dll	1/12/2021 1:44 PM	Application exten...	268 KB
AccountsRt.dll	1/12/2021 1:44 PM	Application exten...	426 KB
AcGenral.dll	10/23/2020 3:20 PM	Application exten...	362 KB
AcLayers.dll	12/11/2020 6:14 PM	Application exten...	319 KB
acledit.dll	12/7/2019 4:09 AM	Application exten...	11 KB
aclui.dll	12/7/2019 4:09 AM	Application exten...	574 KB
acmigration.dll	3/12/2021 10:15 PM	Application exten...	381 KB
ACPBackgroundManagerPolicy.dll	1/12/2021 1:43 PM	Application exten...	191 KB
acppage.dll	1/12/2021 1:43 PM	Application exten...	87 KB
acprox.dll	12/7/2019 4:09 AM	Application exten...	13 KB

Portable Executable (.exe)

- Machine code that is executed by the operating system
- May be written using high-level languages
 - GO, C++, C, Ruby etc.

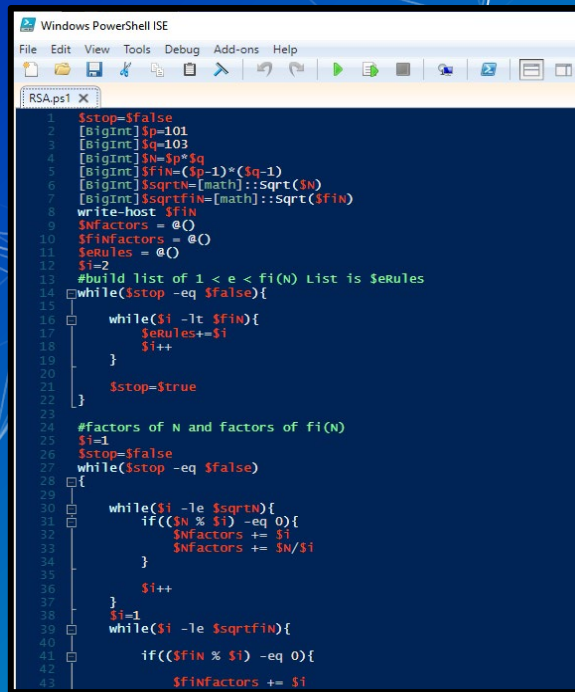


```
HxD - [C:\Windows\notepad.exe]
File Edit Search View Analysis Tools Window Help
16 Windows (ANSI) hex
notepad.exe
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....yy..
00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000030 00 00 00 00 00 00 00 00 00 00 00 00 F8 00 00 00 .....8.....
00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 .....!.!..LifTh
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F ..is program canno
00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 ..t be run in DOS
00000070 6D 6F 64 65 2E 0D 0A 24 00 00 00 00 00 00 00 00 ..mode...$.
00000080 14 D9 54 C8 50 B8 3A 9B 50 B8 3A 9B 50 B8 3A 9B ..ÛTEP...>P...>P...>
00000090 59 C0 A9 9B 7E B8 3A 9B 44 D3 3E 9A 5A B8 3A 9B ..Y&e>...>DÓ&SZ...>
000000A0 44 D3 39 9A 53 B8 3A 9B 44 D3 3B 9A 59 B8 3A 9B ..DÓ&S&...>DÓ&SY...>
000000B0 50 B8 3B 9B 7C BD 3A 9B 44 D3 32 9A 4E B8 3A 9B ..F...>|%>DÓ&2M...>
000000C0 44 D3 3F 9A 71 B8 3A 9B 44 D3 37 9B 51 B8 3A 9B ..DÓ&B&g...>DÓ&Q...>
000000D0 44 D3 C5 9B 51 B8 3A 9B 44 D3 38 9A 51 B8 3A 9B ..DÓ&A...>DÓ&S&Q...>
000000E0 52 69 63 68 50 B8 3A 9B 00 00 00 00 00 00 00 00 ..RichP...>.....
000000F0 00 00 00 00 00 00 00 00 50 45 00 00 64 86 07 00 .....FE...dt.
00000100 69 BD FC 86 00 00 00 00 00 00 00 00 F0 00 22 00 ..i&áit.....&.".
00000110 0B 02 0E 14 00 4A 02 00 00 E2 00 00 00 00 00 00 ..J...&.....
00000120 B0 3D 02 00 00 10 00 00 00 00 00 40 01 00 00 00 ..*=.....&.....
00000130 00 10 00 00 00 02 00 00 0A 00 00 00 0A 00 00 00 .....e.....
00000140 0A 00 00 00 00 00 00 00 00 00 80 03 00 00 04 00 00 .....k.....A.....
00000150 B0 6B 03 00 02 00 60 C1 00 00 08 00 00 00 00 00 ..*k.....A.....
00000160 00 10 01 00 00 00 00 00 00 00 10 00 00 00 00 00 .....
00000170 00 10 00 00 00 00 00 00 00 00 00 00 00 10 00 00 .....
00000180 00 00 00 00 00 00 00 00 88 D2 02 00 30 02 00 00 .....0...0...
00000190 00 60 03 00 D8 0B 00 00 00 30 03 00 28 11 00 00 ..&...0...{...
000001A0 00 00 00 00 00 00 00 00 70 03 00 D4 02 00 00 .....p...0...
000001B0 50 AD 02 00 54 00 00 00 00 00 00 00 00 00 00 00 ..E...T.....
000001C0 00 00 00 00 00 00 00 00 B8 67 02 00 28 00 00 00 .....g...{...
```

geckodriver.exe	10/12/2019 8:38 AM	Application	3,483 KB
-----------------	--------------------	-------------	----------

PowerShell Script (.ps1)

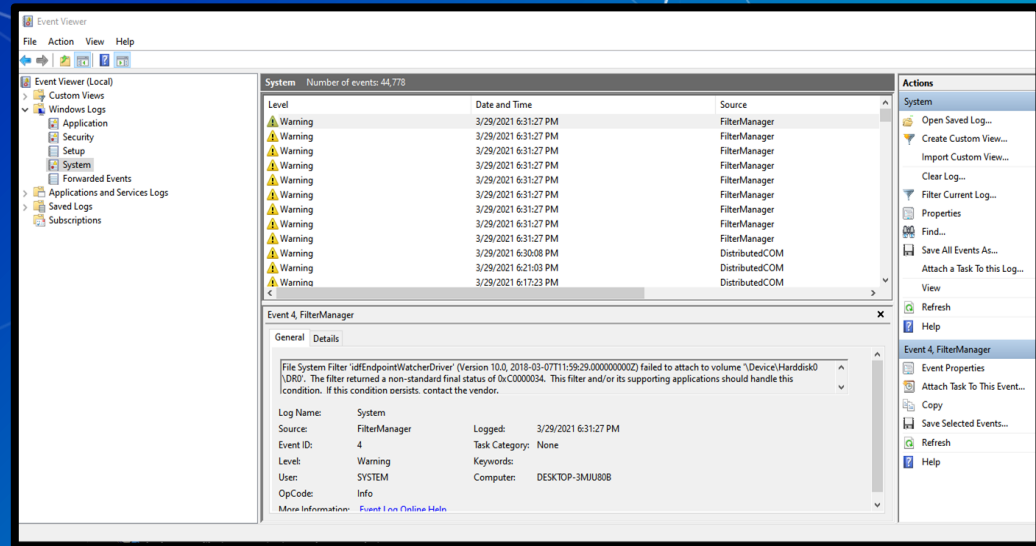
- PowerShell Integrated Scripting Environment (ISE)
- Extensive .NET integration



```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
RSA.ps1 X
1 $stop=$false
2 [bigint]$p=101
3 [bigint]$p=103
4 [bigint]$N=$p*$q
5 [bigint]$fN=(($p-1)*($q-1))
6 [bigint]$sqrtN=[math]::Sqrt($N)
7 [bigint]$sqrtfN=[math]::Sqrt($fN)
8 write-host $fN
9 $Nfactors = @()
10 $fNfactors = @()
11 $eRules = @()
12 $i=2
13 #build list of 1 < e < fi(N) List is $eRules
14 while($stop -eq $false){
15     while($i -lt $fN){
16         $eRules+=$i
17         $i++
18     }
19     $stop=$true
20 }
21
22 #Factors of N and factors of fi(N)
23 $i=1
24 $stop=$false
25 while($stop -eq $false)
26 {
27     while($i -le $sqrtN){
28         if(($N % $i) -eq 0){
29             $Nfactors += $i
30             $Nfactors += $N/$i
31         }
32         $i++
33     }
34     $i=1
35     while($i -le $sqrtfN){
36         if(($fN % $i) -eq 0){
37             $fNfactors += $i
38         }
39     }
40 }
```

Event Log (.evtx)

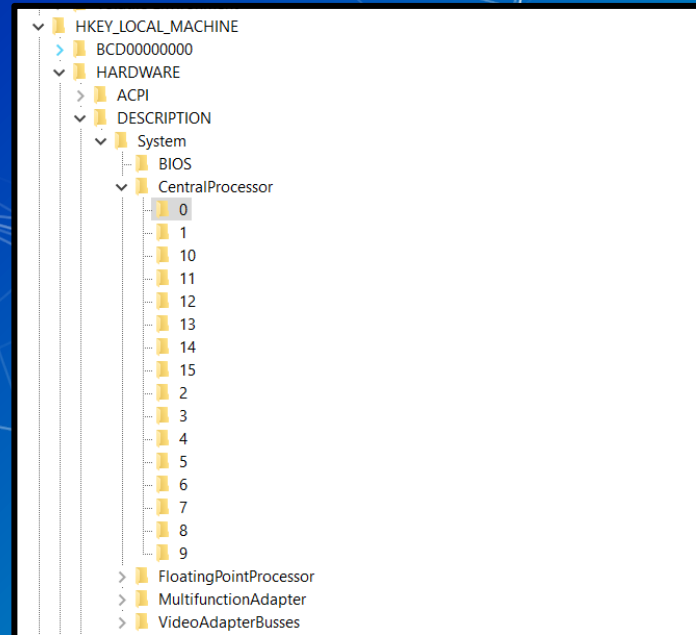
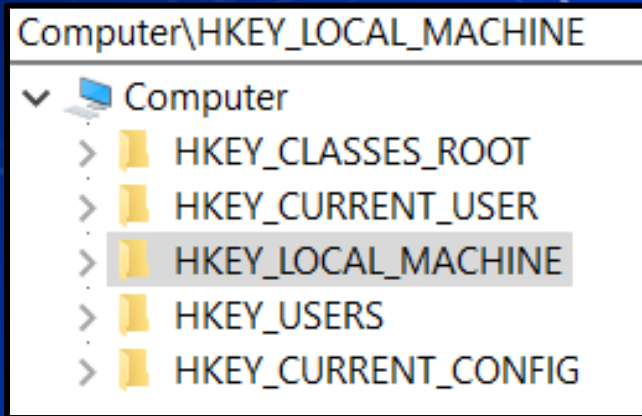
- Stores Windows Logs
- Located `C:\Windows\System32\winevt\Logs\`
- Event viewer used to view logs



The Registry

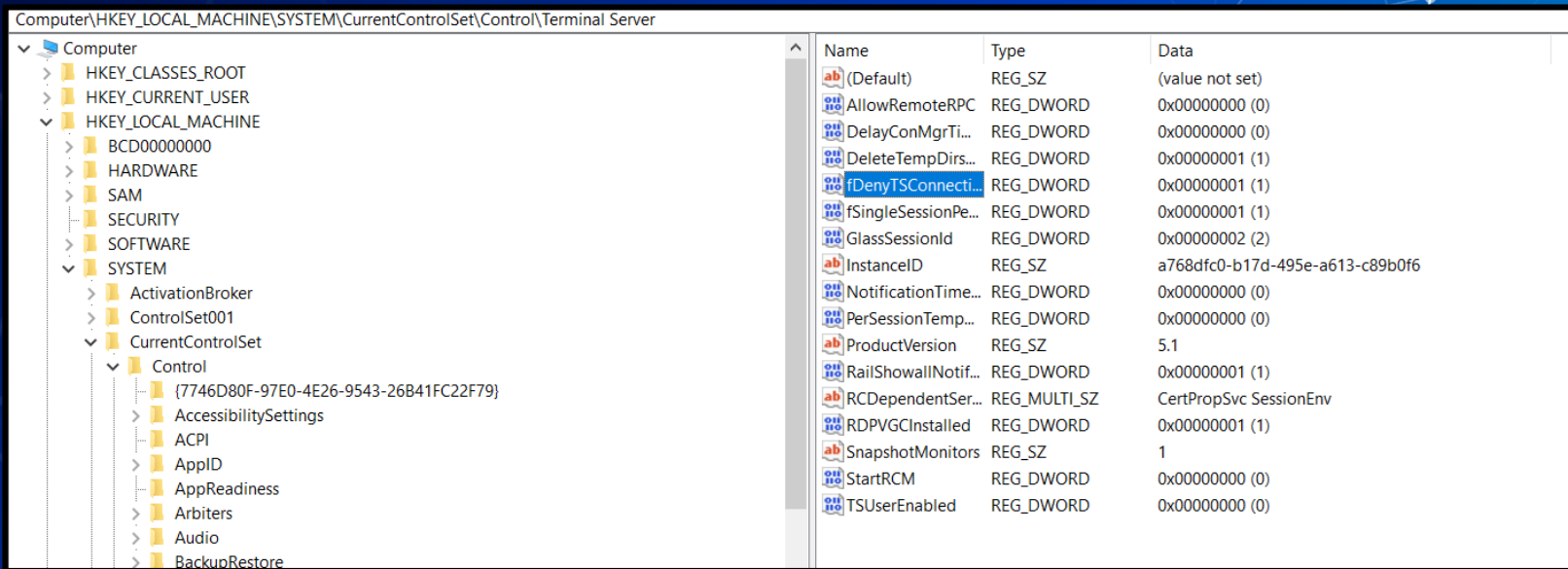
Registry

- Hierarchical database
 - Stores low-level settings



Registry cont.

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server



Name	Type	Data
(Default)	REG_SZ	(value not set)
AllowRemoteRPC	REG_DWORD	0x00000000 (0)
DelayConMgrTi...	REG_DWORD	0x00000000 (0)
DeleteTempDir...	REG_DWORD	0x00000001 (1)
fDenyTSConnecti...	REG_DWORD	0x00000001 (1)
fSingleSessionPe...	REG_DWORD	0x00000001 (1)
GlassSessionId	REG_DWORD	0x00000002 (2)
InstanceID	REG_SZ	a768dfc0-b17d-495e-a613-c89b0f6
NotificationTime...	REG_DWORD	0x00000000 (0)
PerSessionTemp...	REG_DWORD	0x00000000 (0)
ProductVersion	REG_SZ	5.1
RailShowallNotif...	REG_DWORD	0x00000001 (1)
RCDependentSer...	REG_MULTI_SZ	CertPropSvc SessionEnv
RDPVGCInstalled	REG_DWORD	0x00000001 (1)
SnapshotMonitors	REG_SZ	1
StartRCM	REG_DWORD	0x00000000 (0)
TSUserEnabled	REG_DWORD	0x00000000 (0)

Registry cont.

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server

Computer

CurrentControlSet

Control

{7746D80F-97E0-4E26-9543-26B41FC22F79}

AccessibilitySettings

ACPI

AppID

AppReadiness

Arbiters

Edit DWORD (32-bit) Value

Value name:
fDenyTSConnections

Value data:
1

Base
 Hexadecimal
 Decimal

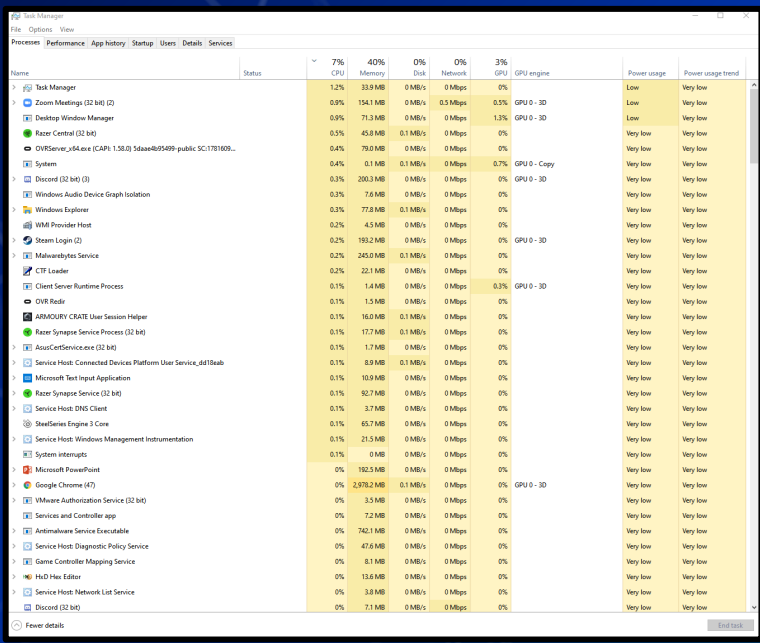
OK Cancel

Name	Type	Data
(Default)	REG_SZ	(value not set)
AllowRemoteRPC	REG_DWORD	0x00000000 (0)
DelayConMgrTi...	REG_DWORD	0x00000000 (0)
DeleteTempDir...	REG_DWORD	0x00000001 (1)
fDenyTSConnect...	REG_DWORD	0x00000001 (1)
fSingleSessionPe...	REG_DWORD	0x00000001 (1)
GlassSessionId	REG_DWORD	0x00000002 (2)
InstanceID	REG_SZ	a768dfc0-b17d-495e-a613-c89b0f6
NotificationTime...	REG_DWORD	0x00000000 (0)
PerSessionTemp...	REG_DWORD	0x00000000 (0)
ProductVersion	REG_SZ	5.1
RailShowallNotif...	REG_DWORD	0x00000001 (1)
RCDependentSer...	REG_MULTI_SZ	CertPropSvc SessionEnv
RDPVGCInstalled	REG_DWORD	0x00000001 (1)
SnapshotMonitors	REG_SZ	1
StartRCM	REG_DWORD	0x00000000 (0)
TSUserEnabled	REG_DWORD	0x00000000 (0)

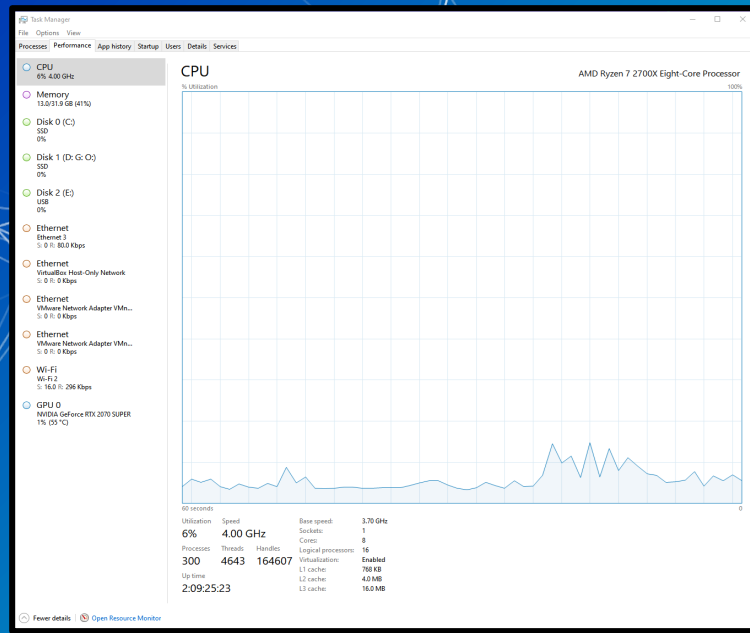
Task Manager

Task Manager

Provides high-level view of what is running

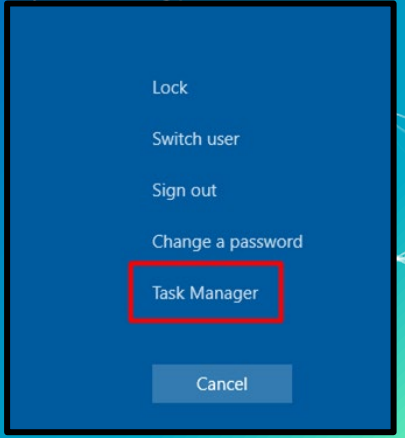
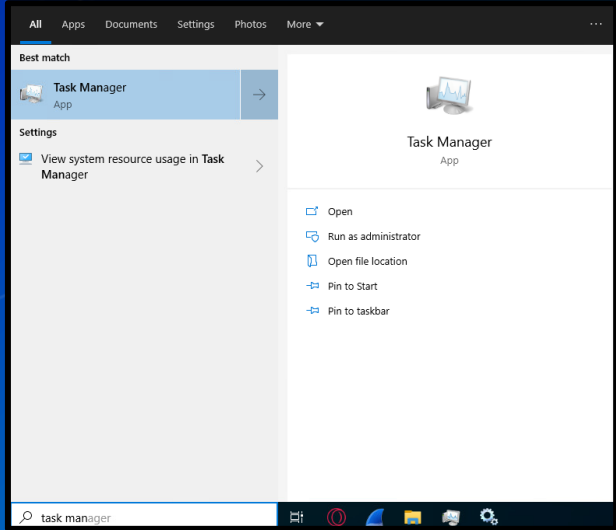
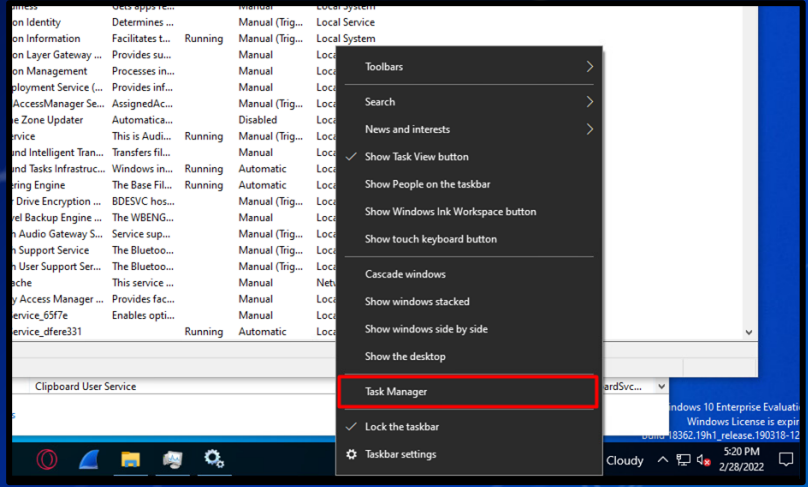


Name	Status	7% CPU	40% Memory	0% Disk	0% Network	3% GPU	GPU engine	Power usage	Power usage trend
Task Manager		1.2%	33.9 MB	0 MB/s	0 Mbps	0%		Low	Very low
Zoom Meetings (32 bit) (2)		0.9%	154.1 MB	0 MB/s	0.5 Mbps	0.5%	GPU 0 - 3D	Low	Very low
Desktop Window Manager		0.9%	71.3 MB	0 MB/s	0 Mbps	1.3%	GPU 0 - 3D	Low	Very low
Razer Central (32 bit)		0.5%	45.8 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
OVIServer_u64.exe (CAPI: 1.58.0) SmaaB09499-public SC1781609...		0.4%	79.0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
System		0.4%	0.1 MB	0.1 MB/s	0 Mbps	0.7%	GPU 0 - Copy	Very low	Very low
Discord (32 bit) (3)		0.3%	200.3 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low	Very low
Windows Audio Device Graph Isolation		0.3%	7.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Windows Explorer		0.3%	77.8 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
WM Provider Host		0.2%	4.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Steam Login (2)		0.2%	193.2 MB	0 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low	Very low
Malwarebytes Service		0.2%	245.0 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
CTF Leader		0.2%	22.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Client Server Runtime Process		0.1%	1.8 MB	0 MB/s	0 Mbps	0.3%	GPU 0 - 3D	Very low	Very low
OVIS-Ruler		0.1%	15.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low
ADBUSDRIVE.exe User Session Helper		0.1%	16.0 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
Razer Synapse Service Process (32 bit)		0.1%	17.7 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
AssocCatService.exe (32 bit)		0.1%	1.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Connected Device Platform User Service_daf8ab		0.1%	8.9 MB	0.1 MB/s	0 Mbps	0%		Very low	Very low
Microsoft Text Input Application		0.1%	10.9 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Razer Synapse Service (32 bit)		0.1%	92.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: DNS Client		0.1%	3.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
SteelSeries Engine 3 Core		0.1%	65.7 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Windows Management Instrumentation		0.1%	21.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low
System interrupts		0.1%	0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Microsoft PowerPoint		0%	192.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Google Chrome (47)		0%	2,978.2 MB	0.1 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low	Very low
VMware Authorization Service (32 bit)		0%	3.5 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Services and Controller app		0%	7.2 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Antimalware Service Executable		0%	742.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Diagnostic Policy Service		0%	47.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Game Controller Mapping Service		0%	8.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low
HxD Hex Editor		0%	13.6 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Service Host: Network List Service		0%	3.8 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Discord (32 bit)		0%	7.1 MB	0 MB/s	0 Mbps	0%		Very low	Very low



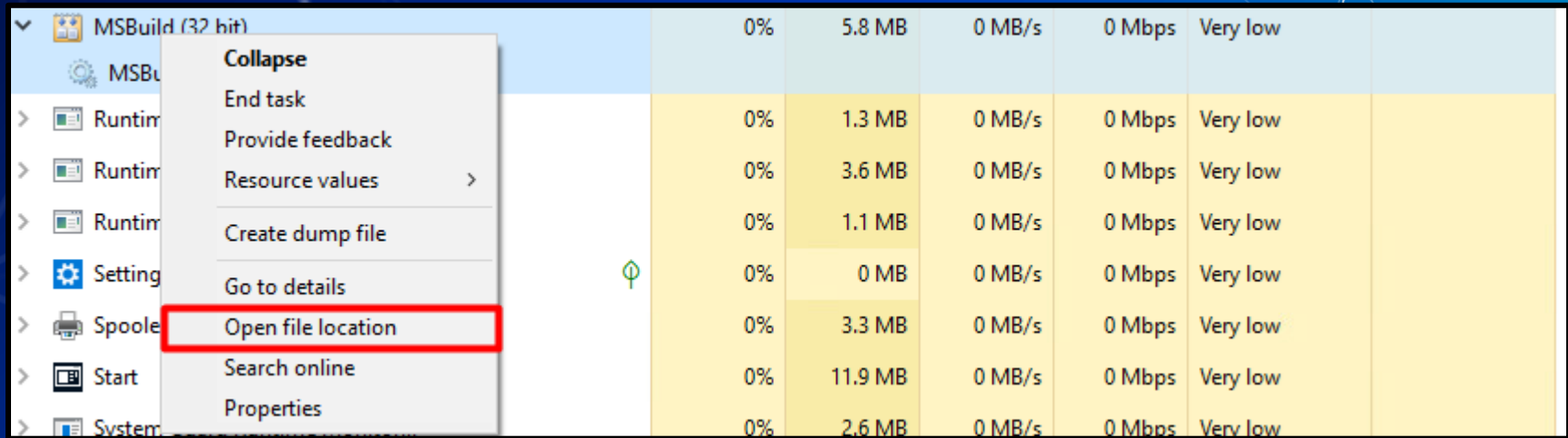
Task Manager cont.

How to open it?



Task Manager cont.

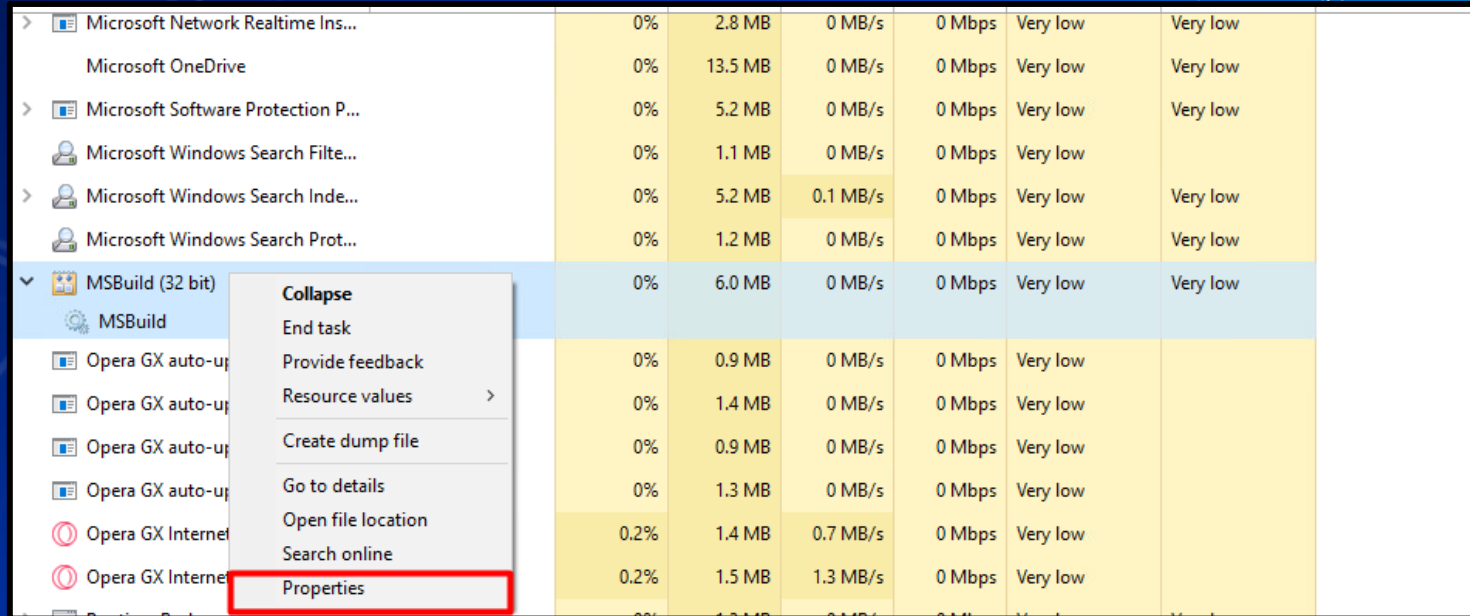
■ Can be used to find the location a running executable.



Task Name	CPU	Private	Working Set	IO	Network	Priority	...
MSBuild (32 bit)	0%	5.8 MB	0 MB/s	0 Mbps	Very low		
MSBuild (32 bit)							
Runtime	0%	1.3 MB	0 MB/s	0 Mbps	Very low		
Runtime	0%	3.6 MB	0 MB/s	0 Mbps	Very low		
Runtime	0%	1.1 MB	0 MB/s	0 Mbps	Very low		
Setting	0%	0 MB	0 MB/s	0 Mbps	Very low		
Spoole	0%	3.3 MB	0 MB/s	0 Mbps	Very low		
Start	0%	11.9 MB	0 MB/s	0 Mbps	Very low		
System	0%	2.6 MB	0 MB/s	0 Mbps	Very low		

Task Manager cont.

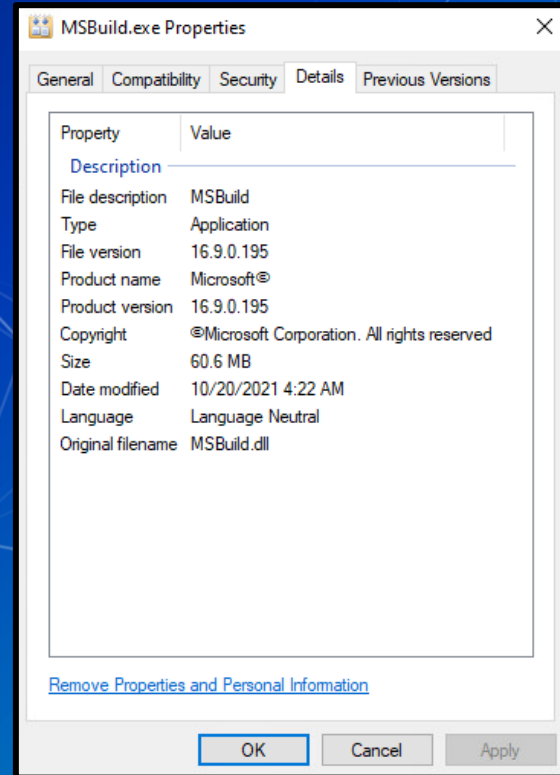
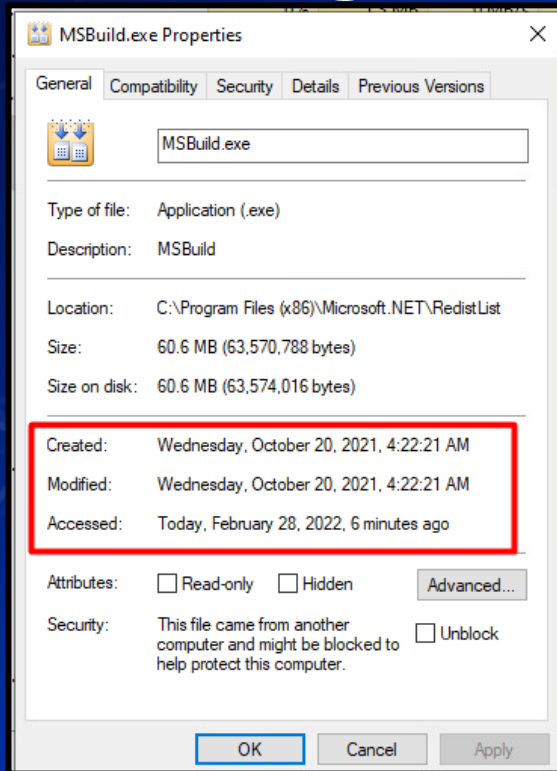
■ Show the properties of an executable



> Microsoft Network Realtime Ins...	0%	2.8 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft OneDrive	0%	13.5 MB	0 MB/s	0 Mbps	Very low	Very low
> Microsoft Software Protection P...	0%	5.2 MB	0 MB/s	0 Mbps	Very low	Very low
Microsoft Windows Search Filte...	0%	1.1 MB	0 MB/s	0 Mbps	Very low	Very low
> Microsoft Windows Search Inde...	0%	5.2 MB	0.1 MB/s	0 Mbps	Very low	Very low
Microsoft Windows Search Prot...	0%	1.2 MB	0 MB/s	0 Mbps	Very low	Very low
▼ MSBuild (32 bit)	0%	6.0 MB	0 MB/s	0 Mbps	Very low	Very low
MSBuild						
Opera GX auto-up	0%	0.9 MB	0 MB/s	0 Mbps	Very low	
Opera GX auto-up	0%	1.4 MB	0 MB/s	0 Mbps	Very low	
Opera GX auto-up	0%	0.9 MB	0 MB/s	0 Mbps	Very low	
Opera GX auto-up	0%	1.3 MB	0 MB/s	0 Mbps	Very low	
Opera GX Internet	0.2%	1.4 MB	0.7 MB/s	0 Mbps	Very low	
Opera GX Internet	0.2%	1.5 MB	1.3 MB/s	0 Mbps	Very low	

- Collapse
- End task
- Provide feedback
- Resource values >
- Create dump file
- Go to details
- Open file location
- Search online
- Properties

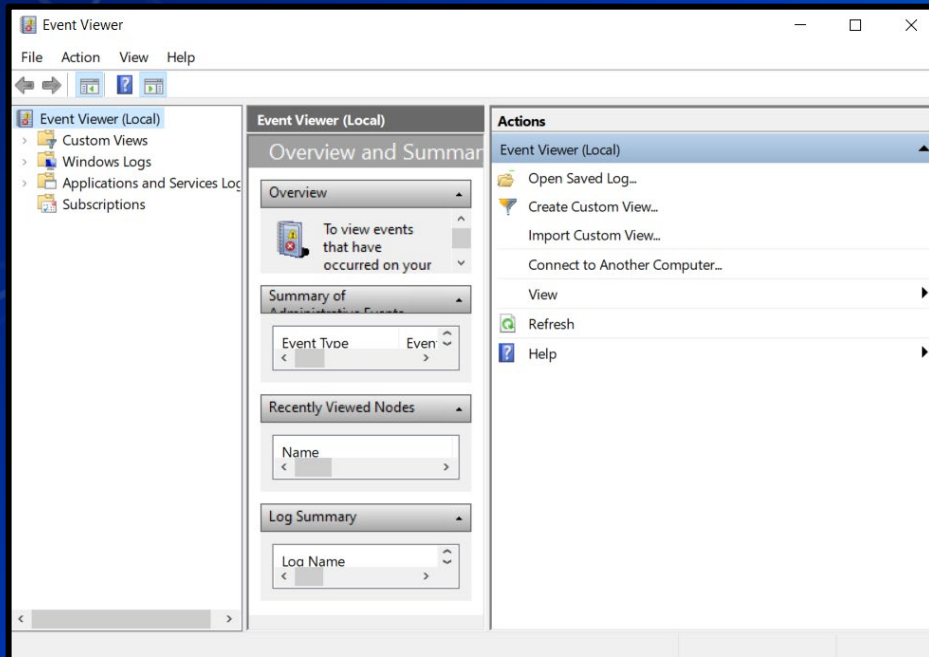
Task Manager cont.



Event Viewer

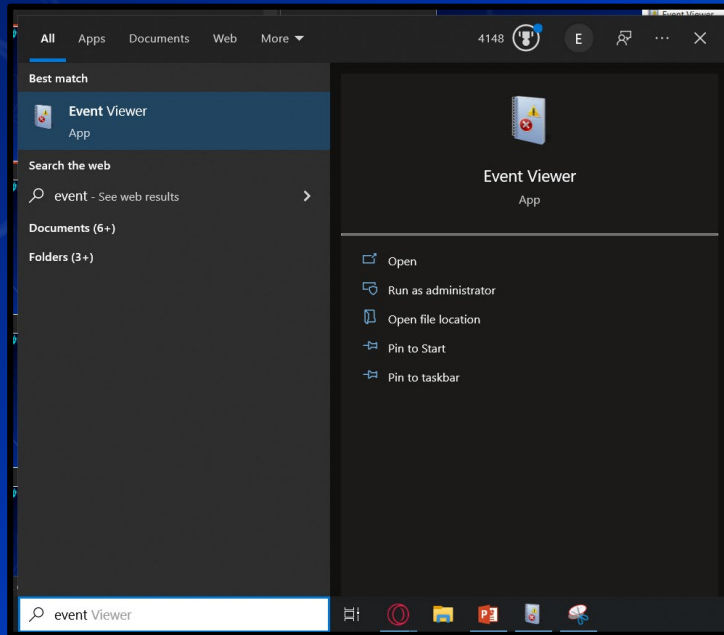
Event Viewer

■ Log viewer for Windows



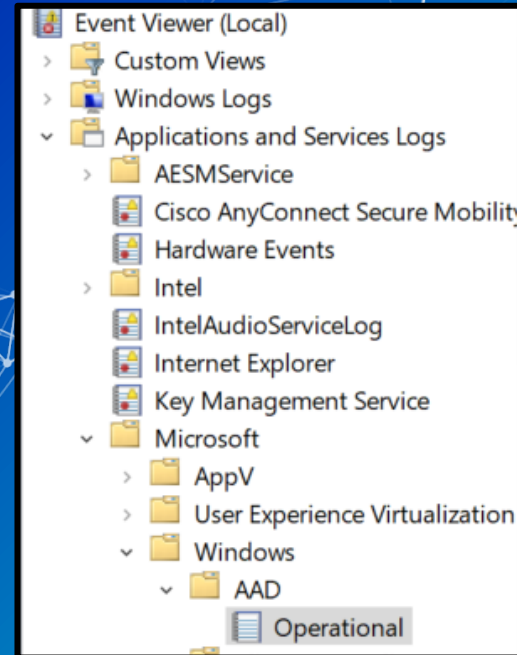
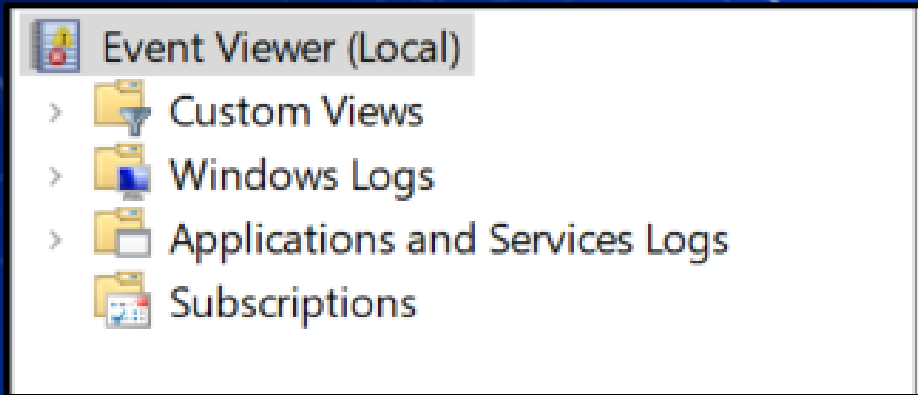
Event Viewer

■ Can be opened by searching for “event” and clicking open



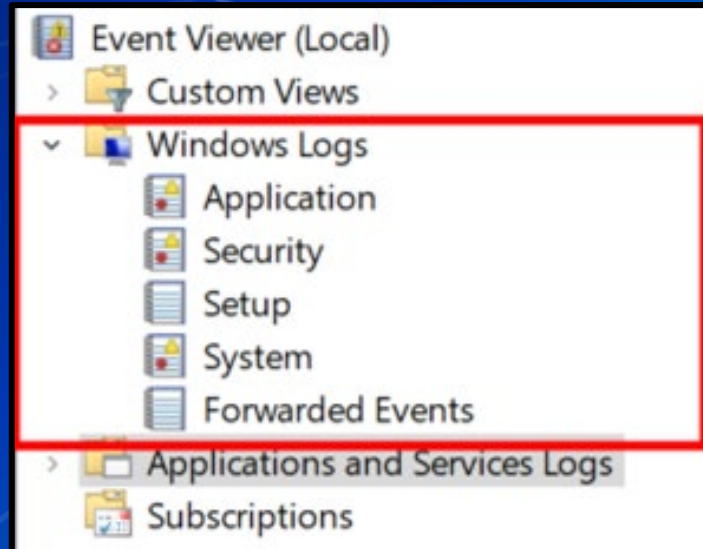
Event Viewer cont.

■ Logs are stored in a hierarchical structure



Event Viewer cont.

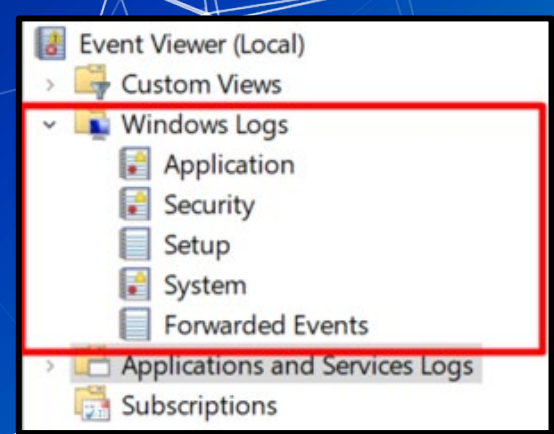
■ Windows activities are stored within the “Windows Logs” folder



Event Viewer cont.

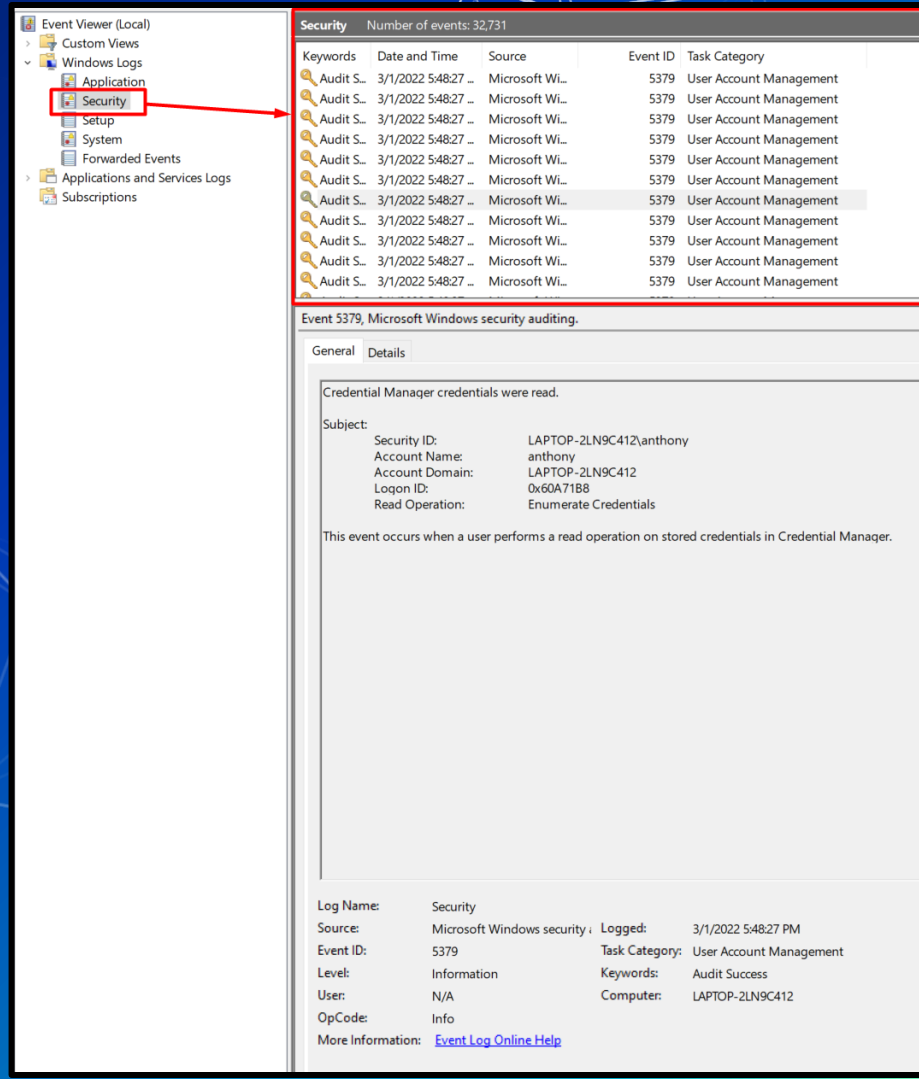
Windows Logs are divided into 5 categories

- Application
 - Logs related to some applications installed on system
- Security
 - Security related logs (authentication actions are found here)
- Setup
 - Installation of software on system (e.g., update installs are logged)
- System
 - Low-level system events
- Forwarded events
 - Events forwarded to local machine by remote machines



Event Viewer cont.

Individual logs are listed in the middle pane



The screenshot displays the Windows Event Viewer interface. The left pane shows the tree view with 'Security' selected. The middle pane lists 12 events, all with Event ID 5379 and Task Category 'User Account Management'. The right pane shows the details for event 5379, which is a 'Credential Manager credentials were read' event.

Keywords	Date and Time	Source	Event ID	Task Category
Audit S...	3/1/2022 5:48:27 ...	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 5:48:27 ...	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 5:48:27 ...	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 5:48:27 ...	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 5:48:27 ...	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 5:48:27 ...	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 5:48:27 ...	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 5:48:27 ...	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 5:48:27 ...	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 5:48:27 ...	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 5:48:27 ...	Microsoft Wi...	5379	User Account Management

Event 5379, Microsoft Windows security auditing.

General Details

Credential Manager credentials were read.

Subject:

Security ID: LAPTOP-2LN9C412\anthony
Account Name: anthony
Account Domain: LAPTOP-2LN9C412
Logon ID: 0x60A71B8
Read Operation: Enumerate Credentials

This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Log Name: Security
Source: Microsoft Windows security : Logged: 3/1/2022 5:48:27 PM
Event ID: 5379 Task Category: User Account Management
Level: Information Keywords: Audit Success
User: N/A Computer: LAPTOP-2LN9C412
OpCode: Info
More Information: [Event Log Online Help](#)

Event Viewer cont.

- Individual logs vary in complexity
- Windows generates many logs
 - Many of these logs are not helpful

An account was successfully logged on.

Subject:

Security ID: SYSTEM
Account Name: LAPTOP-2LN9C412\$
Account Domain: WORKGROUP
Logon ID: 0x3E7

Logon Information:

Logon Type: 2
Restricted Admin Mode: -
Virtual Account: No
Elevated Token: Yes

Impersonation Level:

Impersonation

New Logon:

Security ID: LAPTOP-2LN9C412\anthony
Account Name: anthony
Account Domain: LAPTOP-2LN9C412
Logon ID: 0x40A47CA
Linked Logon ID: 0x40A47FD
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

Process ID: 0x88c
Process Name: C:\Windows\System32\svchost.exe

Network Information:

Log Name: Security
Source: Microsoft Windows security i Logged: 2/28/2022 4:53:53 PM
Event ID: 4624 Task Category: Logon
Level: Information Keywords: Audit Success
User: N/A Computer: LAPTOP-2LN9C412
OpCode: Info
More Information: [Event Log Online Help](#)

Event Viewer cont.

■ Event IDs

- Identifier numbers Microsoft assigns to types of events.

■ Resource for Security Event IDs

- <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx>

Event Viewer cont.



← **Windows Security Log Event ID 4624** →

4624: An account was successfully logged on

On this page

- Description of this event
- Field level details
- Examples
- Discuss this event
- Mini-seminars on this event

[Ask a question about this event](#)

This is a highly valuable event since it documents each and every successful attempt to logon to the local computer regardless of logon type, location of the user or type of account. You can tie this event to logoff events 4634 and 4647 using Logon ID.

Win2012 adds the Impersonation Level field as shown in the example.

Win2016/10 add further fields explained below.

Operating Systems	Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and 2022
Category	Logon/Logoff
Subcategory	Logon
Type	Success
Corresponding events in Windows 2003 and before	528 , 540

Discussions on Event ID 4624

- Where does descriptive text come from at the end of 4624?
- 4624 Type 3 Filtering Help

Event Viewer cont.

Windows Security Log Event ID 4624

4624: An account was successfully logged on

On this page

- Description of this event
- Field level details
- Examples
- Discuss this event
- Mini-seminars on this event



This is a highly valuable event since it documents each and every successful attempt to logon to the local computer regardless of logon type, location of the user or type of account. You can tie this event to logoff events 4634 and 4647 using Logon ID.

Win2012 adds the Impersonation Level field as shown in the example.

Win2016/10 add further fields explained below.

Operating Systems	Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and 2022
Category	Logon/Logoff
• Subcategory	• Logon
Type	Success
Corresponding events in Windows 2003 and before	528 , 540

Discussions on Event ID 4624

- Where does descriptive text come from at the end of 4624?
- 4624 Type 3 Filtering Help

Security Number of events: 32,737 (1) New events available

Filtered: Log: Security; Source: ; Event ID: 4624. Number of events: 1,663

Keywords	Date and Time	Source	Event ID	Task Category
Audit S...	3/1/2022 6:13:59 PM	Microsoft Wi...	4624	Logon
Audit S...	3/1/2022 6:03:24 PM	Microsoft Wi...	4624	Logon
Audit S...	3/1/2022 6:03:22 PM	Microsoft Wi...	4624	Logon
Audit S...	3/1/2022 5:48:26 PM	Microsoft Wi...	4624	Logon
Audit S...	3/1/2022 5:47:27 PM	Microsoft Wi...	4624	Logon
Audit S...	3/1/2022 5:37:42 PM	Microsoft Wi...	4624	Logon
Audit S...	3/1/2022 5:36:37 PM	Microsoft Wi...	4624	Logon
Audit S...	3/1/2022 5:36:34 PM	Microsoft Wi...	4624	Logon
Audit S...	3/1/2022 5:35:36 PM	Microsoft Wi...	4624	Logon
Audit S...	3/1/2022 5:34:15 PM	Microsoft Wi...	4624	Logon

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID:	SYSTEM
Account Name:	LAPTOP-2LN9C4125
Account Domain:	WORKGROUP
Logon ID:	0x3E7

Logon Information:

Logon Type:	5
Restricted Admin Mode:	-
Virtual Account:	No
Elevated Token:	Yes

Impersonation Level: Impersonation

New Logon:

Security ID:	SYSTEM
Account Name:	SYSTEM
Account Domain:	NT AUTHORITY
Logon ID:	0x3E7
Linked Logon ID:	0x0
Network Account Name:	-
Network Account Domain:	-
Logon GUID:	(00000000-0000-0000-0000-000000000000)

Process Information:

Process ID:	0x470
Process Name:	C:\Windows\System32\services.exe

Network Information:

Log Name: Security

Source: Microsoft Windows security ; Logged: 3/1/2022 6:13:59 PM

Event ID: 4624 Task Category: Logon

Level: Information Keywords: Audit Success

User: N/A Computer: LAPTOP-2LN9C412

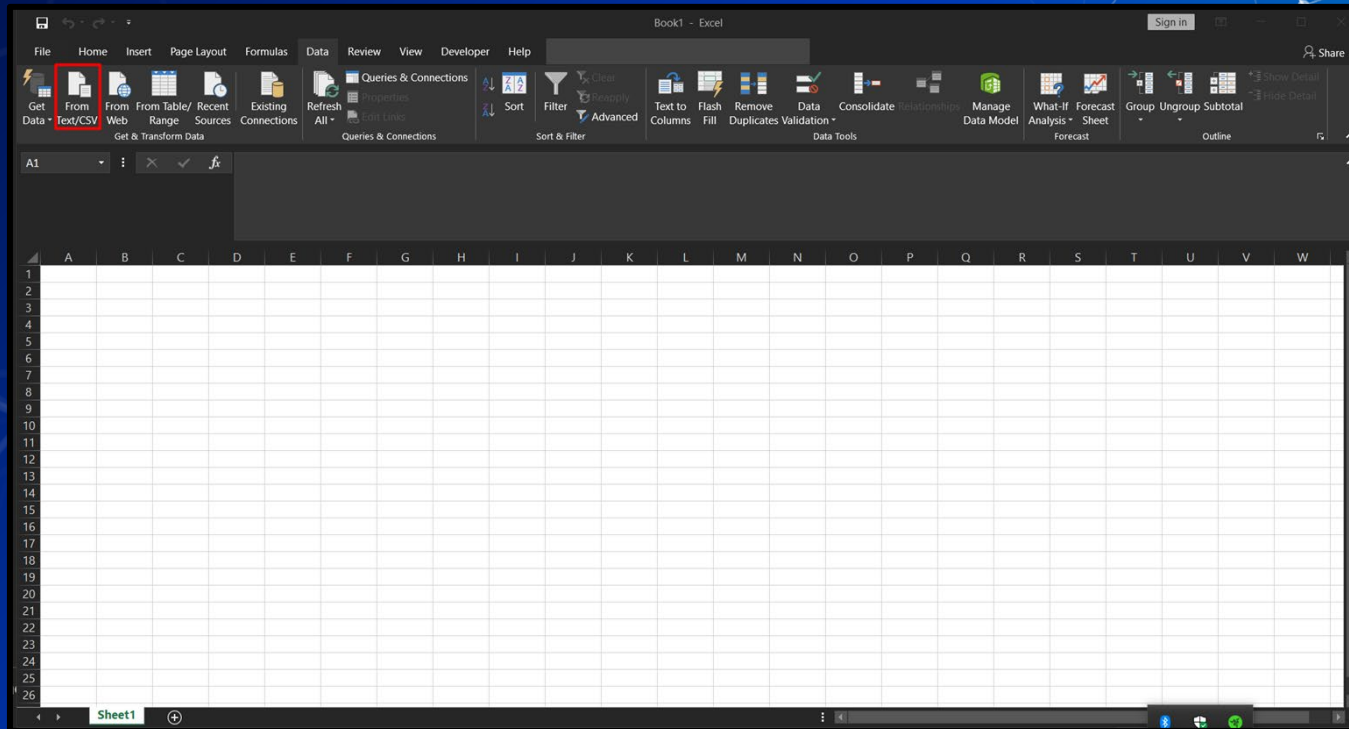
OpCode: Info

More Information: [Event Log Online Help](#)

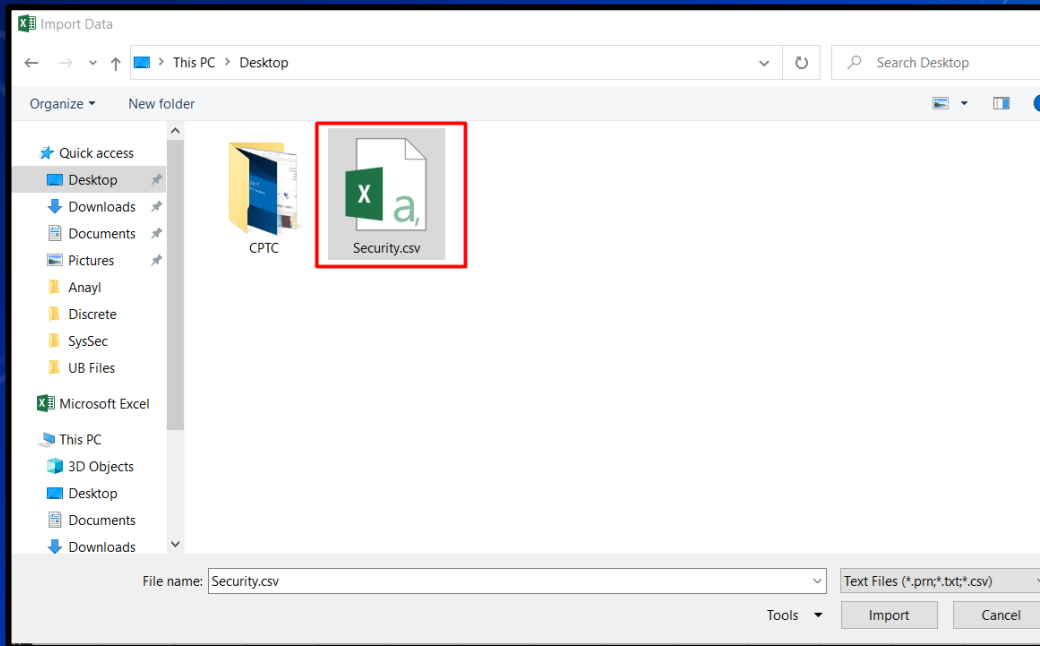
Event Viewer cont.

- Excel can interpret these logs and be used to search them.
 - The CSV must be imported properly

Importing Logs in Excel



Importing Logs in Excel



Importing Logs in Excel

Security.csv

File Origin: 65001: Unicode (UTF-8) | Delimiter: Comma | Data Type Detection: Based on first 200 rows

Keywords	Date and Time	Source	Event ID	Task Category	
Audit Success	3/1/2022 6:21:00 PM	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enr
Audit Success	3/1/2022 6:21:00 PM	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enr
Audit Success	3/1/2022 6:20:54 PM	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enr
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read
Audit Success	3/1/2022 6:16:02 PM	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read

Load | Transform Data | Cancel

Homework Hint

- The initial vector of breach is in the Windows logs.
- The attack was a brute force attack against one of the Windows remote access tools.

Questions?

Network Forensics

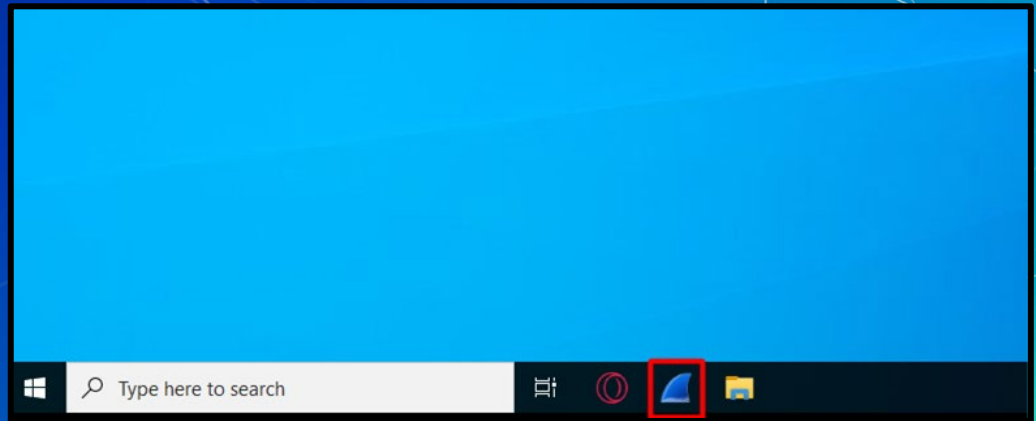
Network Forensics Hands-on

- Sign onto the machine in your team folder called "WINIRForClass"
 - Username: sysadmin
 - Password: Change.me!



Wireshark

- Packet analyzer
- Free
- Open-source
- Available on:
 - Windows
 - Linux
 - MacOS



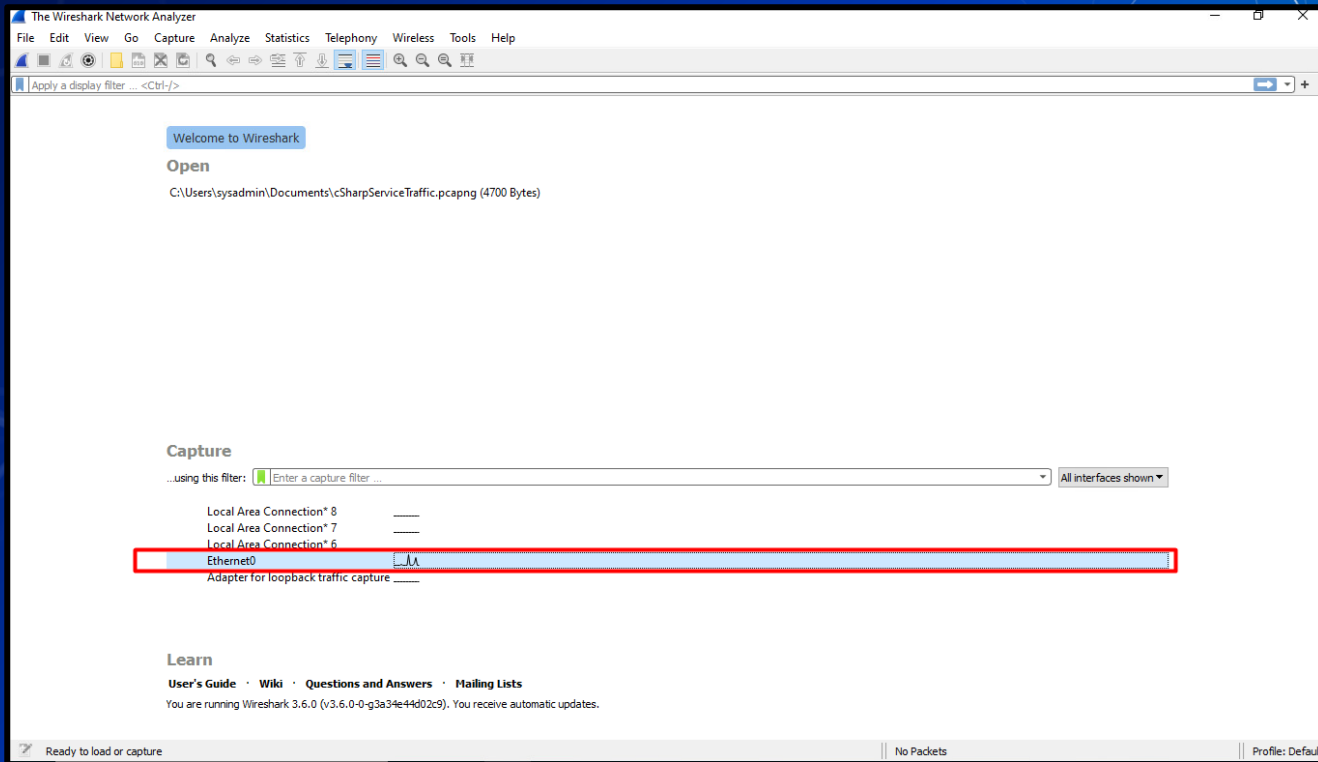
In Class Activity

WireShark

Hands on 0 - Wireshark

- Locate suspicious network traffic
- Create a Windows firewall rule to block the traffic

Network Forensics Hands-on





Break Slide



PowerShell For IR

PowerShell

■ Automation and configuration tool

■ <https://docs.microsoft.com/en-us/powershell/>

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

Try the new cross-platform PowerShell https://aka.ms/powershell

PS C:\Users\anthony>
```

Cmdlets

- Cmdlets are commands in PowerShell
- Cmdlets use verb-noun format
 - `Get-computerinfo`
 - `Get-filehash`
 - `Write-output`
 - Etc...

Get-Filehash

- "Computes the hash value for a file by using a specified hash algorithm."

In Class Activity

PowerShell

Hands on 1 – Piping Output

- Compute the SHA384 hash of test.exe on your desktop using `get-filehash`
- Get-Filehash documentation
 - <https://tinyurl.com/yw9zv3cw>

Hands on 1 – Piping Output

■ Any problems with the result?

Hands on 1 – Piping Output

- We can send output from one command to another
- Output of command 1 is sent to command 2
 - Ex: `<command_1> | <command_2>`
- Using the documentation below what command can we pipe to for the fix the output?
 - <https://tinyurl.com/yw9zv3cw>

Searching PowerShell Output

■ `Get-Service` "Gets the services on the computer."

```
PS C:\Users\anthony> get-service
```

Status	Name	DisplayName
Stopped	AarSvc_4dd2c3d	Agent Activation Runtime_4dd2c3d
Running	AdobeARMService	Adobe Acrobat Update Service
Running	AESMSvc	Intel® SGX AESM
Stopped	AJRouter	AllJoyn Router Service
Stopped	ALG	Application Layer Gateway Service
Stopped	AppIDSvc	Application Identity
Running	AppInfo	Application Information
Stopped	AppMgmt	Application Management
Stopped	AppReadiness	App Readiness
Stopped	AppVClient	Microsoft App-V Client
Running	AppSvc	AppX Deployment Service (AppXSVC)
Stopped	AssignedAccessM...	AssignedAccessManager Service
Running	AudioEndpointBu...	Windows Audio Endpoint Builder
Running	Audiosrv	Windows Audio
Stopped	autoimesvc	Cellular Time
Stopped	AxInstSV	ActiveX Installer (AxInstSV)
Stopped	BcastDVRUserSer...	GameDVR and Broadcast User Service...
Running	BDESVC	BitLocker Drive Encryption Service
Stopped	BESvc	BattlEye Service
Running	BFE	Base Filtering Engine
Stopped	BITS	Background Intelligent Transfer Ser...
Stopped	BluetoothUserSe...	Bluetooth User Support Service_4dd2c3d
Running	BrokenInfrastru...	Background Tasks Infrastructure Ser...
Running	BTAGService	Bluetooth Audio Gateway Service
Running	BthAvctpSvc	AVCTP service
Running	bthserv	Bluetooth Support Service
Running	camsvc	Capability Access Manager Service
Stopped	CaptureService_...	CaptureService_4dd2c3d
Running	cbdhsvc_4dd2c3d	Clipboard User Service_4dd2c3d
Running	CDPSvc	Connected Devices Platform Service
Running	CDPSvc_4dd2c3d	Connected Devices Platform User Ser...
Stopped	CertPropSvc	Certificate Propagation
Running	ClickToRunSvc	Microsoft Office Click-to-Run Service
Running	ClipSVC	Client License Service (ClipSVC)
Stopped	COMSysApp	COM+ System Application
Stopped	ConsentUxUserSv...	ConsentUX_4dd2c3d
Running	CoreMessagingRe...	CoreMessaging
Running	cpbs	Intel(R) Content Protection HECI Se...
Running	cpispcon	Intel(R) Content Protection HDCP Se...
Stopped	CredentialEnrol...	CredentialEnrollmentManagerUserSvc...
Running	CryptSvc	Cryptographic Services
Stopped	CscService	Offline Files
Running	DcomLaunch	DCOM Server Process Launcher

Hands on 2 – Searching Output

- Run `get-service`
- Run `get-service | select *`
- What is the difference of the output?

Hands on 2 – Searching Output

```
PS C:\Users\anthony> get-service
```

Status	Name	DisplayName
Running	AarSvc_197f19e7	Agent Activation Runtime_197f19e7
Running	AdobeARMService	Adobe Acrobat Update Service
Running	AESMSvc	Intel® SGX AESM
Stopped	AJRouter	AllJoyn Router Service
Stopped	ALG	Application Layer Gateway Service
Stopped	AppIDSvc	Application Identity
Running	Appinfo	Application Information
Stopped	AppMgmt	Application Management
Stopped	AppReadiness	App Readiness
Stopped	AppVClient	Microsoft App-V Client
Stopped	AppXSvc	AppX Deployment Service (AppXSvc)
Stopped	AssignedAccessM...	AssignedAccessManager Service
Running	AudioEndpointBu...	Windows Audio Endpoint Builder
Running	Audiosrv	Windows Audio
Stopped	autotimesvc	Cellular Time
Stopped	AxInstSV	ActiveX Installer (AxInstSV)
Stopped	BcastDVRUserSer...	GameDVR and Broadcast User Service_...
Running	BDESVC	BitLocker Drive Encryption Service
Stopped	BESvc	BattlEye Service
Running	BFE	Base Filtering Engine
Stopped	BITS	Background Intelligent Transfer Ser...
Stopped	BluetoothUserSe...	Bluetooth User Support Service_197f...
Running	BrokerInfrastru...	Background Tasks Infrastructure Ser...
Running	BTAGService	Bluetooth Audio Gateway Service
Running	BthAvctpSvc	AVCTP service
Running	bthserv	Bluetooth Support Service

```
PS C:\Users\anthony> get-service | select * | format-list
```

```
Name : AarSvc_197f19e7
RequiredServices : {}
CanPauseAndContinue : False
CanShutdown : False
CanStop : True
DisplayName : Agent Activation Runtime_197f19e7
DependentServices : {}
MachineName : -
ServiceName : AarSvc_197f19e7
ServicesDependedOn : {}
ServiceHandle :
Status : Running
ServiceType : 240
StartType : Manual
Site :
Container :

Name : AdobeARMService
RequiredServices : {}
CanPauseAndContinue : False
CanShutdown : False
CanStop : True
DisplayName : Adobe Acrobat Update Service
DependentServices : {}
MachineName : -
ServiceName : AdobeARMService
ServicesDependedOn : {}
ServiceHandle :
Status : Running
ServiceType : Win32OwnProcess
StartType : Automatic
Site :
Container :

Name : AESMSvc
RequiredServices : {RPCSS}
CanPauseAndContinue : False
CanShutdown : False
CanStop : True
DisplayName : Intel® SGX AESM
DependentServices : {}
MachineName : -
ServiceName : AESMSvc
ServicesDependedOn : {RPCSS}
ServiceHandle :
Status : Running
ServiceType : Win32OwnProcess
StartType : Automatic
Site :
Container :
```


Hands on 2 – Searching Output

- List ONLY services that have a StartType as automatic
 - Ensure the output DOESN'T get trimmed
- Use the below documentation
 - <https://tinyurl.com/z5psdn87>

WMI & Services

Windows Management Instrumentation (WMI)

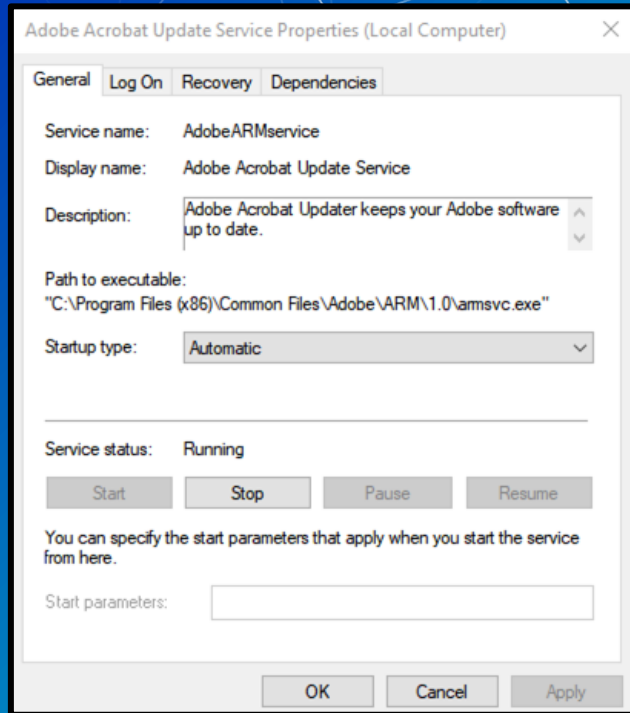
- Can be used to manage Windows devices
- Allows remote communications through:
 - Distributed Component Object Model (DCOM)
 - Windows Remote Management (WINRM)
- Great tool for IT personnel and malicious actors

Services

■ Behind the scenes to keep things working

■ 4 startup types

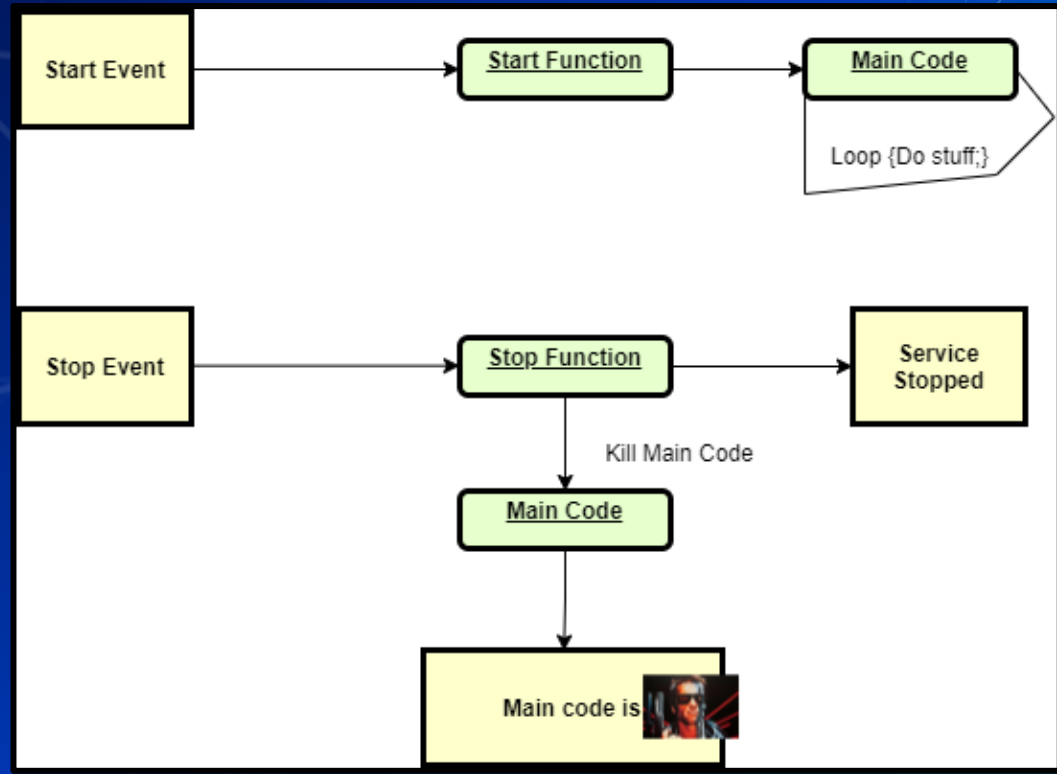
- Automatic (Delayed Start)
- Automatic
- Manual
- Disabled



Services

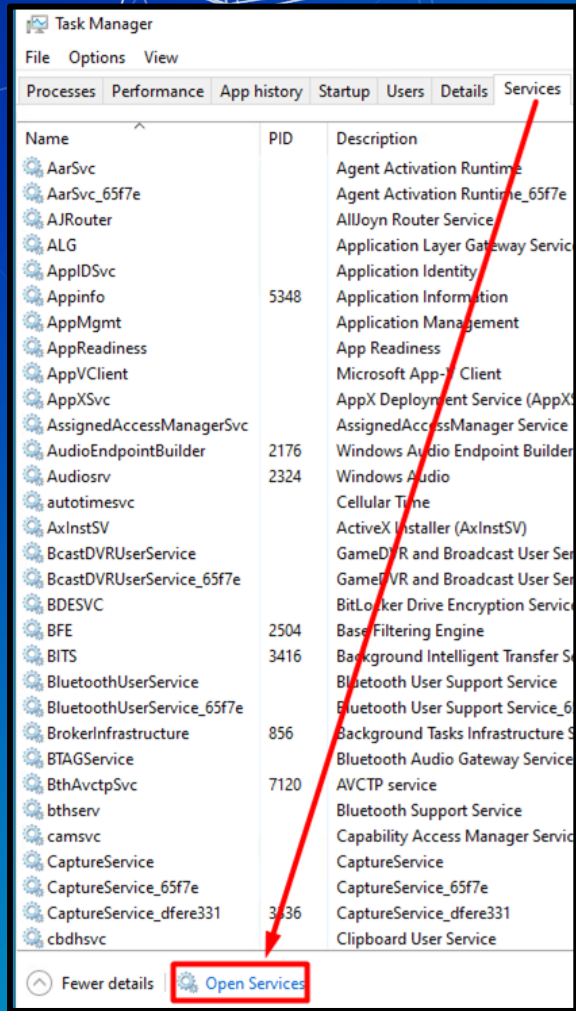
- Can run as nt authority \system
 - nt authority \system != root
 - Is more powerful than an “administrator”
- Active even when no user is signed in
- May be hosted by the service host (svchost.exe)
- May executables that are designated to be services
- Follow a defined service model

Service Model



How to list services?

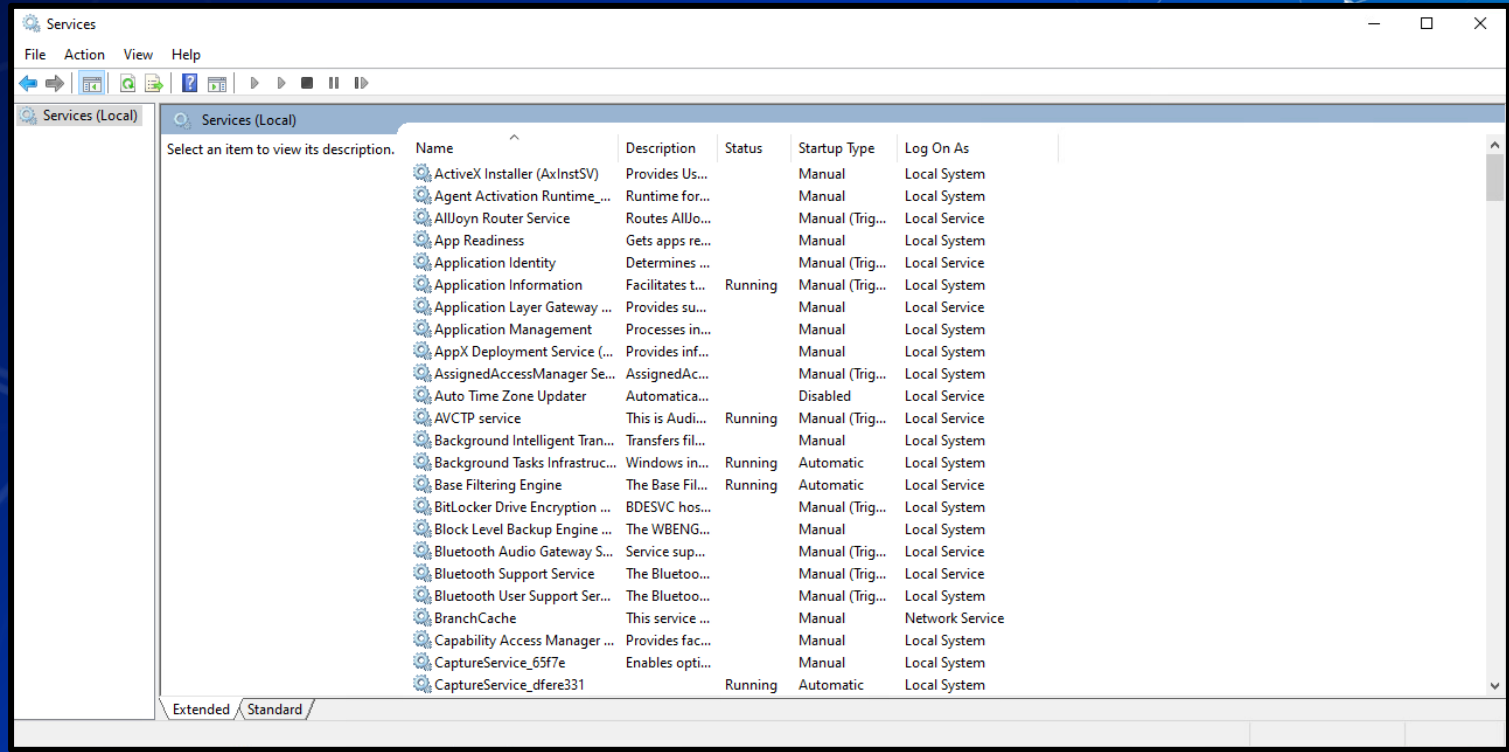
■ Open Task Manager and navigate to services tab



The screenshot shows the Windows Task Manager application with the 'Services' tab selected. A red arrow points from the 'Services' tab header to the 'Open Services' button at the bottom of the list.

Name	PID	Description
AarSvc		Agent Activation Runtime
AarSvc_65f7e		Agent Activation Runtime_65f7e
AJRouter		AllJoyn Router Service
ALG		Application Layer Gateway Service
AppIDSvc		Application Identity
Appinfo	5348	Application Information
AppMgmt		Application Management
AppReadiness		App Readiness
AppVClient		Microsoft App-V Client
AppXSvc		AppX Deployment Service (AppX)
AssignedAccessManagerSvc		AssignedAccessManager Service
AudioEndpointBuilder	2176	Windows Audio Endpoint Builder
Audiosrv	2324	Windows Audio
autotimesvc		Cellular Time
AxInstSV		ActiveX Installer (AxInstSV)
BcastDVRUserService		GameDVR and Broadcast User Ser
BcastDVRUserService_65f7e		GameDVR and Broadcast User Ser
BDESVC		BitLocker Drive Encryption Service
BFE	2504	Base Filtering Engine
BITS	3416	Background Intelligent Transfer S
BluetoothUserService		Bluetooth User Support Service
BluetoothUserService_65f7e		Bluetooth User Support Service,6
BrokerInfrastructure	856	Background Tasks Infrastructure S
BTAGService		Bluetooth Audio Gateway Service
BthAvctpSvc	7120	AVCTP service
bthserv		Bluetooth Support Service
camsvc		Capability Access Manager Servi
CaptureService		CaptureService
CaptureService_65f7e		CaptureService_65f7e
CaptureService_dfare331	3336	CaptureService_dfare331
cbdhsvc		Clipboard User Service

Services List



The screenshot shows the Windows Services console window. The title bar reads "Services". The menu bar includes "File", "Action", "View", and "Help". The address bar shows "Services (Local)". The main area displays a list of services with columns for Name, Description, Status, Startup Type, and Log On As. The "Standard" tab is selected at the bottom.

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local System
Agent Activation Runtime...	Runtime for...		Manual	Local System
AllJoyn Router Service	Routes AllJo...		Manual (Trig...	Local Service
App Readiness	Gets apps re...		Manual	Local System
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...	Running	Manual (Trig...	Local System
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local System
AppX Deployment Service (...)	Provides inf...		Manual	Local System
AssignedAccessManager Se...	AssignedAc...		Manual (Trig...	Local System
Auto Time Zone Updater	Automatica...		Disabled	Local Service
AVCTP service	This is Audi...	Running	Manual (Trig...	Local Service
Background Intelligent Tran...	Transfers fil...		Manual	Local System
Background Tasks Infrastruc...	Windows in...	Running	Automatic	Local System
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
BitLocker Drive Encryption ...	BDESVC hos...		Manual (Trig...	Local System
Block Level Backup Engine ...	The WBENG...		Manual	Local System
Bluetooth Audio Gateway S...	Service sup...		Manual (Trig...	Local Service
Bluetooth Support Service	The Bluetoo...		Manual (Trig...	Local Service
Bluetooth User Support Ser...	The Bluetoo...		Manual (Trig...	Local System
BranchCache	This service ...		Manual	Network Service
Capability Access Manager ...	Provides fac...		Manual	Local System
CaptureService_65f7e	Enables opti...		Manual	Local System
CaptureService_dfere331		Running	Automatic	Local System

Services List

Services (Local)

Cryptographic Services

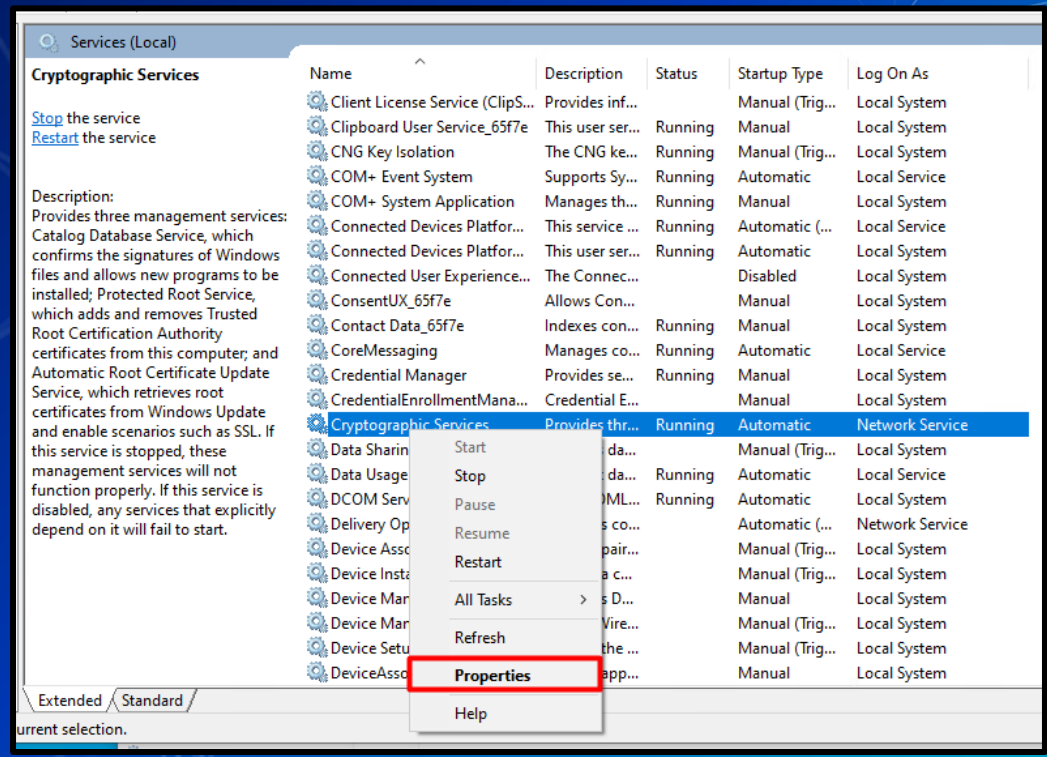
[Stop](#) the service
[Restart](#) the service

Description:
Provides three management services: Catalog Database Service, which confirms the signatures of Windows files and allows new programs to be installed; Protected Root Service, which adds and removes Trusted Root Certification Authority certificates from this computer; and Automatic Root Certificate Update Service, which retrieves root certificates from Windows Update and enable scenarios such as SSL. If this service is stopped, these management services will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start.

Name	Description	Status	Startup Type	Log On As
Client License Service (ClipS...	Provides inf...		Manual (Trig...	Local System
Clipboard User Service_65f7e	This user ser...	Running	Manual	Local System
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Local System
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...	Running	Manual	Local System
Connected Devices Platfor...	This service ...	Running	Automatic (...)	Local Service
Connected Devices Platfor...	This user ser...	Running	Automatic	Local System
Connected User Experience...	The Connec...		Disabled	Local System
ConsentUX_65f7e	Allows Con...		Manual	Local System
Contact Data_65f7e	Indexes con...	Running	Manual	Local System
CoreMessaging	Manages co...	Running	Automatic	Local Service
Credential Manager	Provides se...	Running	Manual	Local System
CredentialEnrollmentMana...	Credential E...		Manual	Local System
Cryptographic Services	Provides thr...	Running	Automatic	Network Service
Data Sharing Service	Provides da...		Manual (Trig...	Local System
Data Usage	Network da...	Running	Automatic	Local Service
DCOM Server Process Laun...	The DCOML...	Running	Automatic	Local System
Delivery Optimization	Performs co...		Automatic (...)	Network Service
Device Association Service	Enables pair...		Manual (Trig...	Local System
Device Install Service	Enables a c...		Manual (Trig...	Local System
Device Management Enroll...	Performs D...		Manual	Local System
Device Management Wirel...	Routes Wire...		Manual (Trig...	Local System
Device Setup Manager	Enables the ...		Manual (Trig...	Local System
DeviceAssociationBroker_65...	Enables app...		Manual	Local System

Extended / Standard

Services List



The screenshot shows the Windows Services console window titled 'Services (Local)'. The 'Cryptographic Services' group is expanded, and a context menu is open over the 'Cryptographic Services' entry. The menu options include Start, Stop, Pause, Resume, Restart, All Tasks, Refresh, Properties (highlighted with a red box), and Help. The background shows a list of services with columns for Name, Description, Status, Startup Type, and Log On As.

Name	Description	Status	Startup Type	Log On As
Client License Service (ClipS...	Provides inf...	Manual (Trig...	Local System	
Clipboard User Service_65f7e	This user ser...	Running	Manual	Local System
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Local System
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...	Running	Manual	Local System
Connected Devices Platfor...	This service ...	Running	Automatic (...)	Local Service
Connected Devices Platfor...	This user ser...	Running	Automatic	Local System
Connected User Experience...	The Connec...	Disabled	Local System	
ConsentUX_65f7e	Allows Con...	Manual	Local System	
Contact Data_65f7e	Indexes con...	Running	Manual	Local System
CoreMessaging	Manages co...	Running	Automatic	Local Service
Credential Manager	Provides se...	Running	Manual	Local System
CredentialEnrollmentMana...	Credential E...	Manual	Local System	
Cryptographic Services	Provides thr...	Running	Automatic	Network Service
Data Sharin...	da...	Manual (Trig...	Local System	
Data Usage	da...	Running	Automatic	Local Service
DCOM Serv...	ML...	Running	Automatic	Local System
Delivery Op...	s co...	Automatic (...)	Network Service	
Device Assc...	pair...	Manual (Trig...	Local System	
Device Insta...	a c...	Manual (Trig...	Local System	
Device Mar...	s D...	Manual	Local System	
Device Mar...	Vire...	Manual (Trig...	Local System	
Device Setu...	the ...	Manual (Trig...	Local System	
DeviceAsso...	app...	Manual	Local System	

Services List

Cryptographic Services Properties (Local Computer) X

General Log On Recovery Dependencies

Service name: CryptSvc
Display name: Cryptographic Services
Description: Provides three management services: Catalog Database Service, which confirms the signatures of Windows files and allows new programs to be
Path to executable: C:\Windows\system32\svchost.exe -k NetworkService -p
Startup type: Automatic
Service status: Disabled

Start Stop Pause Resume

You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK Cancel Apply

Services List

Cryptographic Services Properties (Local Computer) ✕

General Log On Recovery Dependencies

Log on as:

Local System account
 Allow service to interact with desktop

This account:

Password:

Confirm password:

Services List

Cryptographic Services Properties (Local Computer) ✕

General Log On Recovery Dependencies

Select the computer's response if this service fails. [Help me set up recovery actions](#)

First failure: Restart the Service ▼

Second failure: Take No Action ▼

Subsequent failures: Take No Action ▼

Reset fail count after: 1 days

Restart service after: 1 minutes

Enable actions for stops with errors. Restart Computer Options...

Run program

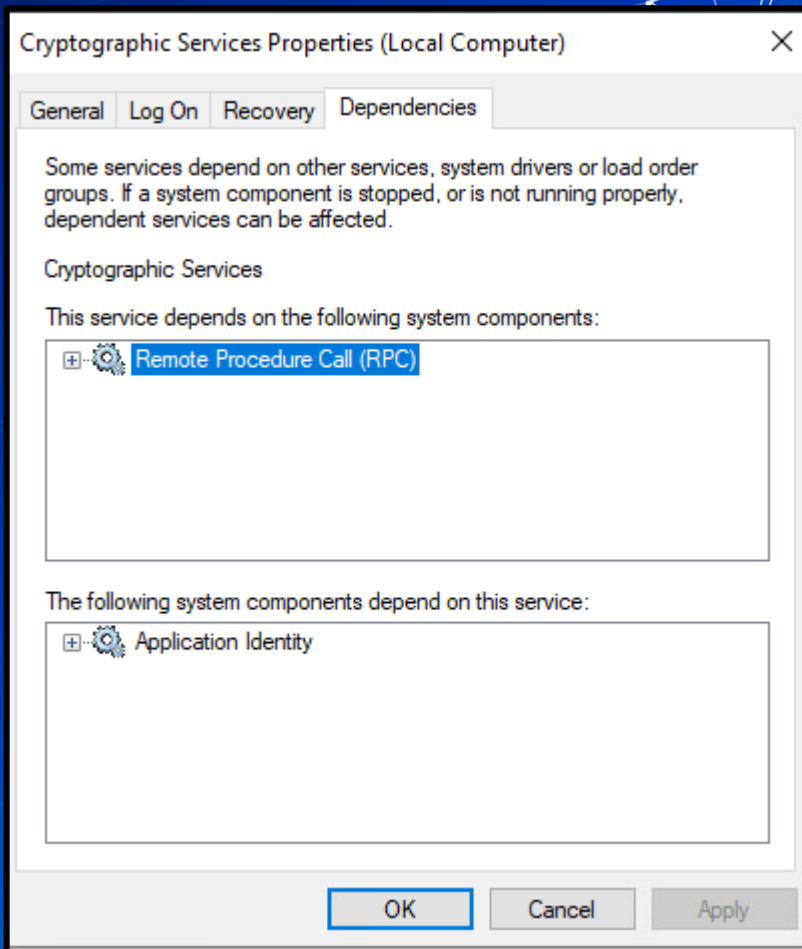
Program: Browse...

Command line parameters:

Append fail count to end of command line (/fail=%1%)

OK Cancel Apply

Services List



In Class Activity

Find a Malicious Service

Hands on 3- Find a Malicious Service

- Use the previous command we learned
 - `Get-WmiObject win32_Service`
 - Add `| ogv` at the end
- Attackers often want constant access
 - What StartType would an attacker use?
- If you see something say something
 - Google anything suspicious
 - Legitimate applications break often and people post online about them
- Remove the malicious service
 - Hint[0]: `sc delete <service name>`
 - Hint[1]: Can services be processes?



Hands on 3- Delete a Malicious Service

1. <REDACTED>
2. Using Command Prompt, enter: <REDACTED>
3. Reboot

RESTART YOUR WINDOWS VM

Persistence

Persistence

- Malware aims to survive
 - Restart
 - Settings Changes
 - Users signing on/off
 - Network connectivity loss
 - Countermeasures
 - Systems updates
 - Anything else....

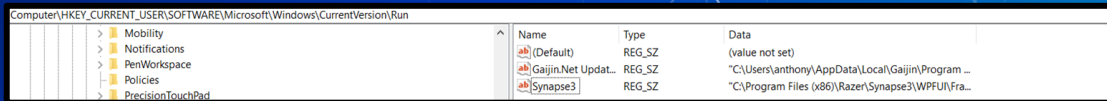
Persistence Methods

■ Windows persistence methods and their complexity

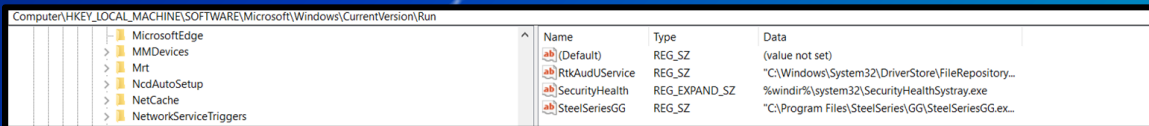
- Drivers (HIGH)
- Registry Keys (LOW)
- Startup Objects (LOW)
- Scheduled Tasks (LOW-MEDIUM)
- Image File Execution Options (MEDIUM)
 - Hint: Might be relevant for your homework this week
- WMI Subscriptions (MEDIUM)
- PowerShell Profiles (LOW-MEDIUM)
- Malicious Group Policies (MEDIUM)

Registry Keys

- Registry Editor is a GUI way of viewing registry
 - `Get-ItemProperty` can be used as well
 - <https://tinyurl.com/9hbeh72f>
- Two directories for running at sign on
 - `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
 - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`



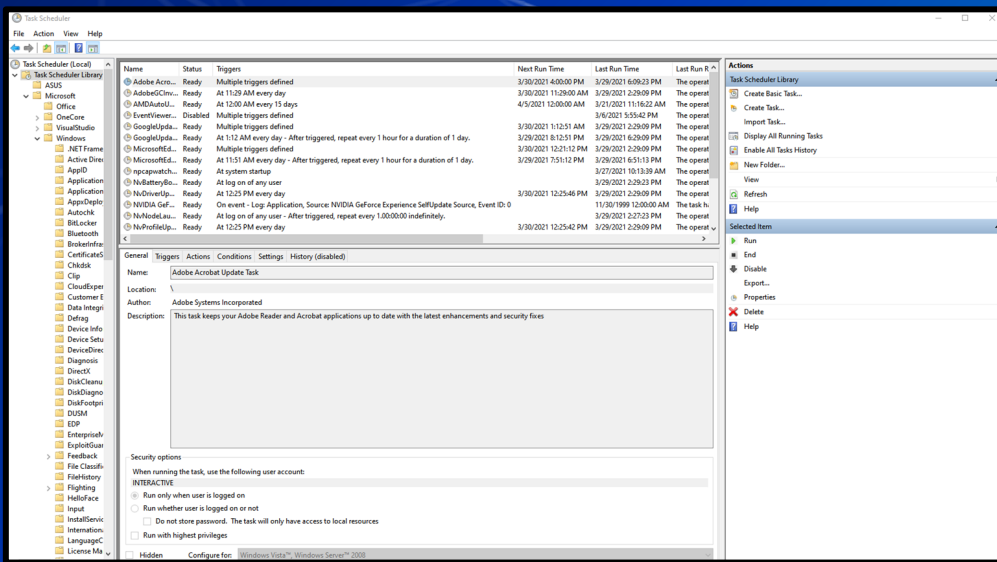
Name	Type	Data
(Default)	REG_SZ	(value not set)
Gaijin.Net Updat...	REG_SZ	"C:\Users\anthony\AppData\Local\Gaijin\Program ...
Synapse3	REG_SZ	"C:\Program Files (x86)\Razer\Synapse3\WPFUI\Fra...



Name	Type	Data
(Default)	REG_SZ	(value not set)
RtkAudUService	REG_SZ	"C:\Windows\System32\DriverStore\FileRepository...
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealth\Systray.exe
SteelSeriesGG	REG_SZ	"C:\Program Files\SteelSeries\GG\SteelSeriesGG.ex...

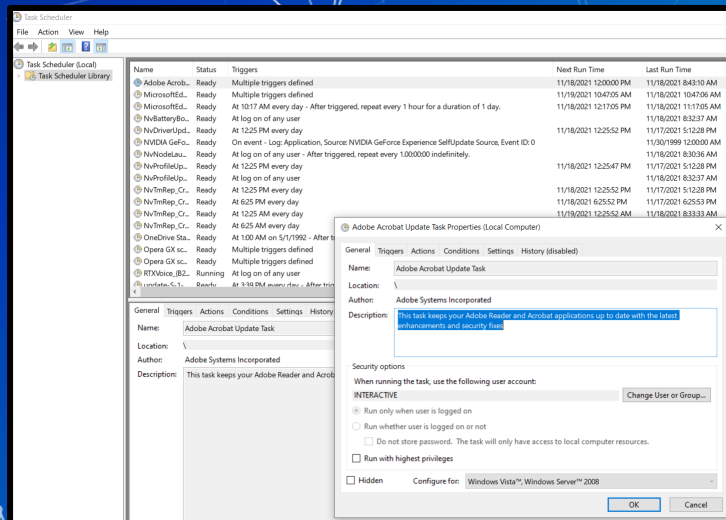
Scheduled Tasks

- Perform actions given specific triggers
- Stored in `C:\Windows\System32\Tasks` as xml files

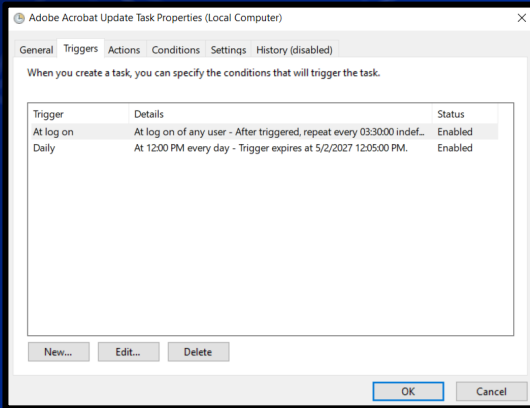


Scheduled Tasks cont.

- Can be managed through Task Scheduler
- Consists of Triggers & Actions
 - Triggers: When Do?
 - Actions: What Do?

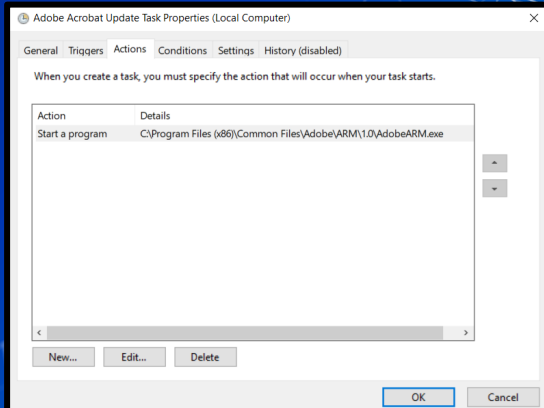


The screenshot shows the Windows Task Scheduler interface. On the left, a list of tasks is displayed with columns for Name, Status, Triggers, Next Run Time, and Last Run Time. The 'Adobe Acrobat Update Task' is highlighted. On the right, the 'Adobe Acrobat Update Task Properties' dialog box is open, showing the 'General' tab. The task name is 'Adobe Acrobat Update Task', the location is '\', and the author is 'Adobe Systems Incorporated'. The description is 'This task keeps your Adobe Reader and Acrobat applications up to date with the latest enhancements and security fixes'. The 'Security options' section is expanded, showing 'INTERACTIVE' selected, with options for 'Run only when user is logged on', 'Run whether user is logged on or not', 'Do not store password', and 'Run with highest privileges'. The 'Hidden' checkbox is unchecked, and the 'Configure for' dropdown is set to 'Windows Vista™, Windows Server™ 2008'. 'OK' and 'Cancel' buttons are at the bottom.



This screenshot shows the 'Triggers' tab of the 'Adobe Acrobat Update Task Properties' dialog. It contains a table with columns for Trigger, Details, and Status. Two triggers are listed: 'At log on' and 'Daily'. The 'At log on' trigger details are 'At log on of any user - After triggered, repeat every 033000 indef...' and its status is 'Enabled'. The 'Daily' trigger details are 'At 12:00 PM every day - Trigger expires at 5/2/2027 12:05:00 PM.' and its status is 'Enabled'. At the bottom, there are 'New...', 'Edit...', and 'Delete' buttons, and 'OK' and 'Cancel' buttons.

Trigger	Details	Status
At log on	At log on of any user - After triggered, repeat every 033000 indef...	Enabled
Daily	At 12:00 PM every day - Trigger expires at 5/2/2027 12:05:00 PM.	Enabled



This screenshot shows the 'Actions' tab of the 'Adobe Acrobat Update Task Properties' dialog. It contains a table with columns for Action and Details. One action is listed: 'Start a program' with details 'C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe'. At the bottom, there are 'New...', 'Edit...', and 'Delete' buttons, and 'OK' and 'Cancel' buttons.

Action	Details
Start a program	C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe

PowerShell Profile

- Runs each time PowerShell.exe is opened
- A PowerShell script

Description	Path
All Users, All Hosts	\$PSHOME\Profile.ps1
All Users, Current Host	\$PSHOME\Microsoft.PowerShell_profile.ps1
Current User, All Hosts	\$Home\[My]Documents\PowerShell\Profile.ps1
Current user, Current Host	\$Home\[My]Documents\PowerShell\ Microsoft.PowerShell_profile.ps1

Malicious Group Policies

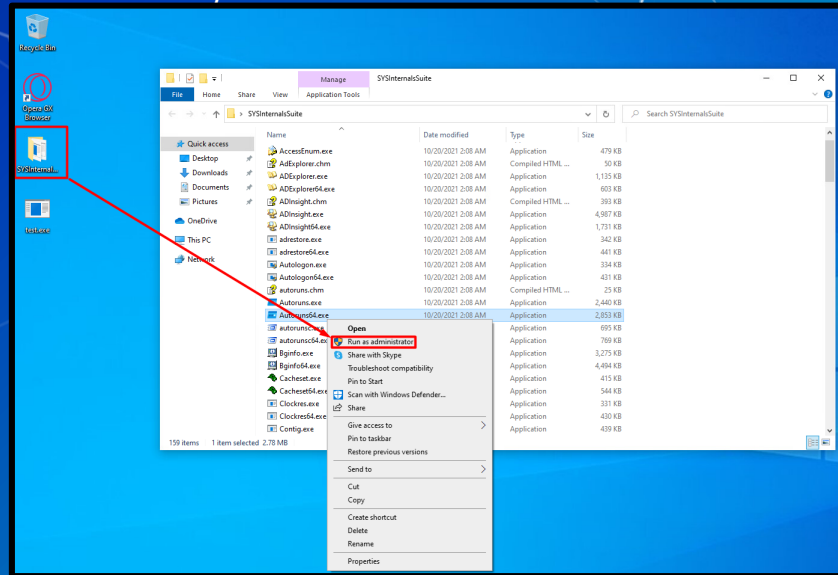
- Group policies can soften the security posture of a device
 - Disable anti-virus
 - Turn off or flood logs
 - Disable firewalls
 - And more!
- Group Policies can be used to establish registry based persistence
- Malicious group policies are very dangerous

Hands on 4 – Combatting Persistence

- Check services again
 - What do you notice?

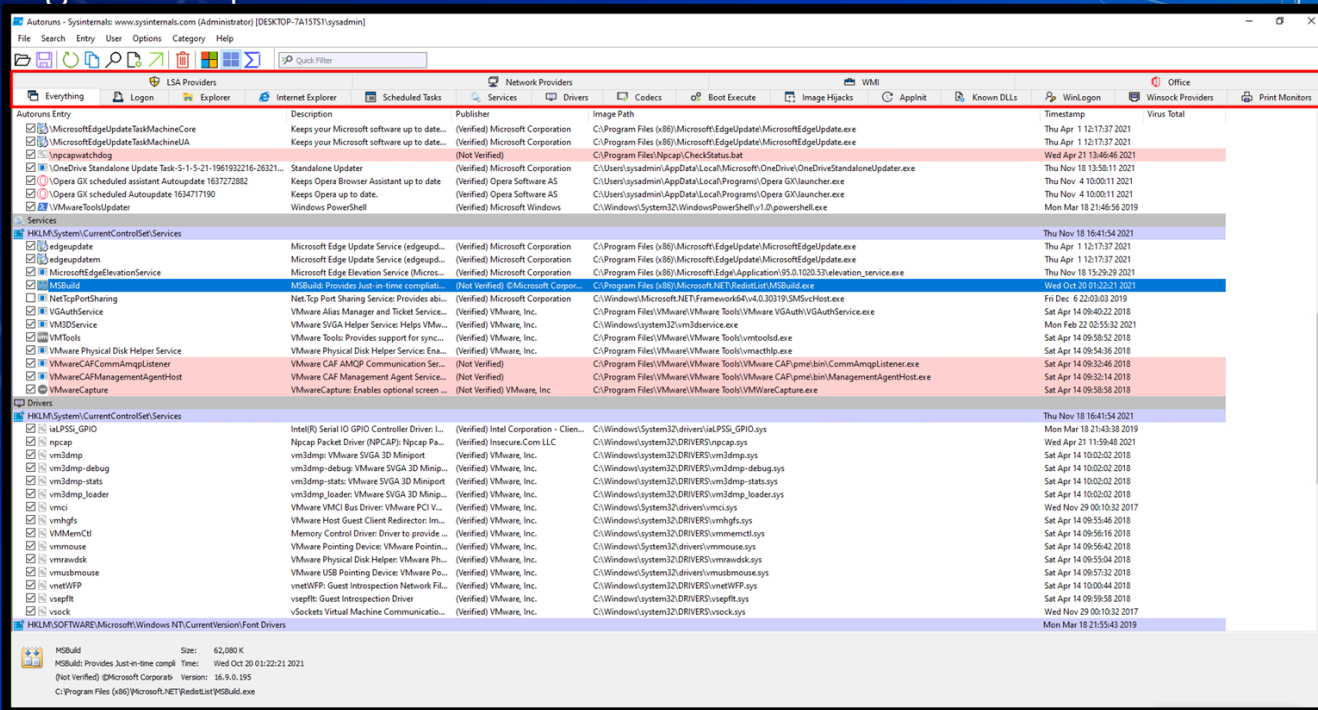
Hands on 4 – Combatting Persistence

- SysInternals is an open-source suite of tools for Windows
 - AutoRuns a tool to detect persistence
 - Run autoruns as Admin from the Sysinternals folder on your desktop



Hands on 4 – Combatting Persistence

Categories of persistence



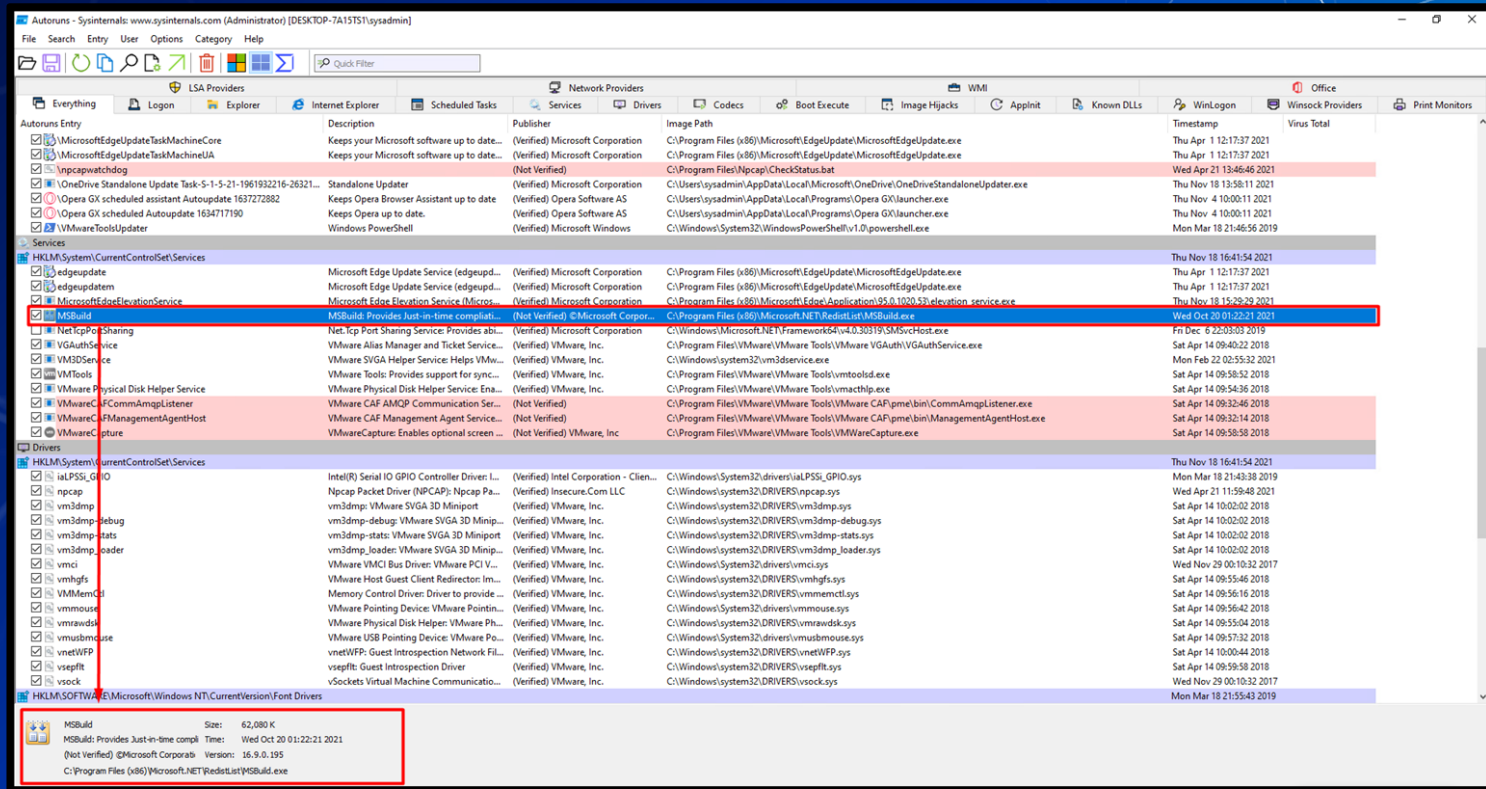
The screenshot shows the Sysinternals Autoruns application window. The interface is divided into several panes: 'Autoreun Entry', 'Services', and 'Drivers'. Each pane contains a list of system components with columns for Description, Publisher, Image Path, and Timestamp. The 'MSBuild' service is highlighted in blue, indicating it is selected. The 'Drivers' pane shows a list of device drivers, including 'Intel(R) Serial IO GPIO Controller Driver', 'Npcap Packet Driver', and 'VMware SVGA 3D Miniport'. The 'MSBuild' service details are shown at the bottom of the window.

Autoreun Entry	Description	Publisher	Image Path	Timestamp
<input checked="" type="checkbox"/> MicrosoftEdgeUpdateTaskMachineCore	Keeps your Microsoft software up to date...	(Verified) Microsoft Corporation	C:\Program Files (x86)\MicrosoftEdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021
<input checked="" type="checkbox"/> MicrosoftEdgeUpdateTaskMachineUA	Keeps your Microsoft software up to date...	(Verified) Microsoft Corporation	C:\Program Files (x86)\MicrosoftEdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021
<input checked="" type="checkbox"/> \OneDrive Standalone Update Task-5-1-5-21-1961932216-26321...	Standalone Updater	(Not Verified)	C:\Program Files\Npcap\CheckStatus.bat	Wed Apr 21 13:46:46 2021
<input checked="" type="checkbox"/> \OneDrive Standalone Update Task-5-1-5-21-1961932216-26321...	Standalone Updater	(Verified) Microsoft Corporation	C:\Users\sysadmin\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdate.exe	Thu Nov 18 13:58:11 2021
<input checked="" type="checkbox"/> Opera GX scheduled assistant Autoupdate 163727282	Keeps Opera Browser Assistant up to date	(Verified) Opera Software AS	C:\Users\sysadmin\AppData\Local\Programs\Opera GX\launcher.exe	Thu Nov 4 10:00:11 2021
<input checked="" type="checkbox"/> Opera GX scheduled Autoupdate 163477190	Keeps Opera up to date.	(Verified) Opera Software AS	C:\Users\sysadmin\AppData\Local\Programs\Opera GX\launcher.exe	Thu Nov 4 10:00:11 2021
<input checked="" type="checkbox"/> VMwareToolsUpdater	Windows PowerShell	(Verified) Microsoft Windows	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Mon Mar 18 21:46:56 2019

Services	Description	Publisher	Image Path	Timestamp
<input checked="" type="checkbox"/> HKLM\System\CurrentControlSet\Services\edgeupdate	Microsoft Edge Update Service (edgeupd...	(Verified) Microsoft Corporation	C:\Program Files (x86)\MicrosoftEdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021
<input checked="" type="checkbox"/> edgeupdate	Microsoft Edge Update Service (edgeupd...	(Verified) Microsoft Corporation	C:\Program Files (x86)\MicrosoftEdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021
<input checked="" type="checkbox"/> MicrosoftEdgeElevationService	Microsoft Edge Application (MSBuild) Provides Just-in-time compilati...	(Not Verified) Microsoft Corpora...	C:\Program Files (x86)\Microsoft.NET\Framework64\v4.0.30319\SMService.exe	Wed Oct 20 01:22:21 2021
<input checked="" type="checkbox"/> MSBuild	MSBuild Provides Just-in-time compilati...	(Not Verified) Microsoft Corpora...	C:\Program Files (x86)\Microsoft.NET\Framework64\v4.0.30319\SMService.exe	Wed Oct 20 01:22:21 2021
<input checked="" type="checkbox"/> NetTcpPortSharing	Net.Tcp Port Sharing Service: Provides ab...	(Verified) Microsoft Corporation	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMService.exe	Fri Dec 6 22:03:03 2019
<input checked="" type="checkbox"/> VGAuthService	VMware Alias Manager and Ticket Service...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\VMware VGAuthService.exe	Sat Apr 14 09:40:22 2018
<input checked="" type="checkbox"/> VM3DSvc	VMware SVGA Helper Service: Helps VMw...	(Verified) VMware, Inc.	C:\Windows\system32\vm3dservice.exe	Mon Feb 22 02:53:32 2021
<input checked="" type="checkbox"/> VMTools	VMware Tools: Provides support for sync...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Sat Apr 14 09:56:32 2018
<input checked="" type="checkbox"/> VMware Physical Disk Helper Service E...	VMware Physical Disk Helper Service: Ena...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmacthlp.exe	Sat Apr 14 09:56:32 2018
<input checked="" type="checkbox"/> VMwareCAFCommAnmpListener	VMware CAF AMCP Communication Ser...	(Not Verified)	C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin\CommAnmpListener.exe	Sat Apr 14 09:32:49 2018
<input checked="" type="checkbox"/> VMwareCAFManagementAgentHost	VMware CAF Management Agent Service...	(Not Verified)	C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin\ManagementAgentHost.exe	Sat Apr 14 09:32:14 2018
<input checked="" type="checkbox"/> VMwareCapture	VMware Capture: Enables optional screen...	(Not Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\VMwareCapture.exe	Sat Apr 14 09:58:58 2018

Drivers	Description	Publisher	Image Path	Timestamp
<input checked="" type="checkbox"/> HKLM\System\CurrentControlSet\Services\iHPSS\GPIO	Intel(R) Serial IO GPIO Controller Driver: L...	(Verified) Intel Corporation - Clien...	C:\Windows\System32\drivers\iHPSS_GPIO.sys	Thu Nov 18 16:41:54 2021
<input checked="" type="checkbox"/> iHPSS\GPIO	Intel(R) Serial IO GPIO Controller Driver: L...	(Verified) Intel Corporation - Clien...	C:\Windows\System32\drivers\iHPSS_GPIO.sys	Mon Mar 18 21:43:38 2019
<input checked="" type="checkbox"/> npcap	Npcap Packet Driver (NPcap): Npcap Pa...	(Verified) Insecure.Com LLC	C:\Windows\system32\DRIVERS\npcap.sys	Wed Apr 21 11:59:40 2021
<input checked="" type="checkbox"/> vm3dmp	VMware SVGA 3D Miniport	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vm3dmp.sys	Sat Apr 14 10:02:02 2018
<input checked="" type="checkbox"/> vm3dmp-debug	vm3dmp-debug: VMware SVGA 3D Minip...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vm3dmp-debug.sys	Sat Apr 14 10:02:02 2018
<input checked="" type="checkbox"/> vm3dmp-status	vm3dmp-status: VMware SVGA 3D Minip...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vm3dmp-status.sys	Sat Apr 14 10:02:02 2018
<input checked="" type="checkbox"/> vm3dmp_loader	vm3dmp_loader: VMware SVGA 3D Minip...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vm3dmp_loader.sys	Sat Apr 14 10:02:02 2018
<input checked="" type="checkbox"/> vmci	VMware VMCI Bus Driver: VMware PCI V...	(Verified) VMware, Inc.	C:\Windows\System32\drivers\vmci.sys	Wed Nov 29 00:10:32 2017
<input checked="" type="checkbox"/> vmhgfs	VMware Host Guest Client Redirector: Im...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmhgfs.sys	Sat Apr 14 09:55:46 2018
<input checked="" type="checkbox"/> VMMemCtl	Memory Control Driver: Driver to provide...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmmemctl.sys	Sat Apr 14 09:56:16 2018
<input checked="" type="checkbox"/> vmmouse	VMware Pointing Device: VMware Point...	(Verified) VMware, Inc.	C:\Windows\system32\drivers\vmmouse.sys	Sat Apr 14 09:56:42 2018
<input checked="" type="checkbox"/> vmrawdsk	VMware Physical Disk Helper: VMware Ph...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmrawdsk.sys	Sat Apr 14 09:55:04 2018
<input checked="" type="checkbox"/> vmusbmouse	VMware USB Pointing Device: VMware P...	(Verified) VMware, Inc.	C:\Windows\System32\drivers\vmusbmouse.sys	Sat Apr 14 09:57:32 2018
<input checked="" type="checkbox"/> vnetWFP	vnetWFP: Guest Interception Network Fil...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vnetWFP.sys	Sat Apr 14 10:00:44 2018
<input checked="" type="checkbox"/> vspfltd	vspfltd: Guest Interception Driver	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vspfltd.sys	Sat Apr 14 09:59:58 2018
<input checked="" type="checkbox"/> vsock	\Sockets Virtual Machine Communicatio...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vsock.sys	Wed Nov 29 00:10:32 2017

Hands on 4 – Combatting Persistence



The screenshot shows the Windows Task Scheduler interface. The 'MSBuild' service is highlighted with a red box. Below the main list, a detailed view of the MSBuild task is shown, also highlighted with a red box.

Task Name	Description	Publisher	Image Path	Timestamp
MicrosoftEdgeUpdateTaskMachineCore	Keeps your Microsoft software up to date...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021
MicrosoftEdgeUpdateTaskMachineUA	Keeps your Microsoft software up to date...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021
npcapwatchdog		(Not Verified)	C:\Program Files\Npcap\CheckStatus.bat	Wed Apr 21 13:46:46 2021
OneDrive Standalone Update Task-S-1-5-21-1961932216-26321...	Standalone Updater	(Verified) Microsoft Corporation	C:\Users\sysadmin\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe	Thu Nov 18 13:58:11 2021
Opera GX scheduled assistant Autoupdate 163727282	Keeps Opera Browser Assistant up to date	(Verified) Opera Software AS	C:\Users\sysadmin\AppData\Local\Programs\Opera GX\launcher.exe	Thu Nov 4 10:00:11 2021
Opera GX scheduled Autoupdate 1634717190	Keeps Opera up to date.	(Verified) Opera Software AS	C:\Users\sysadmin\AppData\Local\Programs\Opera GX\launcher.exe	Thu Nov 4 10:00:11 2021
VMwareToolsUpdater	Windows PowerShell	(Verified) Microsoft Windows	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Mon Mar 18 21:46:56 2019
edgeupdate	Microsoft Edge Update Service (edgeup...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Nov 18 16:41:54 2021
edgeupdateam	Microsoft Edge Update Service (edgeup...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021
MicrosoftEdgeElevationService	Microsoft Edge Elevation Service (Micro...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\95.0.1020.53\elevation_service.exe	Thu Nov 18 15:28:29 2021
MSBuild	MSBuild: Provides Just-in-time complia...	(Not Verified) ©Microsoft Corpora...	C:\Program Files (x86)\Microsoft.NET\RedistList\MSBuild.exe	Wed Oct 20 01:22:21 2021
Net.Lsp.Sharing	Net.Lsp.Sharing Service: Provides ab...	(Verified) Microsoft Corporation	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMsvchost.exe	Fri Dec 6 22:03:03 2019
VGAuthService	VMware Allas Manager and Ticket Service...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware\VMware VGuard\VGAuthService.exe	Sat Apr 14 09:40:22 2018
VM3DService	VMware SVGA Helper Service: Helps VMw...	(Verified) VMware, Inc.	C:\Windows\system32\vm3dservice.exe	Mon Feb 22 02:55:32 2021
VMTools	VMware Tools: Provides support for sync...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware\vmtoolsd.exe	Sat Apr 14 09:58:52 2018
VMware Physical Disk Helper Service	VMware Physical Disk Helper Service: Ena...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware\Tools\vmacthlp.exe	Sat Apr 14 09:54:36 2018
VMware CAF AMQP Communication Ser...	VMware CAF AMQP Communication Ser...	(Not Verified)	C:\Program Files\VMware\VMware\Tools\gme\bin\CommAmqpListener.exe	Sat Apr 14 09:56:46 2018
VMware CAF ManagementAgentHost	VMware CAF Management Agent Service...	(Not Verified)	C:\Program Files\VMware\VMware\Tools\VMware CAF\gme\bin\ManagementAgentHost.exe	Sat Apr 14 09:32:14 2018
VMwareCapture	VMwareCapture: Enables optional screen...	(Not Verified) VMware, Inc	C:\Program Files\VMware\VMware\Tools\VMWareCapture.exe	Sat Apr 14 09:58:58 2018
lspss_gpio	Intel(R) Serial IO GPIO Controller Drive...	(Verified) Intel Corporation - Clien...	C:\Windows\System32\drivers\lspss_gpio.sys	Mon Mar 18 21:43:38 2019
npcap	Npcap Packet Driver (NPCAP): Npcap Pa...	(Verified) Insecure.Com LLC	C:\Windows\system32\DRIVERS\npcap.sys	Wed Apr 21 11:59:48 2021
vm3dmp	vm3dmp: VMware SVGA 3D Miniport...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vm3dmp.sys	Sat Apr 14 10:00:02 2018
vm3dmp-debug	vm3dmp-debug: VMware SVGA 3D Minip...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vm3dmp-debug.sys	Sat Apr 14 10:00:02 2018
vm3dmp-stats	vm3dmp-stats: VMware SVGA 3D Miniport...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vm3dmp-stats.sys	Sat Apr 14 10:00:02 2018
vm3dmp_loader	vm3dmp_loader: VMware SVGA 3D Minip...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vm3dmp_loader.sys	Sat Apr 14 10:00:02 2018
vmcvi	VMware VMCi Bus Driver: VMware PCI V...	(Verified) VMware, Inc.	C:\Windows\System32\drivers\vmcvi.sys	Wed Nov 29 00:10:32 2017
vmhfsfs	VMware Host Guest Client Redirector: Im...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmhfs.sys	Sat Apr 14 09:56:46 2018
VMmemctl	Memory Control Driver: Driver to provide...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmmemctl.sys	Sat Apr 14 09:56:16 2018
vmmouse	VMware Pointing Device: VMware Pointin...	(Verified) VMware, Inc.	C:\Windows\System32\drivers\vmmouse.sys	Sat Apr 14 09:56:42 2018
vsrandsd	VMware Physical Disk Helper: VMware Ph...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmrawdsk.sys	Sat Apr 14 09:55:04 2018
vmusbmouse	VMware USB Pointing Device: VMware Po...	(Verified) VMware, Inc.	C:\Windows\System32\drivers\vmusbmouse.sys	Sat Apr 14 09:57:32 2018
vnetWFP	vnetWFP: Guest Inspection Network Fil...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vnetWFP.sys	Sat Apr 14 10:00:44 2018
vseffit	vseffit: Guest Inspection Driver	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vseffit.sys	Sat Apr 14 09:59:58 2018
vssock	vsockets Virtual Machine Communicatio...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vssock.sys	Wed Nov 29 00:10:32 2017

MSBuild Size: 62,080 K
MSBuild: Provides Just-in-time compli... Time: Wed Oct 20 01:22:21 2021
(Not Verified) ©Microsoft Corpora... Version: 16.3.0.195
C:\Program Files (x86)\Microsoft.NET\RedistList\MSBuild.exe

Hands on 4 – Combatting Persistence

- Find and remove the item that is allowing the <REDACTED> to persist
 - Hint: It is not a GroupPolicy, PowerShell Profile, Driver, Image File Execution Option or Startup Object
- After you have removed the persistence
 - Stop the service using task manager
 - Delete the <REDACTED> using <REDACTED>
- Restart the computer
 - Is the service gone?

Homework Links

- Persistence – Image File Execution Options Injection
 - <https://pentestlab.blog/2020/01/13/persistence-image-file-execution-options-injection/>
- Windows Security Log Event IDs
 - <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx>
- Windows Sysinternals
 - <https://docs.microsoft.com/en-us/sysinternals/>

Additional Resources

- Abusing Windows Management Instrumentation (Black Hat)

- <https://tinyurl.com/a7jzmsc>
- <https://www.youtube.com/watch?v=0SjMgnGwpq8>

- Revoke-Obfuscation: PowerShell Obfuscation Detection (Black hat)

- <https://www.youtube.com/watch?v=x97ejtv56xw>

- PowerShell Documentation

- <https://docs.microsoft.com/en-us/powershell/>

Questions?