

Windows Threat Hunting

UBNetDef, Spring 2023
Week 6

Presenter:
Anthony Magrene & Griffin Refol

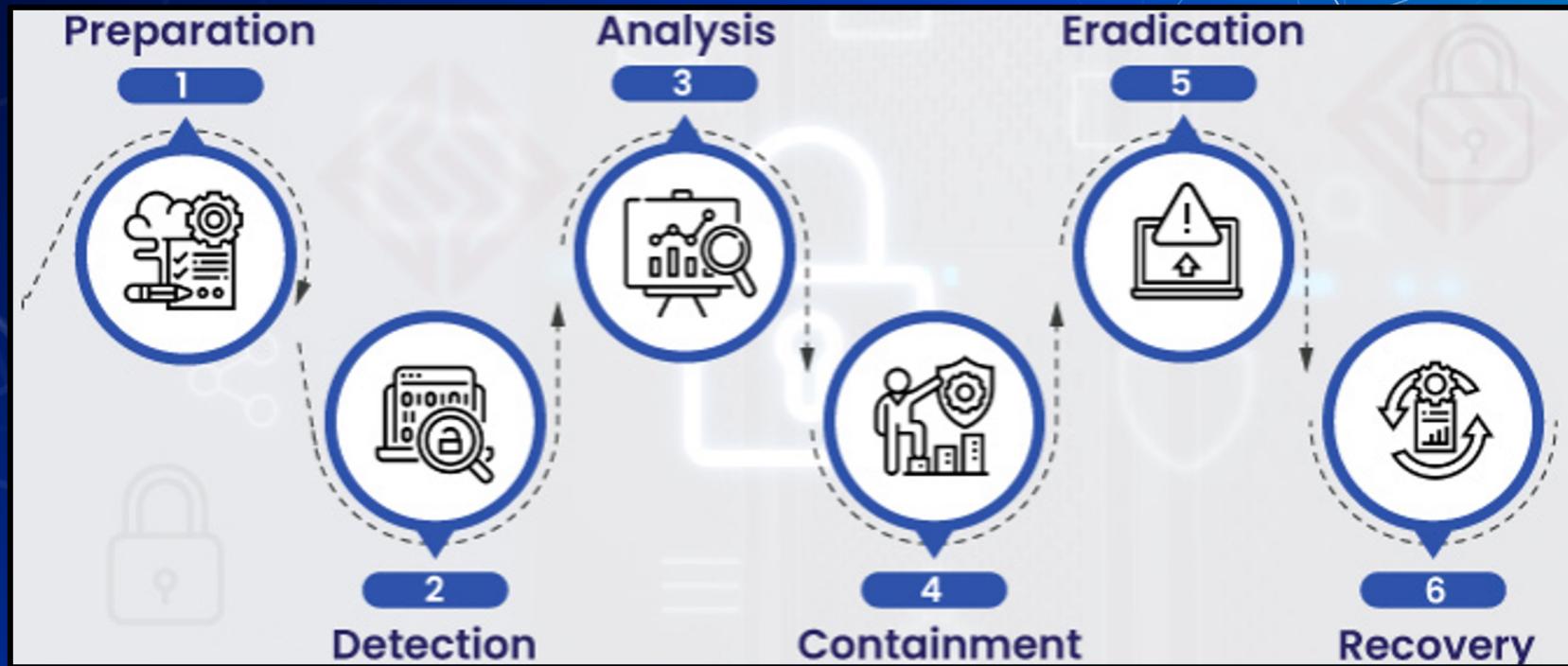


Agenda – Week 6

- 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
aadauthhelper.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
AcGeneral.dll	10/23/2020 3:20 PM	Application exten...	362 KB
AcLayers.dll	12/11/2020 6:14 PM	Application exten...	319 KB
acredit.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
acproxy.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.

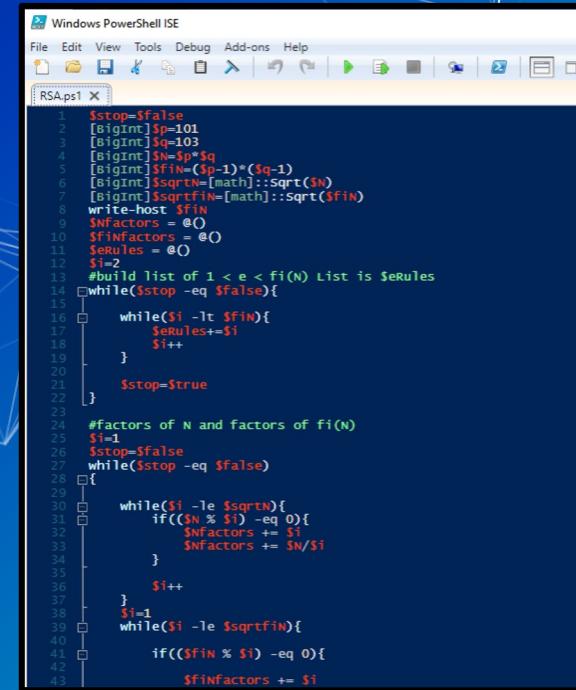
```
HxD - [C:\Windows\notepad.exe]
File Edit Search View Analysis Tools Window Help
16 Windows (ANSI) hex
notepad.exe

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 HZ SA 00 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....yy
00000010 B8 00 00 00 00 00 00 40 00 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 00 00 00 00 .....@.
00000040 41 F1 BA 0E 00 04 09 CD 21 B1 01 4C CD 21 54 68 ..!..L1!.
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6F is program cann
00000060 74 20 65 65 20 72 75 6E 24 65 20 44 4F 53 20 ..TEEP:;P:>:P
00000070 6D 6F 64 65 2E 0D 0A 24 00 00 00 00 00 00 00 00 t be run in DOS
mode...$,.
00000080 14 D9 D4 CA 58 B0 8A 3B 9A 5B 83 9A 5B 80 3A 9B YAE->.:DÖ:SZ;
00000090 59 C0 A9 BB 7B 7B 8A 9B 44 D3 3E 9A 5B 8A 3A 9B
000000A0 44 D3 3B 5A 53 8A 3B 9B 44 D3 3B 9A 59 B3 3A 9B DÖ:SZ;.:DÖ:SZ;
000000B0 58 BB 3B 9B 7C 3D 5A 9B 44 D3 32 9A 4E BB 3A 9B P;,>:M:DÖ:SZN;
000000C0 44 D3 3F 9A 71 8A 3B 9B 44 D3 7C 91 51 BB 3A 9B DÖ:SZ;.:DÖ:SZ;
000000D0 44 D3 C5 9B 51 8A 3B 9A 44 D3 38 91 51 BB 3A 9B DÖ:Q,:DÖ:SQ;
000000E0 52 E9 63 68 50 B8 3A 9B 00 00 00 00 00 00 00 00 RichP;:>:P
000000F0 00 00 00 00 00 00 00 50 45 00 00 64 86 07 00 ..PE.dF
00000100 69 BD FC 86 00 00 00 00 00 00 00 F0 00 22 00 iHd!..@.
00000110 0B 02 OE 14 0A 02 00 00 E2 00 00 00 00 00 00 00 .....J..å.
00000120 B0 3D 02 00 00 10 00 00 00 00 00 40 01 00 00 00 =@.....@.
00000130 00 10 00 00 02 00 00 00 00 OA 00 00 00 OA 00 00 00 .....€.
00000140 0A 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 00 .....€.
00000150 B0 EB 03 02 00 60 C1 00 00 08 00 00 00 00 00 00 %K...A...
00000160 00 10 01 00 00 00 00 00 00 00 00 10 00 00 00 00 .....A.
00000170 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00 .....A.
00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....O..O.
00000190 60 03 00 00 D8 00 00 00 00 30 03 00 28 11 00 00 ..Ø..Ø..Ø.
000001A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 p.Ø.
000001B0 50 AD 02 00 54 00 00 00 00 00 00 00 00 00 00 00 P..T.
000001C0 00 00 00 00 00 00 00 00 00 B8 67 02 00 28 00 00 00 g..!
```



PowerShell Script (.ps1)

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

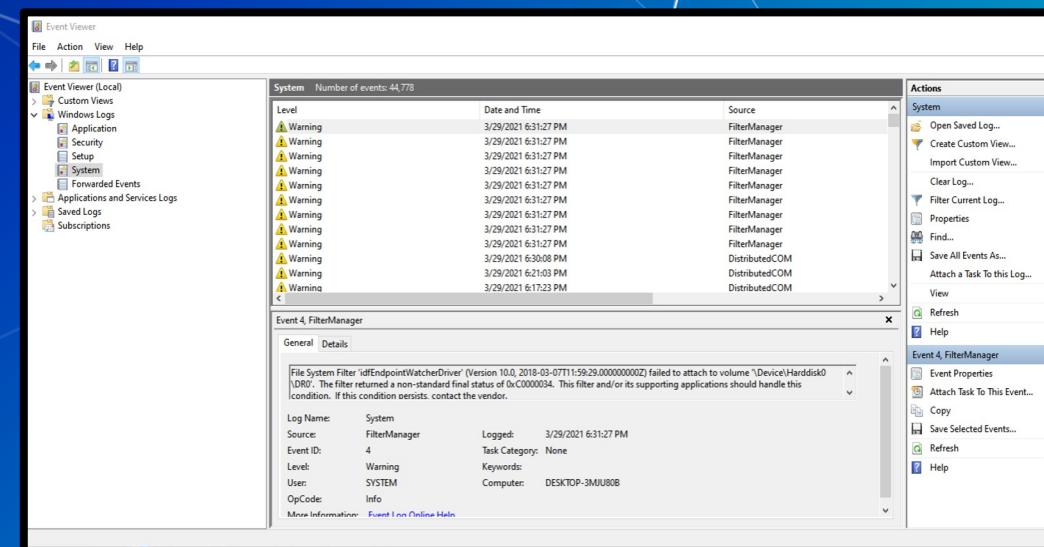


The screenshot shows the Windows PowerShell Integrated Scripting Environment (ISE) window titled "RSA.ps1". The code in the editor is a PowerShell script for generating RSA key pairs. It uses the [math]::sqrt function from .NET to calculate square roots and loops to find factors of N and its totient.

```
$stop=$false
$N=101
$N=$N*$N
$fin=(($N-1)*($N-1))
$sqrtN=[math]::sqrt($N)
$sqrtFin=[math]::sqrt($fin)
write-host $fin
$nfactors = @()
$rules = @()
$i=2
#build list of 1 < e < fi(N) List is $rules
while($stop -eq $false){
    while($i -lt $fin){
        $rules+=$i
        $i++
    }
    $stop=$true
}
#factors of N and factors of fi(N)
$i=1
$stop=$false
while($stop -eq $false){
    while($i -le $sqrtN){
        if($N % $i) -eq 0{
            $nfactors += $i
            $nfactors += $N/$i
        }
        $i++
    }
    $i=1
    while($i -le $sqrtfin){
        if($fin % $i) -eq 0{
            $finfactors += $i
        }
        $i++
    }
}
```

Event Log (.evtx)

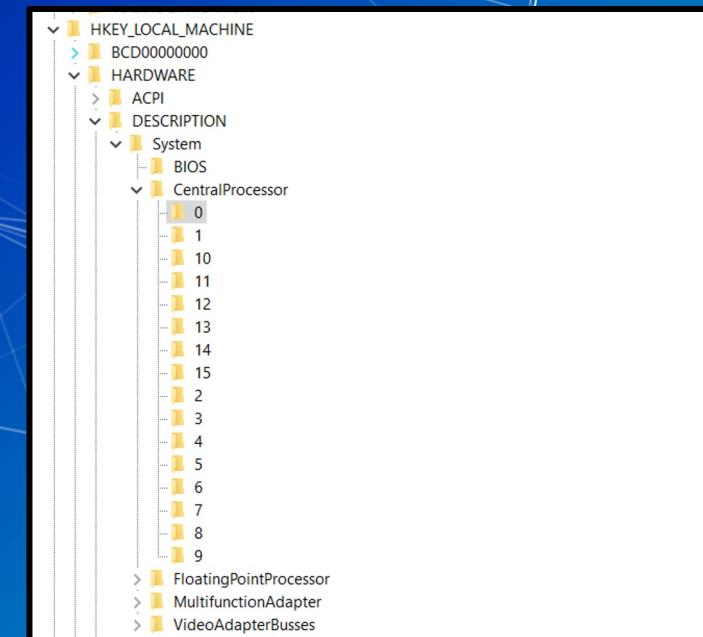
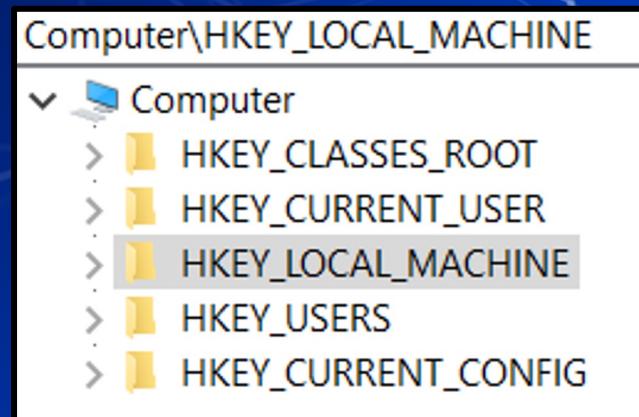
- Stores Windows Logs
 - Located C:\Windows\System32\winevt\Logs\
 - Event viewer used to view logs



The Registry

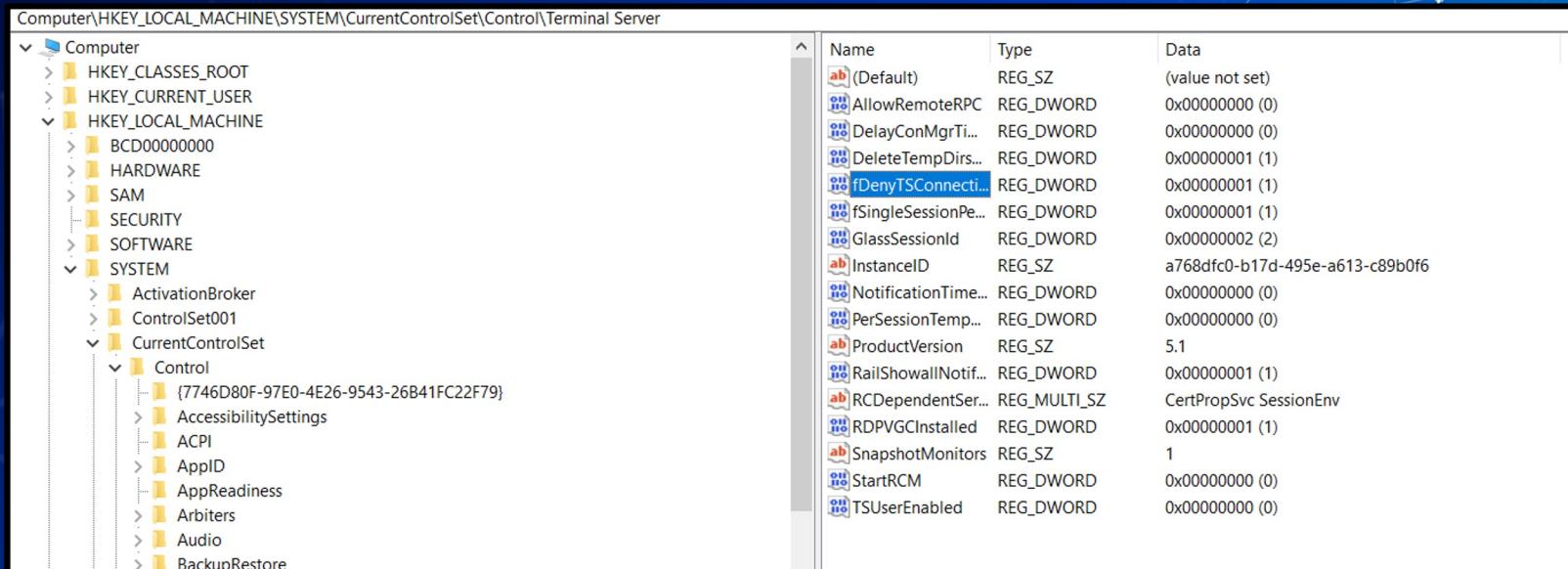
Registry

- Hierarchical database
 - Stores low-level settings



Registry cont.

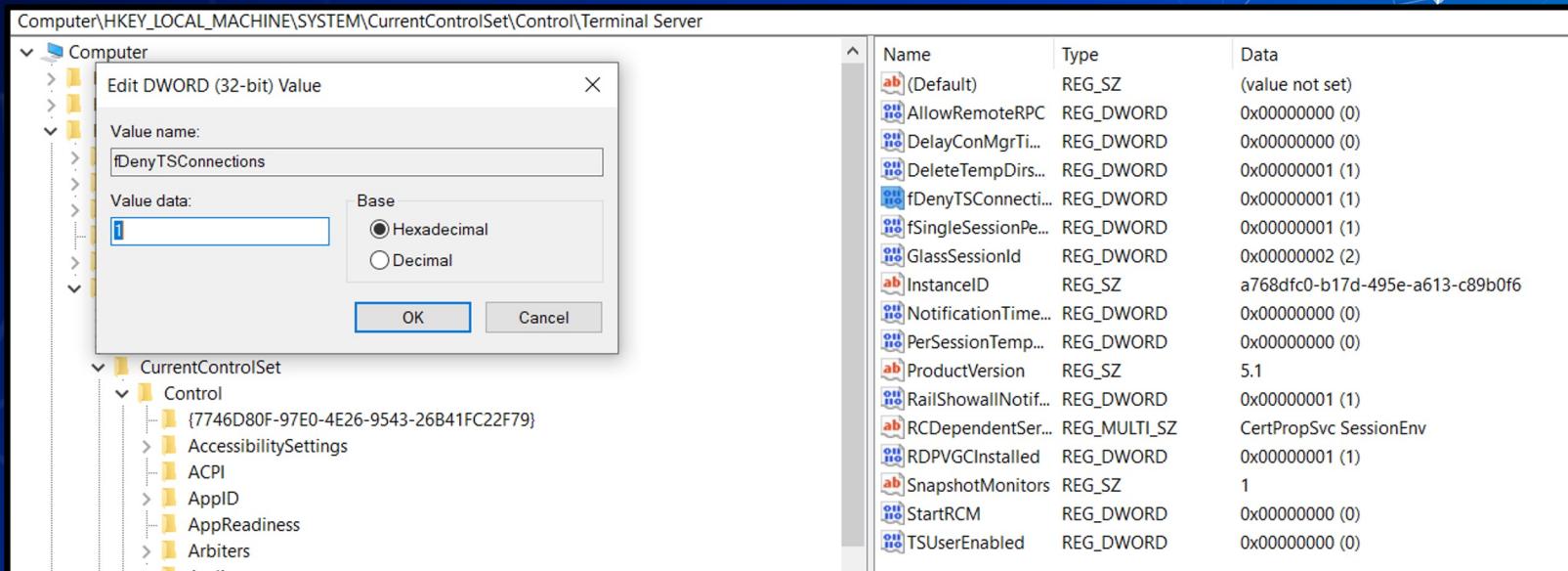
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server



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
RailShowwallNotif...	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



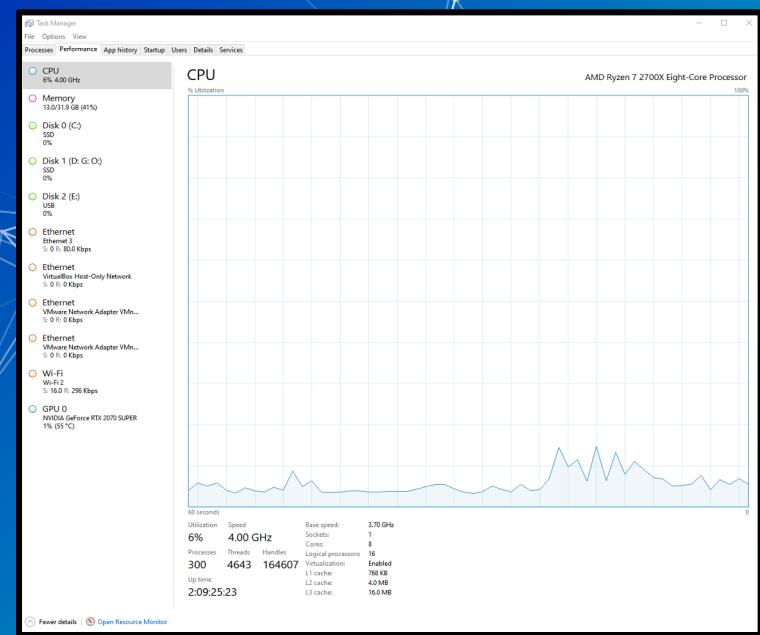
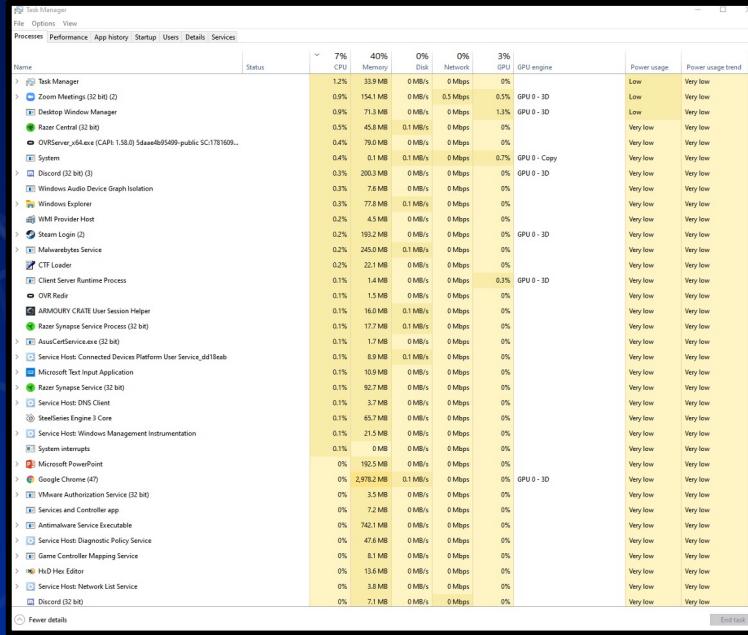
The screenshot shows the Windows Registry Editor interface. On the left, the navigation pane displays the registry path: Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server. A context menu is open over the 'fDenyTSConnections' key, with the option 'Edit DWORD (32-bit) Value' selected. In the center, a dialog box titled 'Edit DWORD (32-bit) Value' shows the current value name as 'fDenyTSConnections' and the value data as '1'. The 'Base' dropdown is set to 'Hexadecimal'. At the bottom of the dialog are 'OK' and 'Cancel' buttons. On the right, the main pane lists various registry keys under the 'Control' subkey, each with its name, type, and data value. The 'fDenyTSConnections' key is listed with a value of 1.

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
RailShowWallNotif...	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

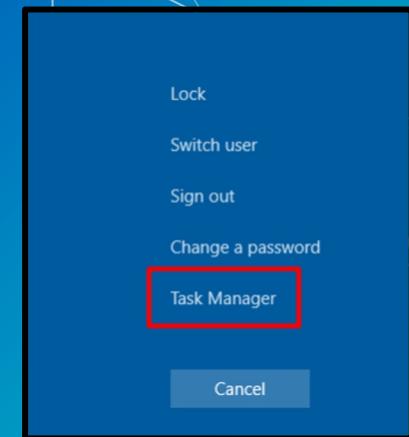
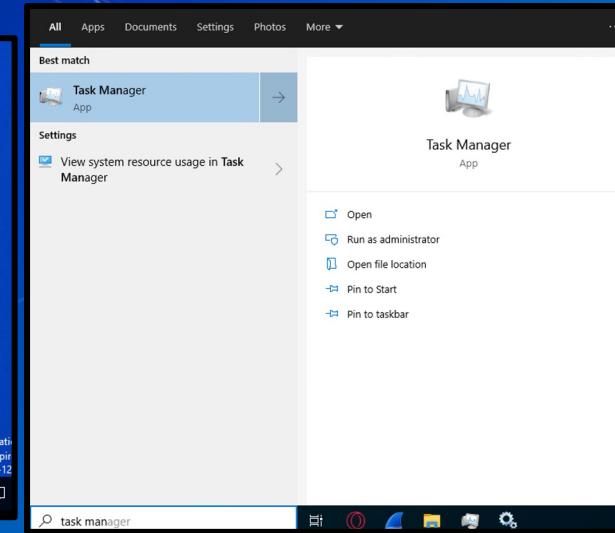
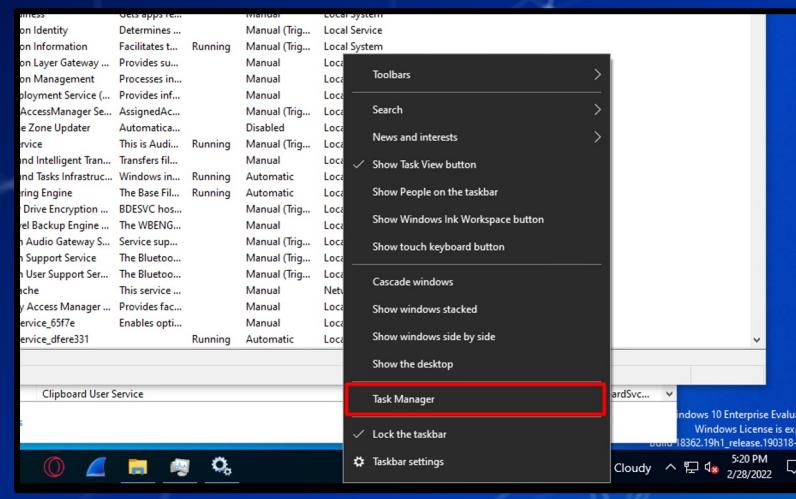
Task Manager

Provides high-level view of what is running



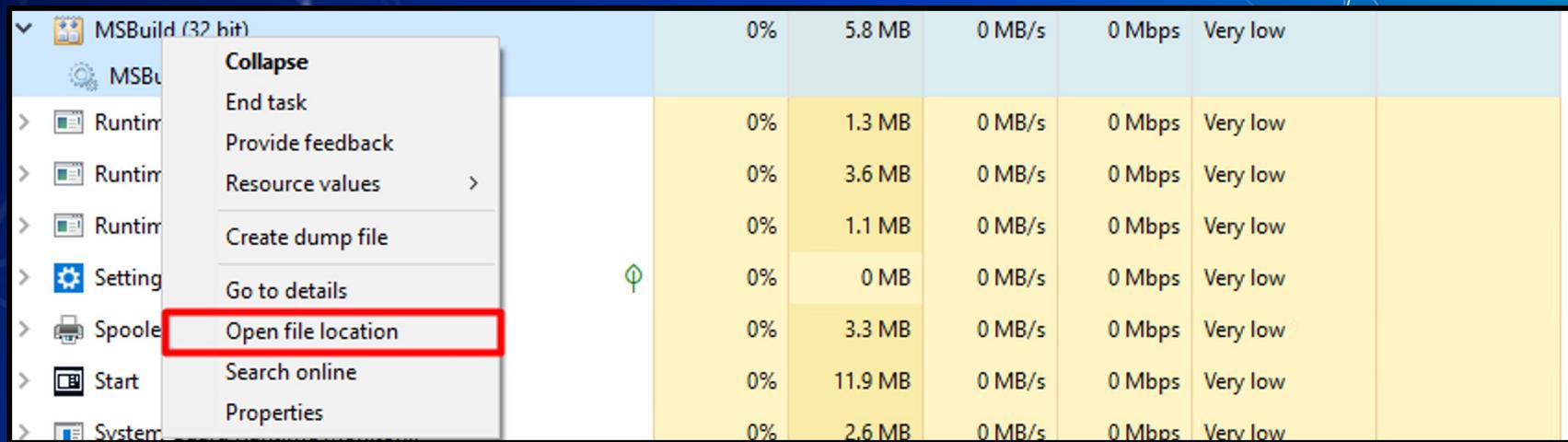
Task Manager cont.

How to open it?



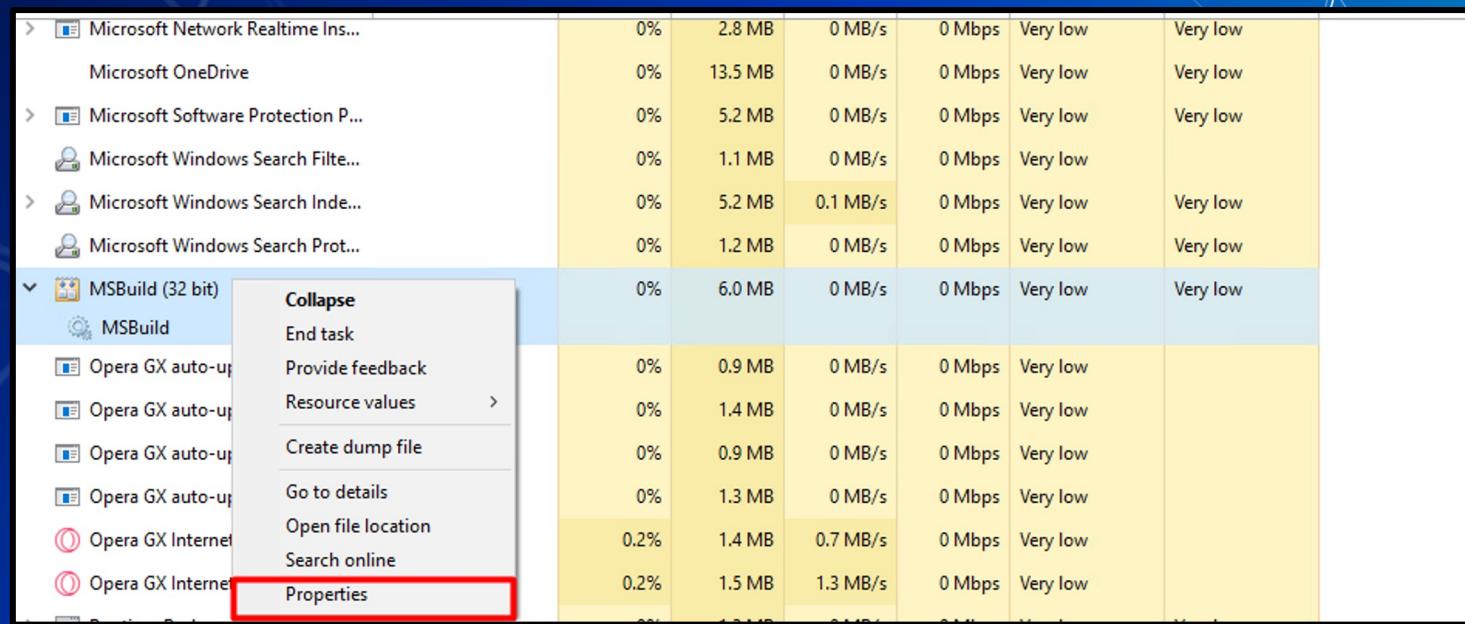
Task Manager cont.

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

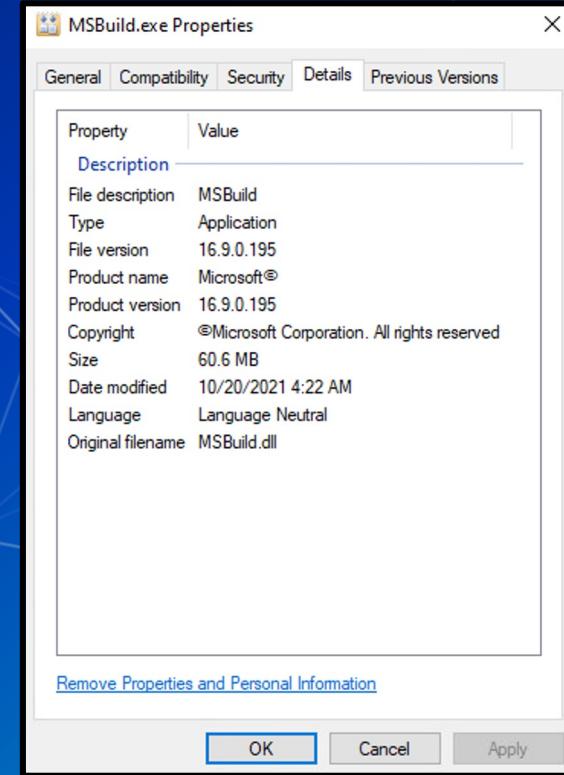
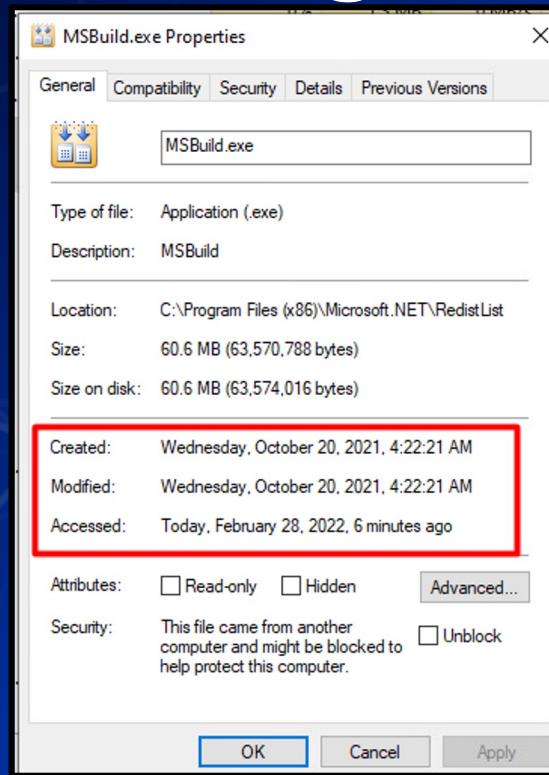


Task Manager cont.

- Show the properties of an executable



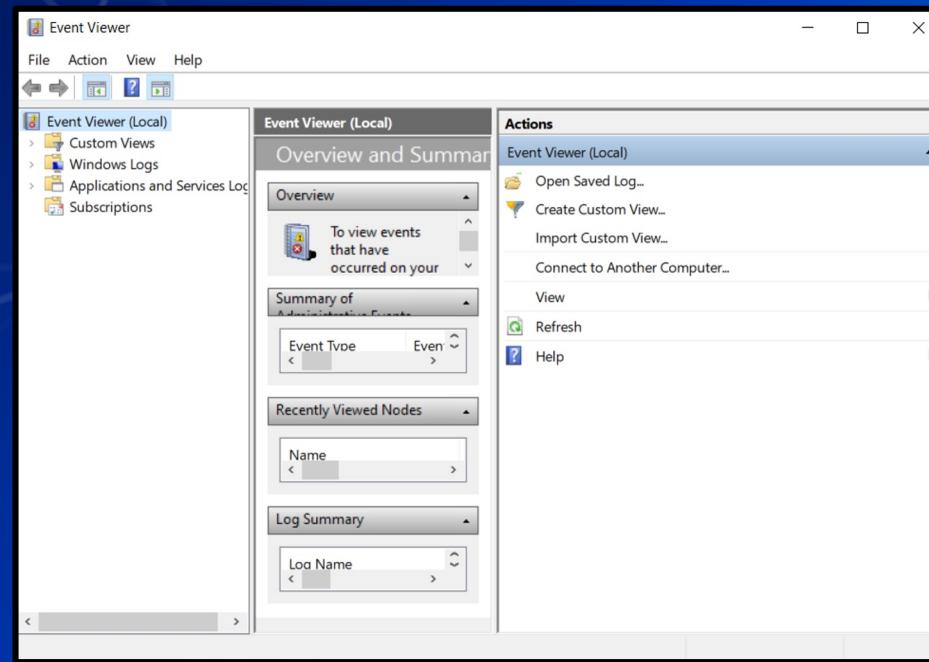
Task Manager cont.



Event Viewer

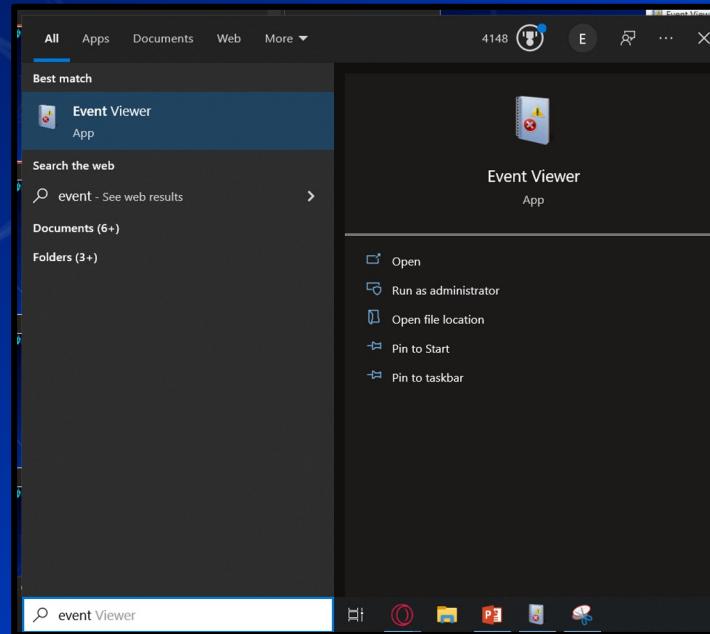
Event Viewer

■ Log viewer for Windows



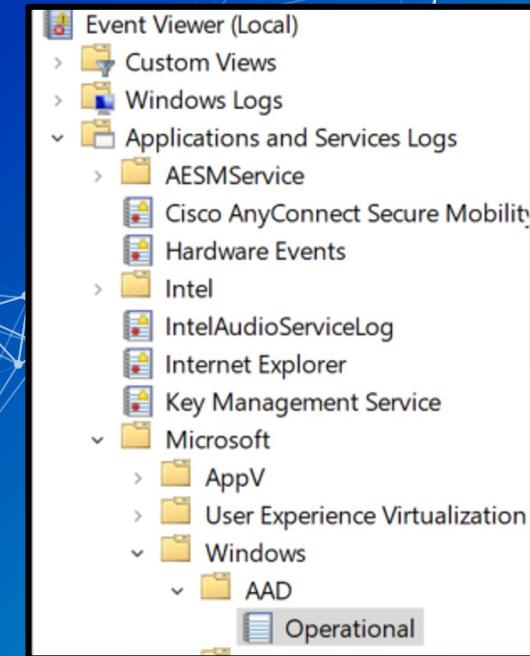
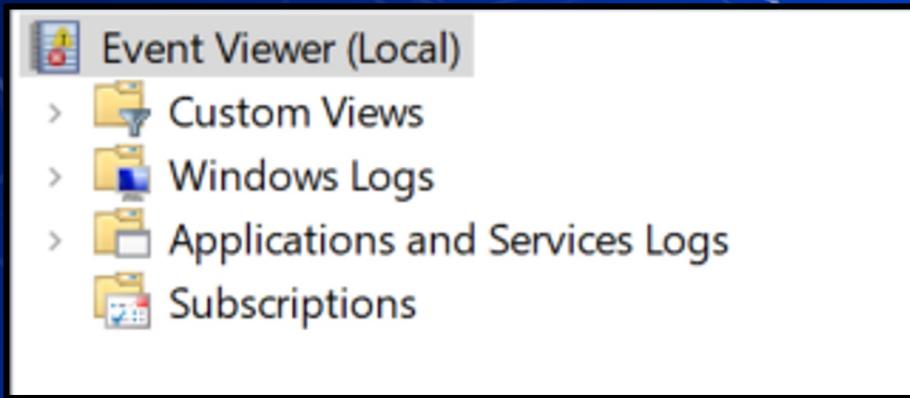
Event Viewer

- Can be opened by searching for "event" and clicking open



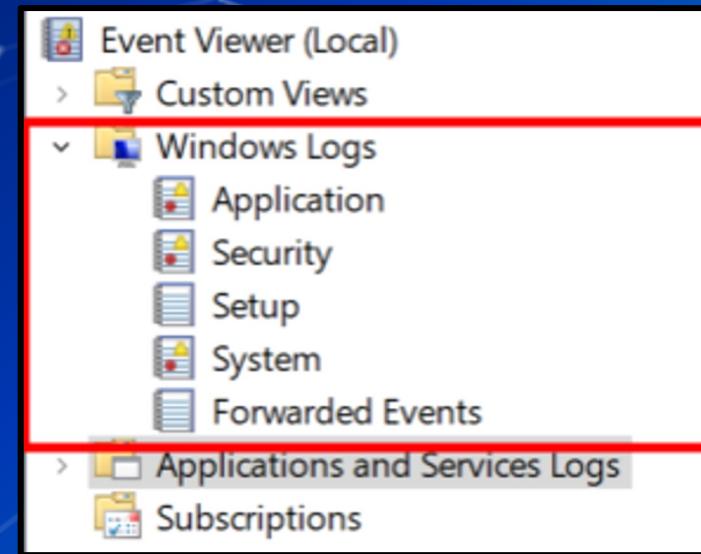
Event Viewer cont.

- Logs are stored in a hierarchical structure



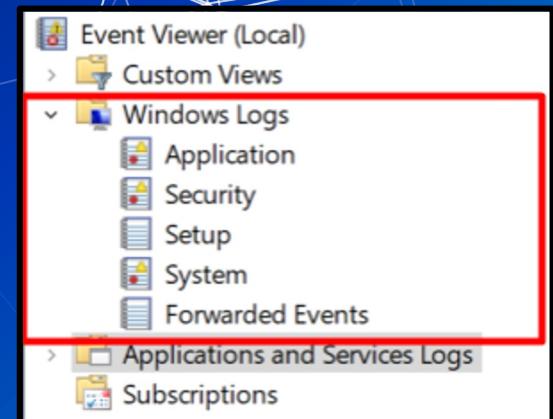
Event Viewer cont.

- 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

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	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.



Security Log | Windows | SharePoint | SQL Server | Exchange | Training | Tools | Webinars | Blog | Forum

Webinars Training Encyclopedia Quick Reference Book

Windows Security Log Events

Go To Event ID: 4624 Go

Encyclopedia

- All Event IDs
- Audit Policy

Windows Audit

- All Sources
- Windows Audit
- SharePoint Audit (LOGbinder for SharePoint)
- SQL Server Audit (LOGbinder for SQL Server)
- Exchange Audit (LOGbinder for Exchange)
- Sysmon (MS Sysinternals Sysmon)

Windows Audit Categories: All categories Subcategories: All subcategories

Windows Versions: All events Win2000, XP and Win2003 only Win2008, Win2012R2, Win2016 and Win10+, Win2019



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

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
• Subcategory
Logon/Logoff

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 (!) 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-2LN9C412\$
Account Domain:	WORKGROUP
Logon ID:	0x3E7

Logon Information:

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

Impersonation Level:

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

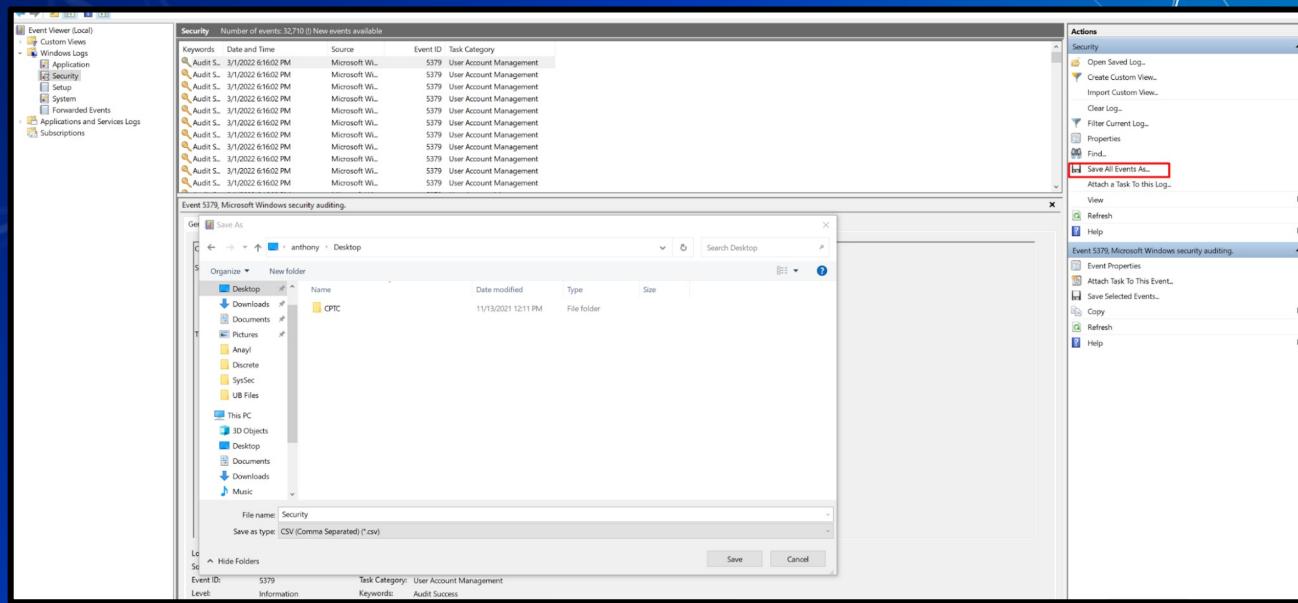
Network Information:

Log Name:	Security
Source:	Microsoft Windows security
Event ID:	4624
Level:	Information
User:	N/A
OpCode:	Info
Keywords:	Audit Success
Computer:	LAPTOP-2LN9C412

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

Event Viewer cont.

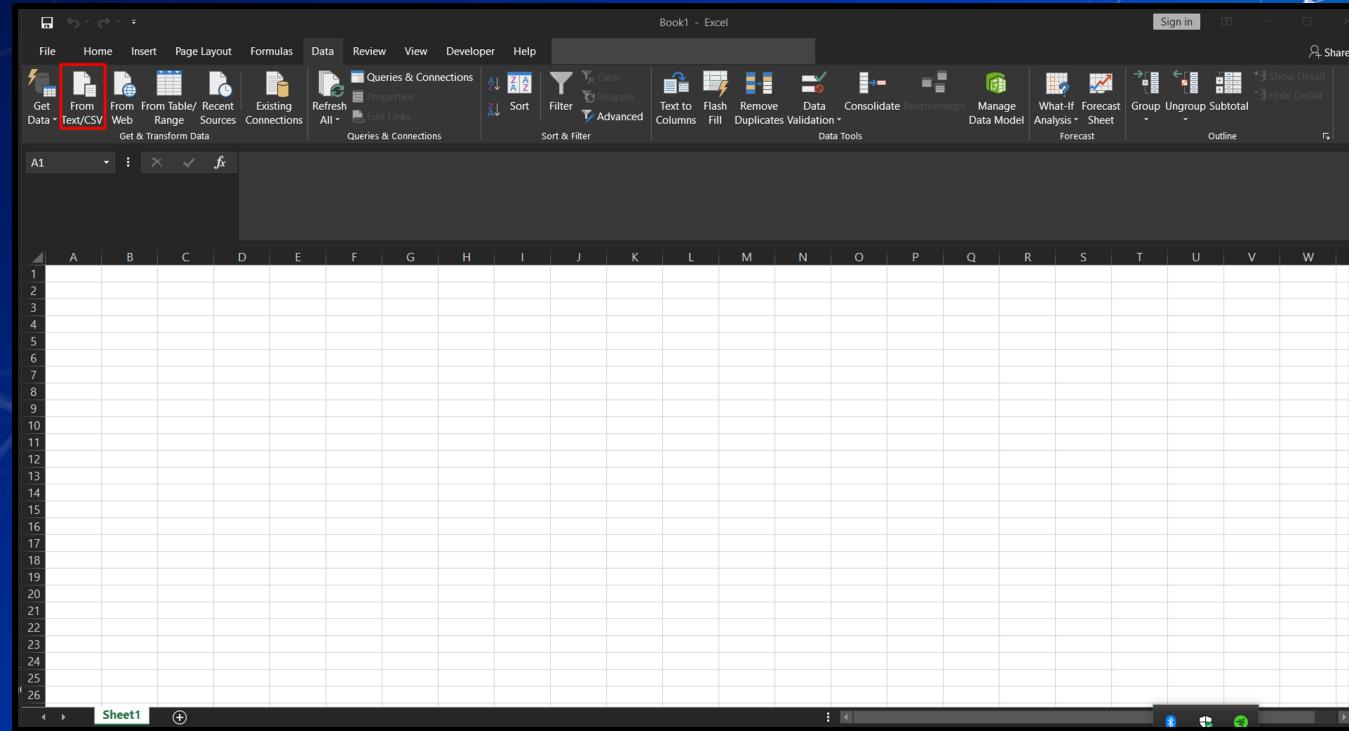
- Event viewer sucks when trying to search logs in bulk.
- We can extract logs to a CSV file



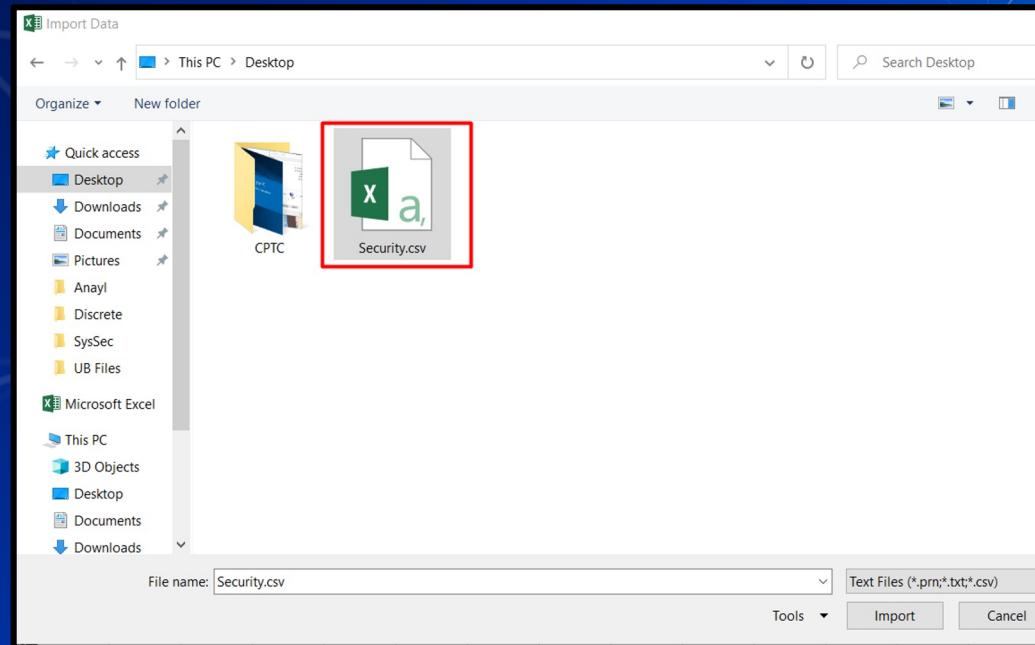
Event Viewer cont.

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

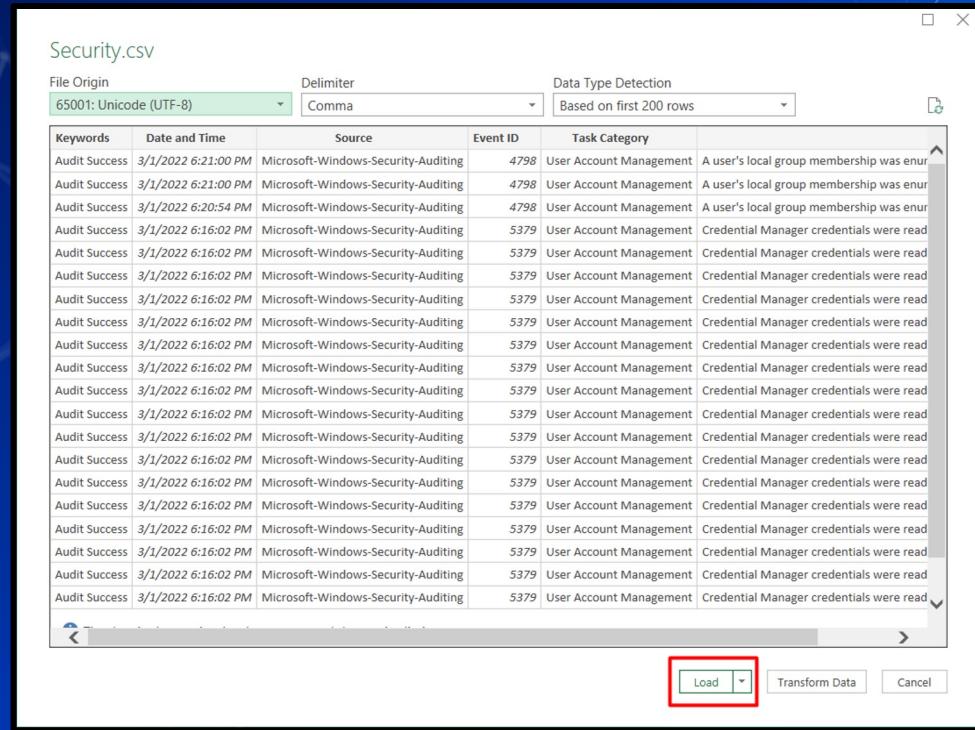
Importing Logs in Excel



Importing Logs in Excel



Importing Logs in Excel





Logs in Excel

Logs in Excel

Within Excel we can search logs using filters.

A	B	C	D	E	F	
1	Keywords	Date and Time	Source	Event ID	Task Category	Column1
2	Audit Success	3/1/2022 18:21 Microsoft	Sort Smallest to Largest	5379	User Account Management	A user's local group membership was enumerated.
3	Audit Success	3/1/2022 18:21 Microsoft	Sort Largest to Smallest	5379	User Account Management	A user's local group membership was enumerated.
4	Audit Success	3/1/2022 18:20 Microsoft	Sort by Color	5379	User Account Management	A user's local group membership was enumerated.
5	Audit Success	3/1/2022 18:16 Microsoft	Clear Filter From "Event ID"	5379	User Account Management	Credential Manager credentials were read.
6	Audit Success	3/1/2022 18:16 Microsoft	Filter by Color	5379	User Account Management	Credential Manager credentials were read.
7	Audit Success	3/1/2022 18:16 Microsoft	Number Filters	5379	User Account Management	Credential Manager credentials were read.
8	Audit Success	3/1/2022 18:16 Microsoft	Search	5379	User Account Management	Credential Manager credentials were read.
9	Audit Success	3/1/2022 18:16 Microsoft	<input type="checkbox"/> (Select All)	5379	User Account Management	Credential Manager credentials were read.
10	Audit Success	3/1/2022 18:16 Microsoft	<input type="checkbox"/> 4608	5379	User Account Management	Credential Manager credentials were read.
11	Audit Success	3/1/2022 18:16 Microsoft	<input type="checkbox"/> 4616	5379	User Account Management	Credential Manager credentials were read.
12	Audit Success	3/1/2022 18:16 Microsoft	<input checked="" type="checkbox"/> 4634	5379	User Account Management	Credential Manager credentials were read.
13	Audit Success	3/1/2022 18:16 Microsoft	<input type="checkbox"/> 4625	5379	User Account Management	Credential Manager credentials were read.
14	Audit Success	3/1/2022 18:16 Microsoft	<input type="checkbox"/> 4634	5379	User Account Management	Credential Manager credentials were read.
15	Audit Success	3/1/2022 18:16 Microsoft	<input type="checkbox"/> 4647	5379	User Account Management	Credential Manager credentials were read.
16	Audit Success	3/1/2022 18:16 Microsoft	<input type="checkbox"/> 4648	5379	User Account Management	Credential Manager credentials were read.
17	Audit Success	3/1/2022 18:16 Microsoft	<input type="checkbox"/> 4672	5379	User Account Management	Credential Manager credentials were read.
18	Audit Success	3/1/2022 18:16 Microsoft	<input type="checkbox"/> 4688	5379	User Account Management	Credential Manager credentials were read.
19	Audit Success	3/1/2022 18:16 Microsoft	<input type="checkbox"/> 4696	5379	User Account Management	Credential Manager credentials were read.
20	Audit Success	3/1/2022 18:16 Microsoft	<input type="checkbox"/> 4707	5379	User Account Management	Credential Manager credentials were read.
21	Audit Success	3/1/2022 18:16 Microsoft	<input type="checkbox"/> 4708	5379	User Account Management	Credential Manager credentials were read.
22	Audit Success	3/1/2022 18:16 Microsoft	<input type="checkbox"/> 4799	5379	User Account Management	Credential Manager credentials were read.
23	Audit Success	3/1/2022 18:16 Microsoft	<input type="checkbox"/> 4854	5379	User Account Management	Credential Manager credentials were read.
24	Audit Success	3/1/2022 18:16 Microsoft	OK	5379	User Account Management	Credential Manager credentials were read.
25	Audit Success	3/1/2022 18:16 Microsoft	Cancel	5379	User Account Management	Credential Manager credentials were read.
26	Audit Success	3/1/2022 18:16 Microsoft		5379	User Account Management	Credential Manager credentials were read.
27	Audit Success	3/1/2022 18:16 Microsoft-Windows-Security-Auditing		5379	User Account Management	Credential Manager credentials were read.
28	Audit Success	3/1/2022 18:16 Microsoft-Windows-Security-Auditing		5379	User Account Management	Credential Manager credentials were read.
29	Audit Success	3/1/2022 18:16 Microsoft-Windows-Security-Auditing		5379	User Account Management	Credential Manager credentials were read.
30	Audit Success	3/1/2022 18:16 Microsoft-Windows-Security-Auditing		5379	User Account Management	Credential Manager credentials were read.
31	Audit Success	3/1/2022 18:16 Microsoft-Windows-Security-Auditing		5379	User Account Management	Credential Manager credentials were read.
32	Audit Success	3/1/2022 18:16 Microsoft-Windows-Security-Auditing		5379	User Account Management	Credential Manager credentials were read.
33	Audit Success	3/1/2022 18:16 Microsoft-Windows-Security-Auditing		5379	User Account Management	Credential Manager credentials were read.
34	Audit Success	3/1/2022 18:16 Microsoft-Windows-Security-Auditing		5379	User Account Management	Credential Manager credentials were read.
35	Audit Success	3/1/2022 18:16 Microsoft-Windows-Security-Auditing		5379	User Account Management	Credential Manager credentials were read.
36	Audit Success	3/1/2022 18:16 Microsoft-Windows-Security-Auditing		5379	User Account Management	Credential Manager credentials were read.
37	Audit Success	3/1/2022 18:16 Microsoft-Windows-Security-Auditing		5379	User Account Management	Credential Manager credentials were read.
38	Audit Success	3/1/2022 18:16 Microsoft-Windows-Security-Auditing		5379	User Account Management	Credential Manager credentials were read.



Logs in Excel

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?

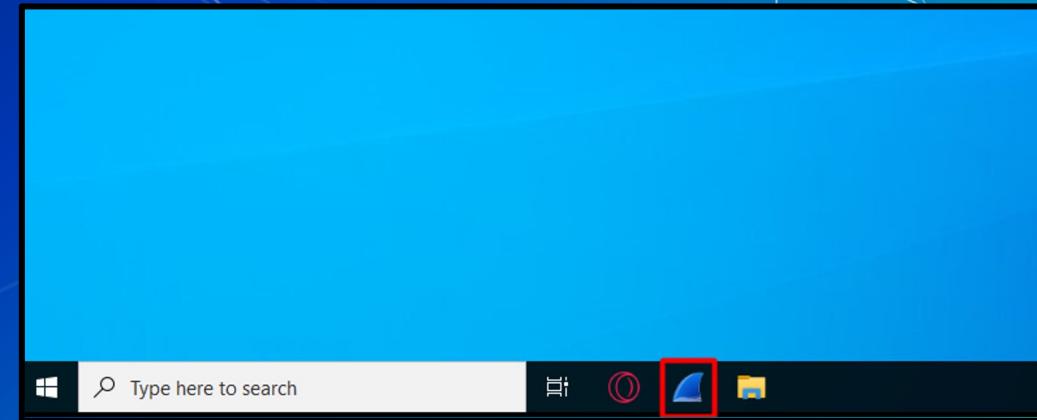
Network Forensics

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



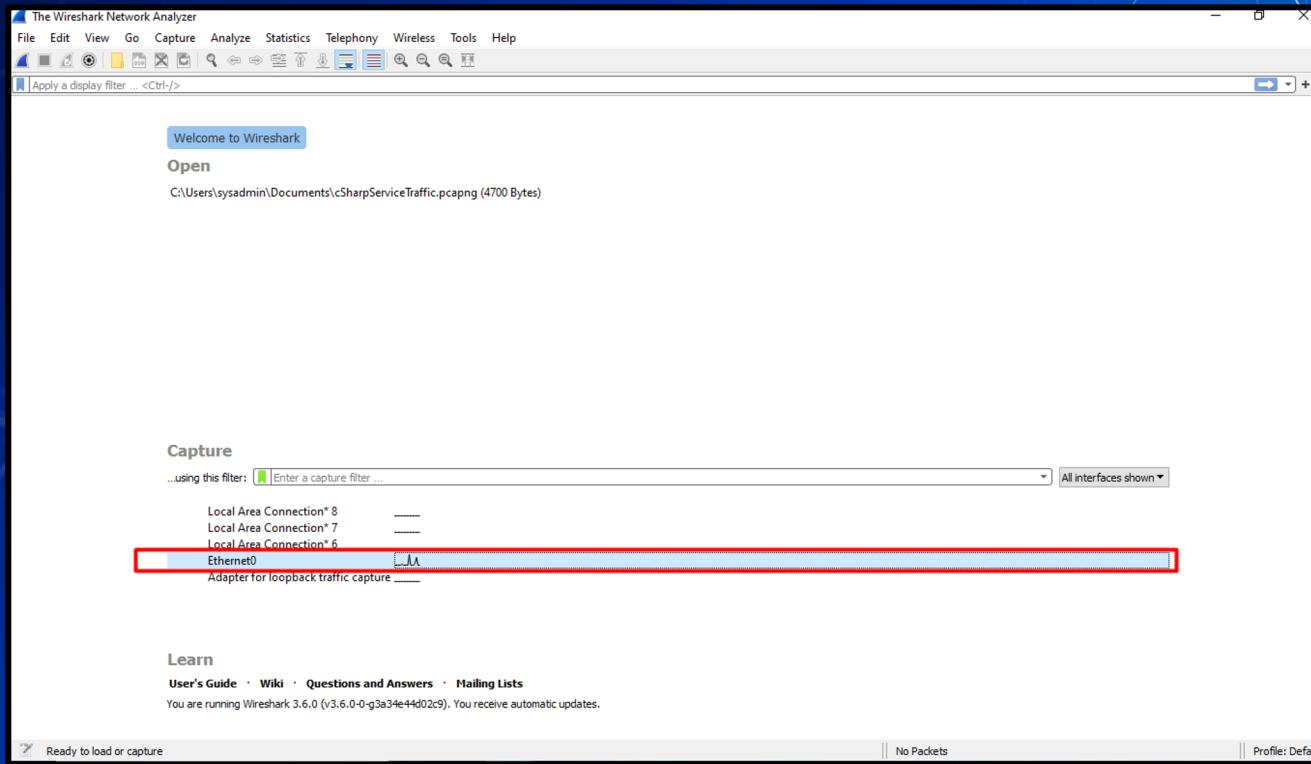
In Class Activity

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/pscore6

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  AESMService      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  AppXSvc           AppX Deployment Service (AppXSVC)
Stopped  AssignedAccessM... AssignedAccessManager Service
Running  AudioEndpointBu... Windows Audio Endpoint Builder
Running  Audiosrv          Windows Audio
Stopped  autotestsvc      Cellular Time
Stopped  AxinstSV         ActiveX Installer (AxInstSV)
Stopped  BroadcastUserSer... GameDVR and Broadcast User Service...
Running  BDESVC            BitLocker Drive Encryption Service
Stopped  BEService          BattleEye Service
Running  BFE                Base Filtering Engine
Stopped  BITS               Background Intelligent Transfer Ser...
Stopped  BluetoothUserSe... Bluetooth User Support Service_4dd2c3d
Running  BrokerInfrastru... 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  CDPUserSvc_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  cpiscon            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	AESMService	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	BcastDVRUserService...	GameDVR and Broadcast User Service_...
Running	BDESVC	BitLocker Drive Encryption Service
Stopped	BEService	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	:	AESMService
RequiredServices	:	{RPCSS}
CanPauseAndContinue	:	False
CanShutdown	:	False
CanStop	:	True
DisplayName	:	Intel® SGX AESM
DependentServices	:	{}
MachineName	:	.
ServiceName	:	AESMService
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>

Hands on 2 – Searching Output

- Run the following command
 - `Get-WmiObject win32_Service | select *`
- What is the difference between this and `Get-Service`?

Break Slide



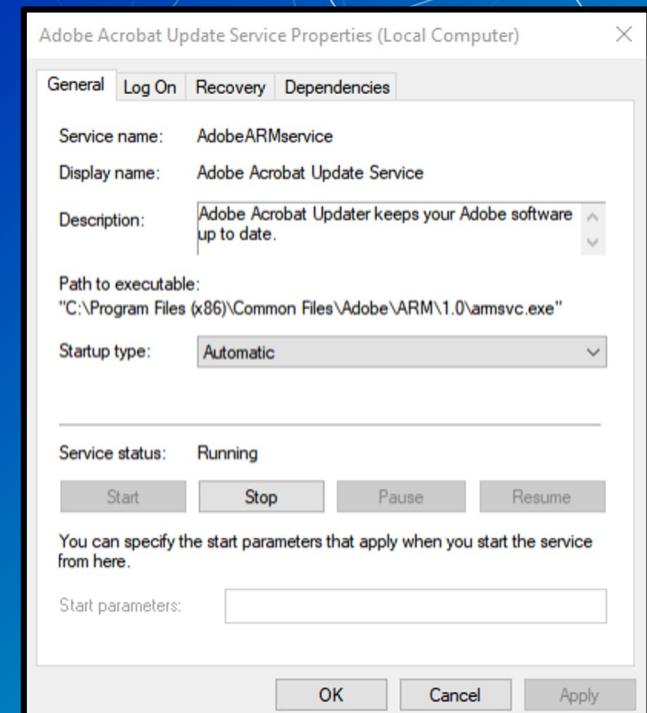
WMI & Services

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

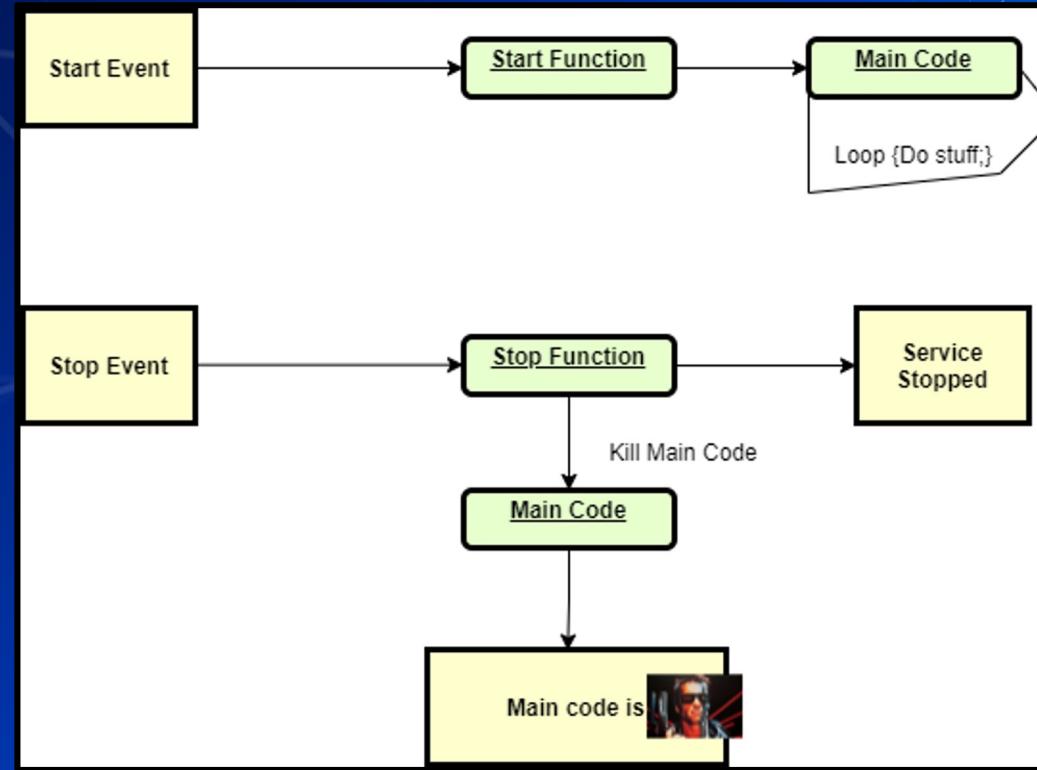
- Behind the scenes to keep things working
- 4 startup types
 - Automatic (Delayed Start)
 - Automatic
 - Manual
 - Disabled



Services

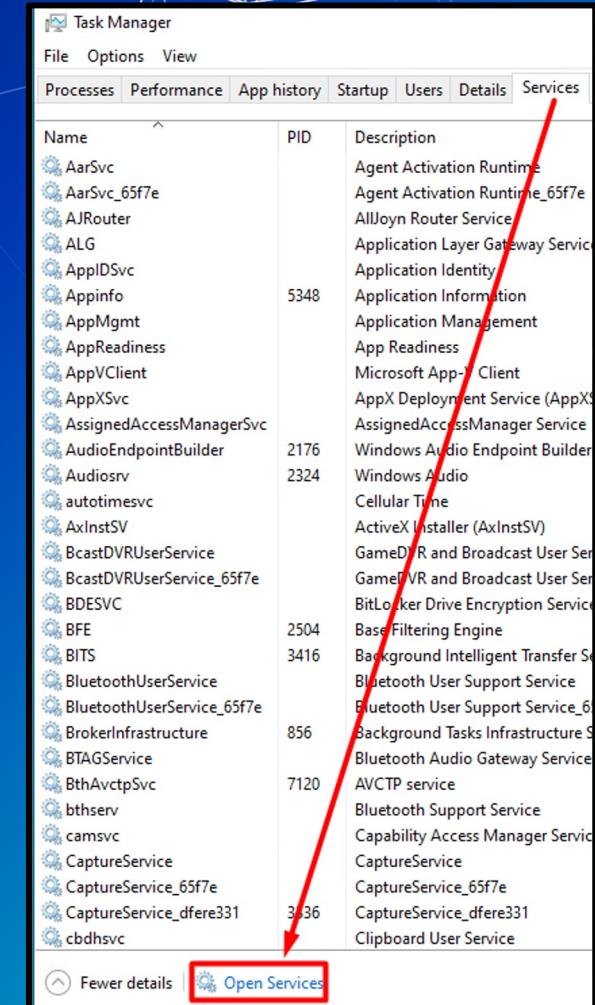
- Can run as nt authority \system
 - nt authority \system != root
 - Is more powerful than an "administrator"
- Active even when no user is signed in
- May be hosted by the service host (svchost.exe)
- May have executables that are designated to be services
- Follow a defined service model

Service Model



How to list services?

- Open Task Manager and navigate to services tab

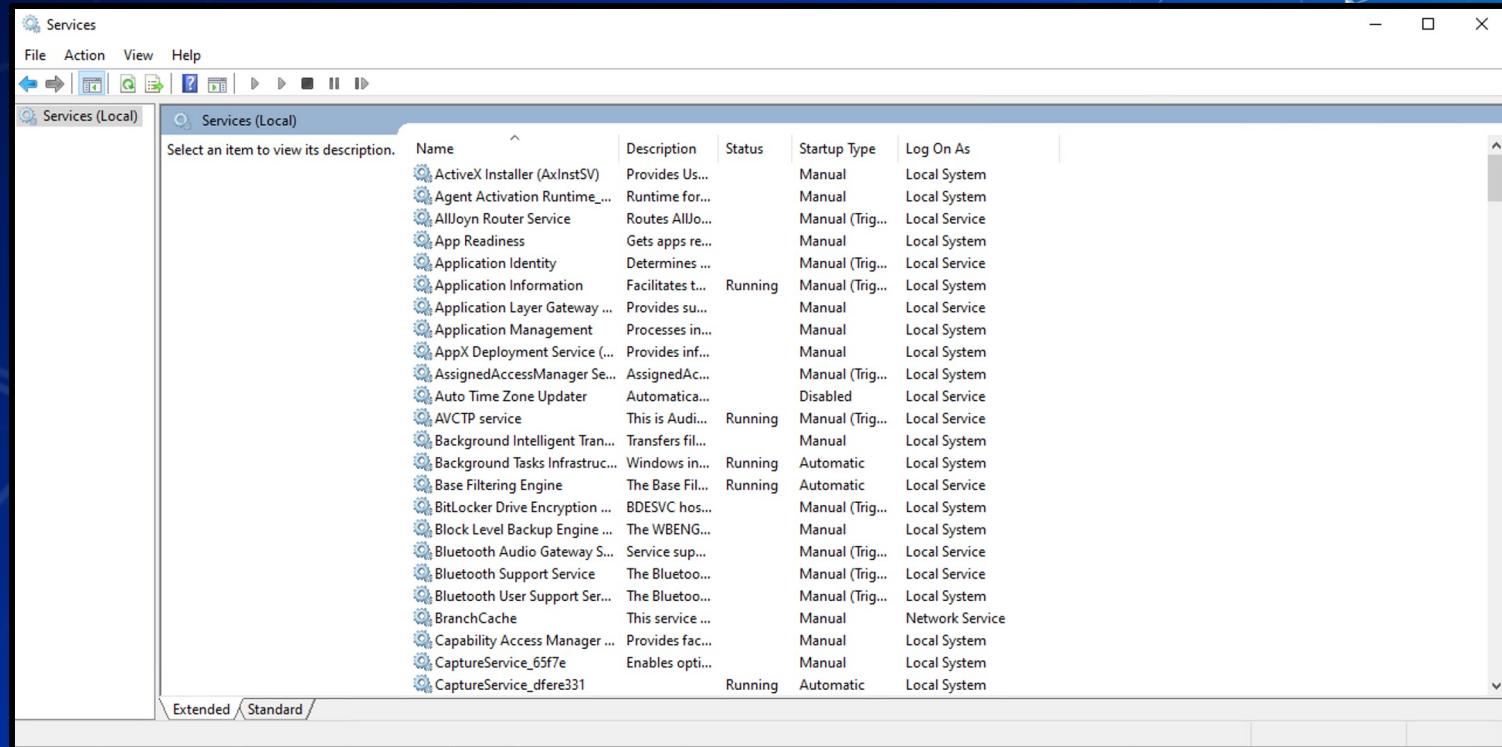


A screenshot of the Windows Task Manager showing the Services tab. The table lists various system services with their names, Process IDs (PID), and descriptions. A red arrow points from the top right towards the bottom right corner of the window, highlighting the 'Open Services' button.

Name	PID	Description
AarSvc		Agent Activation Runtime
AarSvc_65f7e		Agent Activation Runtime_65f7e
AJRouter		AllJoyn Router Service
ALG		Application Layer Gateway Service
ApplDSvc		Application Identity
Appinfo		Application Information
AppMgmt	5348	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		Game DVR and Broadcast User Service
BcastDVRUserService_65f7e		GameVR and Broadcast User Service
BDEsvc		BitLocker Drive Encryption Service
BFE	2504	Base Filtering Engine
BITS	3416	Background Intelligent Transfer Service
BluetoothUserService		Bluetooth User Support Service
BluetoothUserService_65f7e		Bluetooth User Support Service_65f7e
BrokerInfrastructure		Background Tasks Infrastructure Service
BTAGService	856	Bluetooth Audio Gateway Service
BthAvctpSvc	7120	AVCTP service
bthserv		Bluetooth Support Service
camsvc		Capability Access Manager Service
CaptureService		CaptureService
CaptureService_65f7e		CaptureService_65f7e
CaptureService_dfere331		CaptureService_dfere331
cbdhsvc	3436	Clipboard User Service

[Fewer details](#) | [Open Services](#)

Services List



The screenshot shows the Windows Services snap-in window titled "Services (Local)". The window has a toolbar at the top with icons for File, Action, View, and Help, along with navigation buttons like Back, Forward, and Home.

The main area displays a table of services:

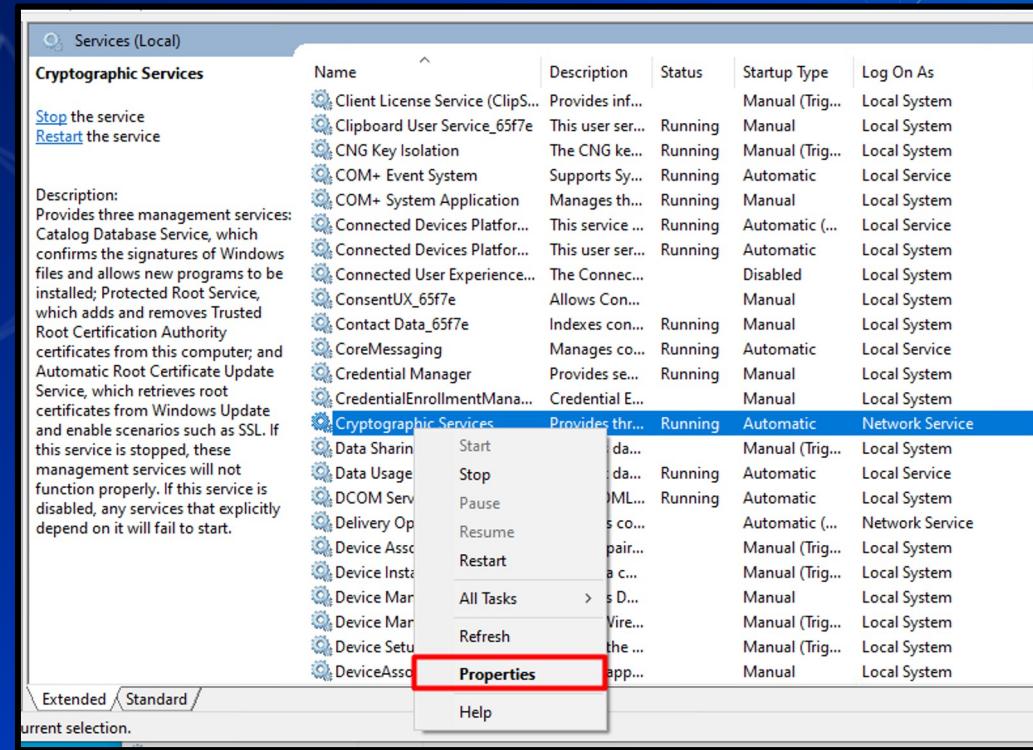
Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...	Manual	Local System	
Agent Activation Runtime_...	Runtime for...	Manual	Local System	
AllJoyn Router Service	Routes Alljo...	Manual (Trig...	Local Service	
App Readiness	Gets apps re...	Manual	Local System	
Application 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 Infrastruct...	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 Blueto...	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_dffere331	Running	Automatic	Local System	

At the bottom, there are tabs for "Extended" and "Standard".

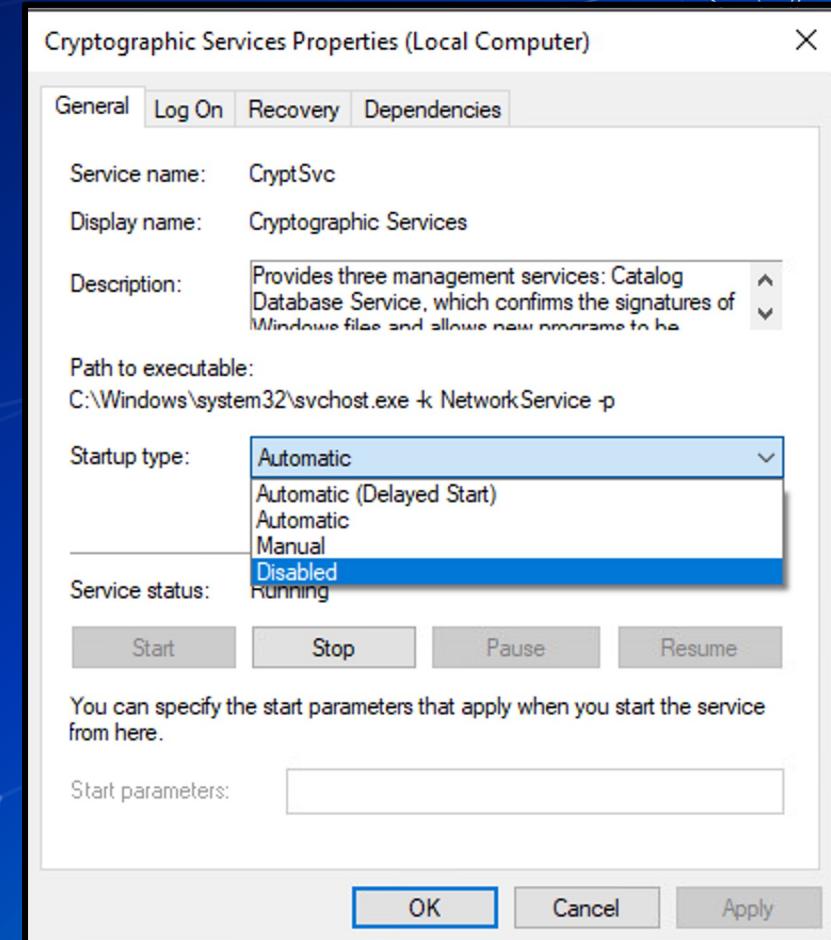
Services List

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...	Running	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...	Running	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...	Running	Automatic (...)	Network Service	
Device Association Service	Enables pair...	Running	Manual (Trig...	Local System	
Device Install Service	Enables a c...	Running	Manual (Trig...	Local System	
Device Management Enroll...	Performs D...	Running	Manual	Local System	
Device Management Wirele...	Routes Wire...	Running	Manual (Trig...	Local System	
Device Setup Manager	Enables the ...	Running	Manual (Trig...	Local System	
DeviceAssociationBroker_65...	Enables app...	Running	Manual	Local System	

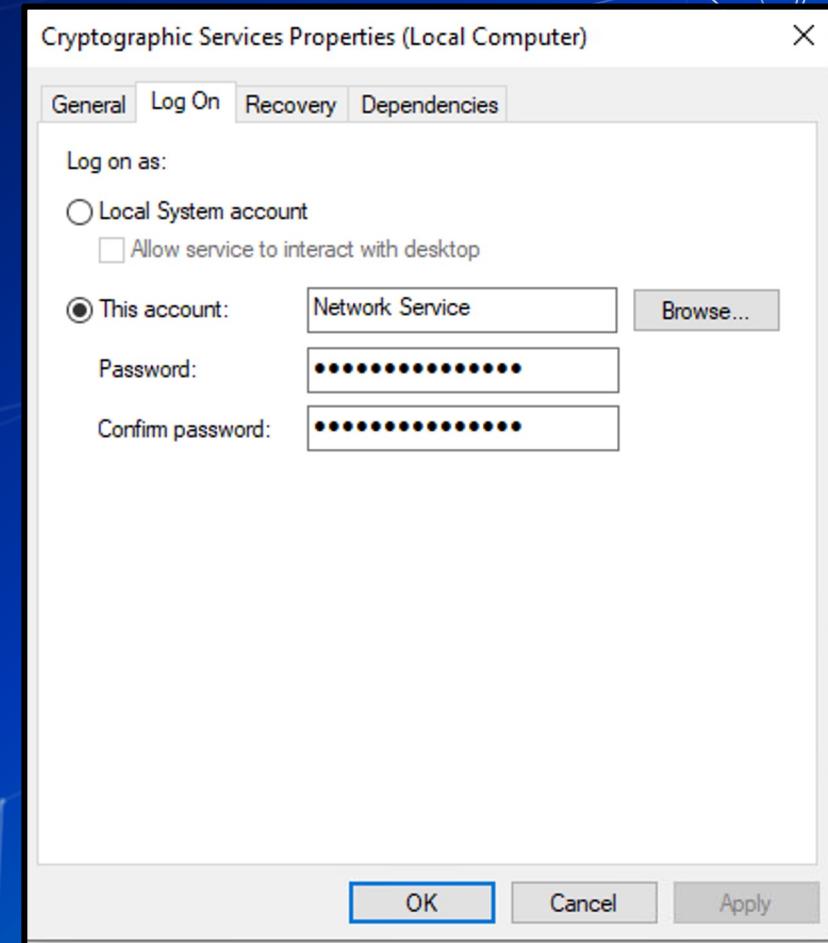
Services List



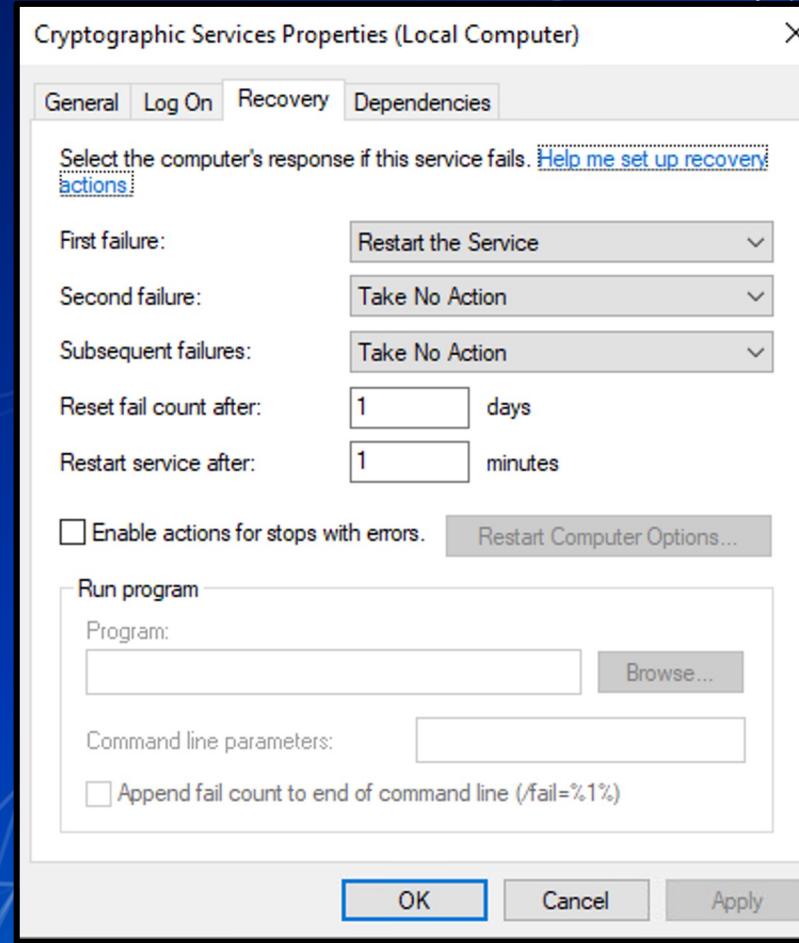
Services List



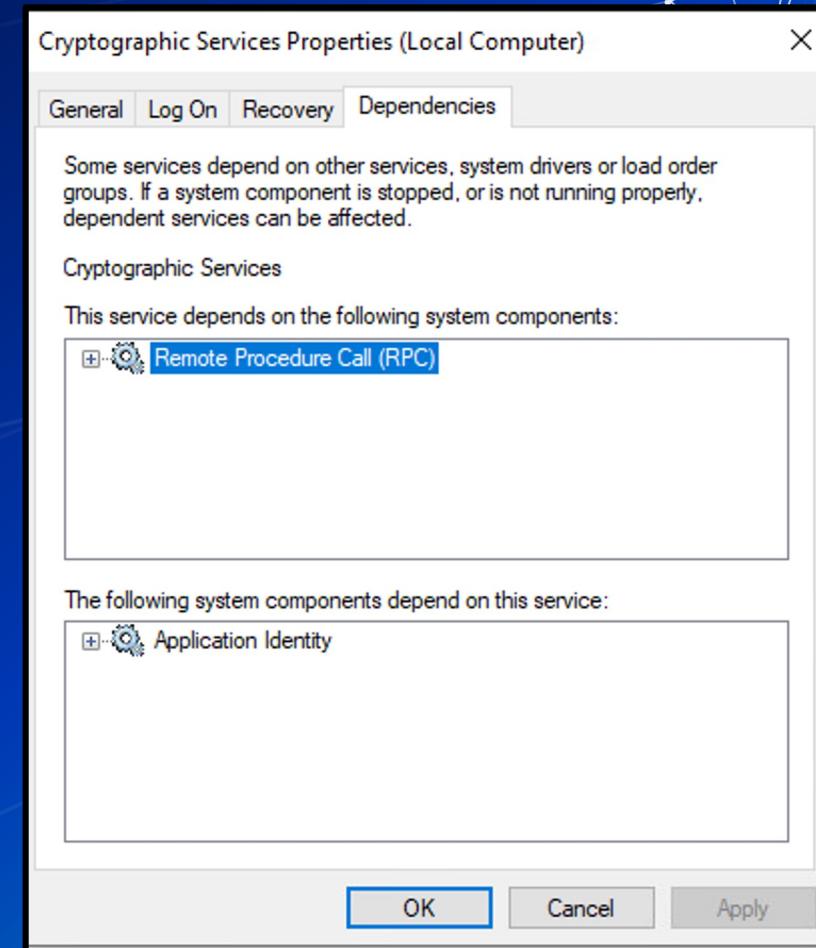
Services List



Services List



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 `| Format-Table` 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

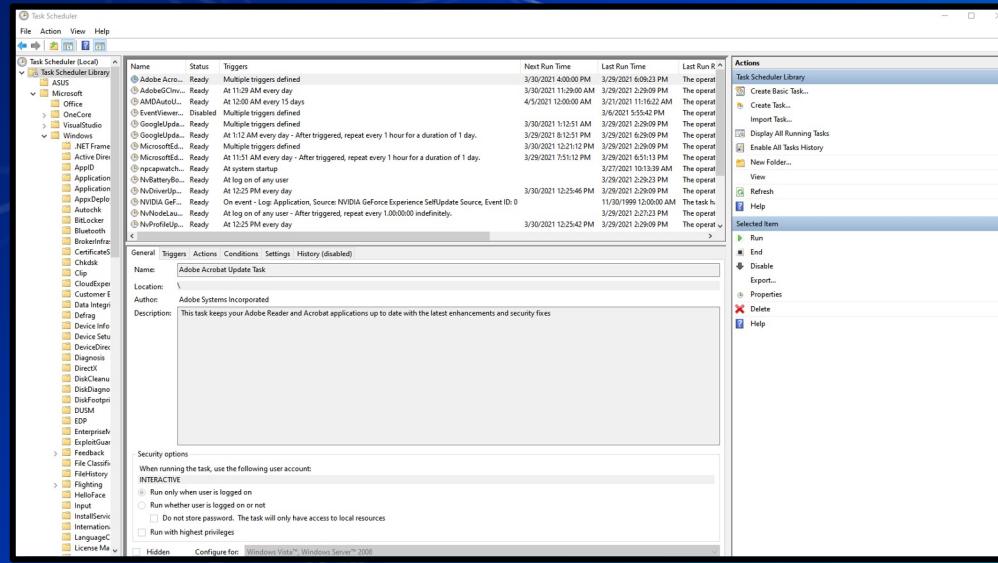
- Registry Editor is a GUI way of viewing registry
 - **Get-ItemProperty** can be used as well
 - <https://tinyurl.com/9hbeh72f>
- Two directories for running at sign on
 - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run			
	Name	Type	Data
>	(Default)	REG_SZ	(value not set)
>	GaijinNet Upda...	REG_SZ	"C:\Users\anthony\AppData\Local\Gaijin\Program ...
>	Synapse3	REG_SZ	"C:\Program Files (x86)\Razer\Synapse3\WPFUI\Fra...

Computer\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run			
	Name	Type	Data
>	(Default)	REG_SZ	(value not set)
>	MMDevices	REG_SZ	
>	Mrt	REG_SZ	
>	NcdAutoSetup	REG_SZ	
>	NetCache	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
>	NetworkServiceTriggers	REG_SZ	
>	SteelSeriesGG	REG_SZ	"C:\Program Files\SteelSeries\GG\SteelSeriesGG.exe"

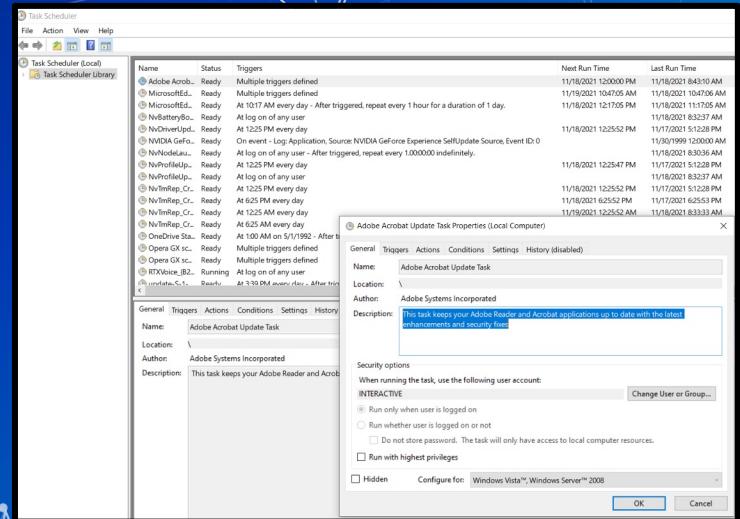
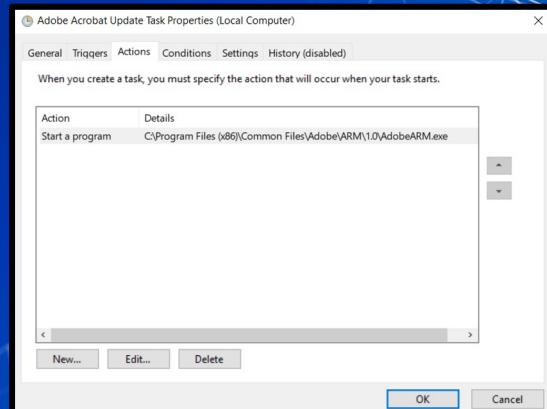
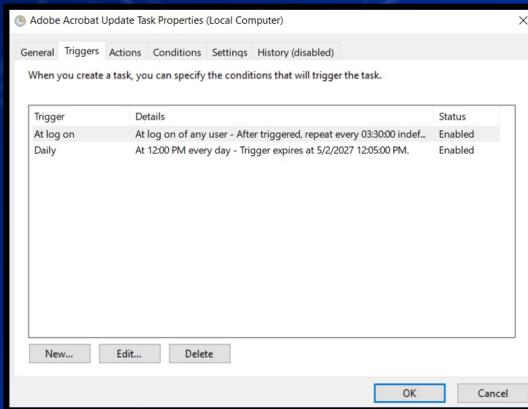
Scheduled Tasks

- 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?



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

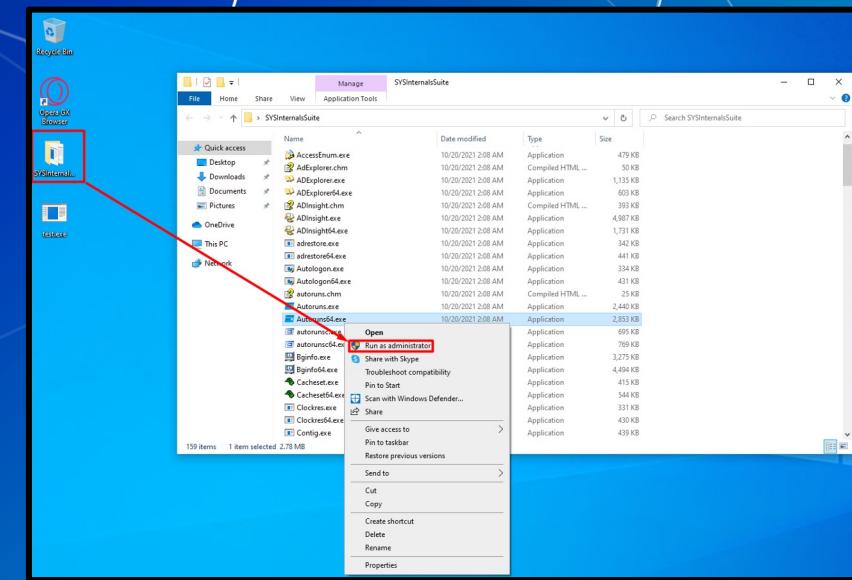
- Group policies can soften the security posture of a device
 - Disable anti-virus
 - Turn off or flood logs
 - Disable firewalls
 - And more!
- Group Policies can be used to establish registry based persistence
- Malicious group policies are very dangerous

Hands on 4 – Combatting Persistence

- Check services again
 - What do you notice?

Hands on 4 – Combating 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

Autons - Systematics: www.sysinternals.com (Administrator) [DESKTOP-7A15TS1\sysadmin]						
	Description	Publisher	Image Path	Timestamp	Virus Total	
Autons Entry						
↳ 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-5-1-21-1961932216-26321...	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 16347272882	Keeps Opera Browser Assistant up to date	(Verified) Opera Software AS	C:\Users\sysadmin\AppData\Local\Programs\Opera GX\launcher.exe	Thu Nov 4 10:00:01 2021		
↳ Opera GX scheduled Autoupdate 1634727190	Keeps Opera up to date	(Verified) Opera Software AS	C:\Users\sysadmin\AppData\Local\Programs\Opera GX\launcher.exe	Thu Nov 4 10:00:01 2021		
↳ VMwareToolsUpdater	Keeps Open PowerShell up to date	(Verified) Microsoft Windows	C:\Windows\System32\WindowsPowerShellV1.0\powershell.exe	Mon Mar 18 14:46:56 2019		
Services						
↳ Edupadate	Microsoft Edge Update Service (edupadate..)	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021		
↳ Edupadates	Microsoft Edge Update Service (edupadate..)	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021		
↳ MicrosoftEdgeElevationService	Microsoft Edge Elevation Service (Micros..)	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\95.0.1020.51\elevation_service.exe	Thu Nov 18 15:29:29 2021		
↳ MSBuild	MSBuild Provides Just-in-time compilati...	(Not Verified) Microsoft Corpor...	C:\Program Files (x86)\Microsoft .NET\Medium\MSBuild\msbuild.exe	Wed Oct 27 12:25:21 2021		
↳ NetTcPPortSharing	Net Tcp Port Sharing Service: Provides ab...	(Verified) Microsoft Corporation	C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMSSvcHost.exe	Fri Dec 6 22:09:03 2019		
↳ VgAuthService	VMware Alias Manager and Ticket Service ..	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\VGAuthService.exe	Sat Apr 14 09:40:22 2018		
↳ VMSDevice	VMware SVGA Helper Service: Helps VMw...	(Verified) VMware, Inc.	C:\Windows\system32\vm3dservice.exe	Mon Feb 21 02:55:32 2021		
↳ VMTools	VMTools: Provides support for sync...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Sat Apr 14 09:45:52 2018		
↳ VMware Physical Disk Helper Service	VMware Physical Disk Helper Service: Ena...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmacthd.exe	Sat Apr 14 09:45:46 2018		
↳ VMwareCAFAMQPListener	VMware CAF AMQP Communication Ser...	(Not Verified)	C:\Program Files\VMware\VMware Tools\vmware_caf\bin\CommAmqpListener.exe	Sat Apr 14 09:24:46 2018		
↳ VMwareCAFManagementAgentHost	VMware CAF Management Agent Service...	(Not Verified)	C:\Program Files\VMware\VMware Tools\vmware_caf\bin\ManagementAgentHost.exe	Sat Apr 14 09:24:14 2018		
↳ VMwareCapture	VMwareCapture: Enables optional screen ...	(Not Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\VMWareCapture.exe	Sat Apr 14 09:35:58 2018		
Drivers						
↳ HKLM\System\CurrentControlSet\Services\lpf\$S\$GPO	Intel® Serial I/O GPO Controller Driver: I...	(Verified) Intel Corporation	C:\Windows\System32\drivers\lpf\$S\$GPO.sys	Thu Nov 18 16:41:54 2021		
↳ Npcap	Npcap Packet Driver (Npcap): Npcap Pa...	(Verified) Insecure.Com LLC	C:\Windows\system32\DRIVERS\npcap.sys	Mon Mar 18 17:45:38 2019		
↳ vmb3dmp	vmb3dmp: VMware SVGA 3D Minport	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vm3dmp.sys	Wed Apr 21 11:59:43 2021		
↳ vmb3dmp-debug	vmb3dmp-debug: VMware SVGA 3D Minipi...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vm3dmp-debug.sys	Sat Apr 14 10:00:02 2018		
↳ vmb3dmp-stats	vmb3dmp-stats: VMware SVGA 3D Minipor...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vm3dmp-stats.sys	Sat Apr 14 10:00:02 2018		
↳ vmb3dmp_Leader	vmb3dmp_Leader: VMware SVGA 3D Minipor...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vm3dmp_leader.sys	Sat Apr 14 10:00:02 2018		
↳ vmd	VMware VMCI Bus Driver: VMware PCI V...	(Verified) VMware, Inc.	C:\Windows\system32\drivers\vmci.sys	Wed Nov 29 10:32 2017		
↳ vmb3dmp	VMware Host Guest Client Redirector: Im...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vm3dmp.sys	Sat Apr 14 09:55:46 2018		
↳ vmmemctrl	Memory Control Driver: Driver to provide ...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmmemctrl.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		
↳ vmsvadsk	VMware Physical Disk Helper: VMware Ph...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmsvadsk.sys	Sat Apr 14 09:55:04 2018		
↳ vmsvabmouse	VMware USB Pointing Device: VMware Po...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmusbmouse.sys	Sat Apr 14 09:57:32 2018		
↳ vnetvfp	vnetvfp: Guest Introspection Network Fil...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vnetaFP.sys	Sat Apr 14 10:00:44 2018		
↳ vesfpt	vesfpt: Guest Introspection Driver	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vesfpt.sys	Sat Apr 14 09:59:58 2018		
↳ vsock	vSockets Virtual Machine Communicatio...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vsock.sys	Wed Nov 29 10:32 2017		
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Font Drivers						
MSBuild	Size: 62,080 K	Time: Wed Oct 20 01:22:21 2021				
	(Not Verified) ©Microsoft Corporation	Version: 16.9.0.195				
	C:\Program Files (x86)\Microsoft.NET\readlist\MSBuild.exe					

Hands on 4 – Combating Persistence

Screenshot of Autoruns (Sysinternals) showing persistence entries:

Category	Description	Publisher	Image Path	Timestamp	Virus Total
Autoruns Entry	Keeps your Microsoft software up to date...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\update\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021	
	Keeps your Microsoft software up to date...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\update\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021	
	(Not Verified)		C:\Program Files\Npcap\CheckStatus.bat	Wed Apr 21 13:46:46 2021	
	Standalone Updater				
	Opera GX scheduled assistant Autoupdate 1637272882	(Verified) Open Software AS	C:\Users\sysadmin\AppData\Local\Programs\Opera GX\launcher.exe	Thu Nov 18 13:58:11 2021	
	Opera GX scheduled Autoupdate 1634717190	(Verified) Open Software AS	C:\Users\sysadmin\AppData\Local\Programs\Opera GX\launcher.exe	Thu Nov 4 10:00:11 2021	
	Keeps Opera up to date.	(Verified) Open Software AS	C:\Users\sysadmin\AppData\Local\Programs\Opera GX\launcher.exe	Thu Nov 4 10:00:11 2021	
	Windows PowerShell	(Verified) Microsoft Windows	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Mon Mar 18 21:46:56 2019	
Services					
HKEY\SYSTEM\CurrentControlSet\Services					
	edgeupdate	Microsoft Edge Update Service (edgeupd...)	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\update\MicrosoftEdgeUpdate.exe	Thu Nov 18 16:41:54 2021
	edgeupdate	Microsoft Edge Update Service (edgeupd...)	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\update\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021
	MicrosoftEdgeElevationService	Microsoft Edge Elevation Service (Micros...)	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\app\MicrosoftEdgeApplication95.0.1020.53\elevation_service.exe	Thu Apr 1 12:17:37 2021
	MSBuild	MSBuild: Provides Just-in-time compli...	(Not Verified) Microsoft Corpor...	C:\Program Files (x86)\Microsoft.NET\Redist\list\MSBuild.exe	Wed Oct 20 01:22:21 2021
	NetCpPo_Sharing	Net Cp Port Sharing Service: Provides ab...	(Verified) Microsoft Corporation	C:\Windows\Microsoft.NET\Framework64\v4.0.3019\MSMSvHost.exe	Fri Dec 6 22:03:00 2019
	vGAuthService	VMware Alias Manager and Ticket Service...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\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 02:53:22 2021
	VMTools	VMware Tools: Provides support for sync...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Sat Apr 14 09:58:52 2018
	VMwarePhysicalDiskHelperService	VMware Physical Disk Helper Service: Ena...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmachp.exe	Sat Apr 14 09:54:36 2018
	VMwareCAFComAmqpListener	VMware CAF AMQP Communication Servic...	(Not Verified)	C:\Program Files\VMware\VMware Tools\CAF\pm\bin\CommAmqpListener.exe	Sat Apr 14 09:52:46 2018
	VMwareCAFManagementAgentHost	VMware CAF Management Agent Service...	(Not Verified)	C:\Program Files\VMware\VMware Tools\CAF\pm\bin\ManagementAgentHost.exe	Sat Apr 14 09:52:14 2018
	VMwareCapture	VMwareCapture: Enables optional screen ...	(Not Verified)	C:\Program Files\VMware\VMware Tools\VMWareCapture.exe	Sat Apr 14 09:58:58 2018
Drivers					
HKEY\SYSTEM\CurrentControlSet\Services					
	iaLPSL_GIO	Intel(R) Serial IO GPIO Controller Driver: ...	(Verified) Intel Corporation - Client	C:\Windows\System32\drivers\iaLPSL_GIO.sys	Thu Nov 18 16:41:54 2021
	npcap	Npcap Packet Driver (NPcap): Npcap Pa...	(Verified) Insecure.Com LLC	C:\Windows\System32\DRIVERS\npcap.sys	Mon Mar 18 21:43:30 2019
	vm3dmp	vm3dmp: VMware SVGA 3D Minip...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vm3dmp.sys	Wed Apr 21 11:59:48 2021
	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
	vm3dmp-state	vm3dmp-state: VMware SVGA 3D Minip...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vm3dmp-state.sys	Sat Apr 14 10:02:02 2018
	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
	vmci	VMware VMCI Bus Driver: VMware PCI V...	(Verified) VMware, Inc.	C:\Windows\System32\drivers\vmci.sys	Sat Apr 14 10:02:02 2018
	vhmgfs	VMware Guest Client Redirector: Im...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vhmgfs.sys	Wed Nov 29 00:10:32 2017
	VMMemCtl	Memory Control Driver: Driver to provide...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vmmemctl.sys	Sat Apr 14 09:55:46 2018
	vnmouse	VMware Pointing Device: VMware Pointin...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vnmouse.sys	Sat Apr 14 09:56:16 2018
	vnrawdsk	VMware Physical Disk Helper: VMware Ph...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vnrawdsk.sys	Sat Apr 14 09:55:04 2018
	vmbusmouse	VMware USB Pointing Device: VMware Po...	(Verified) VMware, Inc.	C:\Windows\System32\drivers\vmbusmouse.sys	Sat Apr 14 09:57:32 2018
	vnetWFP	vnetWFP: Guest Inspection Network Fil...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vmnetWFP.sys	Sat Apr 14 10:00:44 2018
	vespfilt	vespfilt: Guest Inspection Driver	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vespfilt.sys	Sat Apr 14 09:59:58 2018
	vsocsk	vSockets Virtual Machine Communicatio...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vsocsk.sys	Wed Nov 29 00:10:32 2017
HKEY\Software\Microsoft\Windows NT\CurrentVersion\Font Drivers					
	MSBuild	MSBuild: Provides Just-in-time compli...	(Not Verified) Microsoft Corpor...	C:\Program Files (x86)\Microsoft.NET\Redist\list\MSBuild.exe	Mon Mar 18 21:55:43 2019

Detailed description of the highlighted MSBuild entry:

- Category: Services
- Name: **MSBuild**
- Description: **MSBuild: Provides Just-in-time compilation support for Microsoft .NET Framework applications.**
- Publisher: **(Not Verified)** Microsoft Corporation
- Image Path: **C:\Program Files (x86)\Microsoft.NET\Redist\list\MSBuild.exe**
- Timestamp: **Wed Oct 20 01:22:21 2021**
- File Version: **16.9.0.195**
- File Size: **62,080 K**

Hands on 4 – Combating 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/a7jpzmse>
 - <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?