

Windows Threat Hunting

UBNetDef, Spring 2024
Week 6

Presenter:
Anthony Magrene

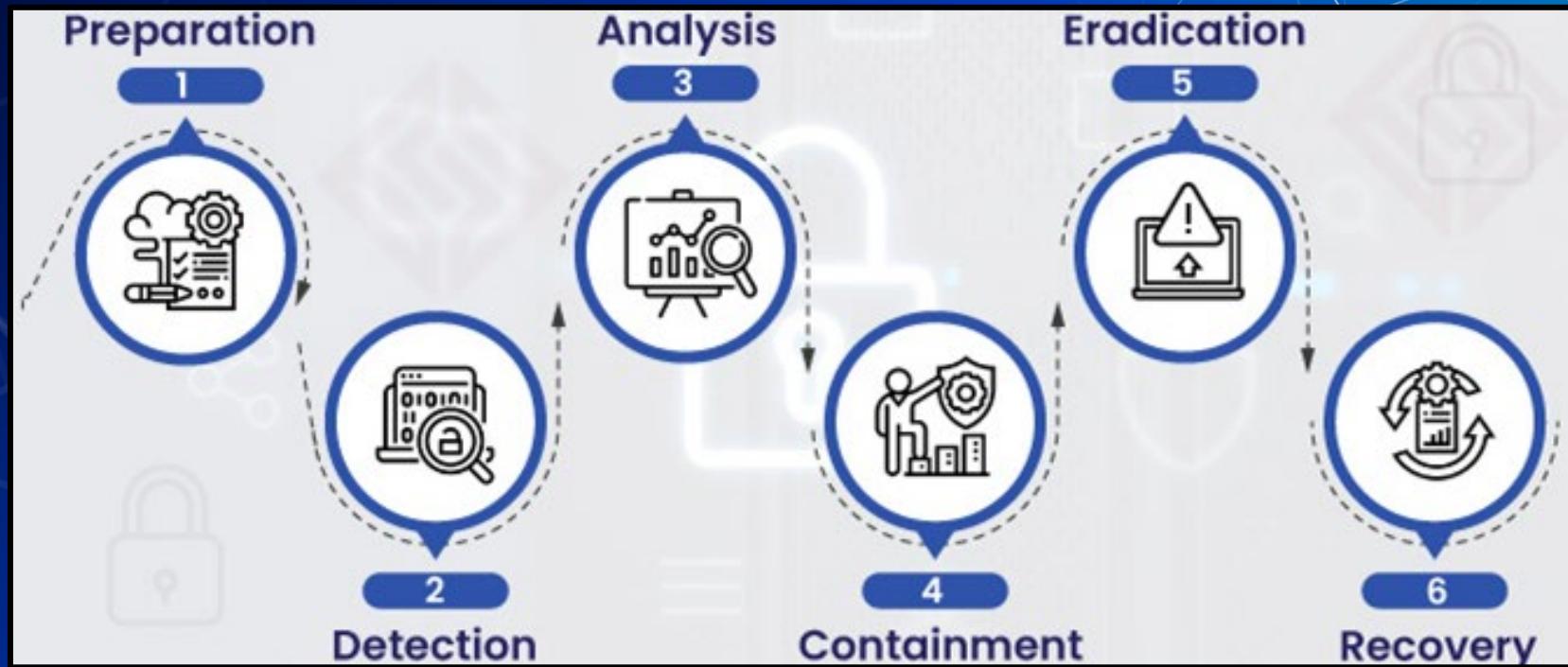


Agenda – Week 6

- 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)

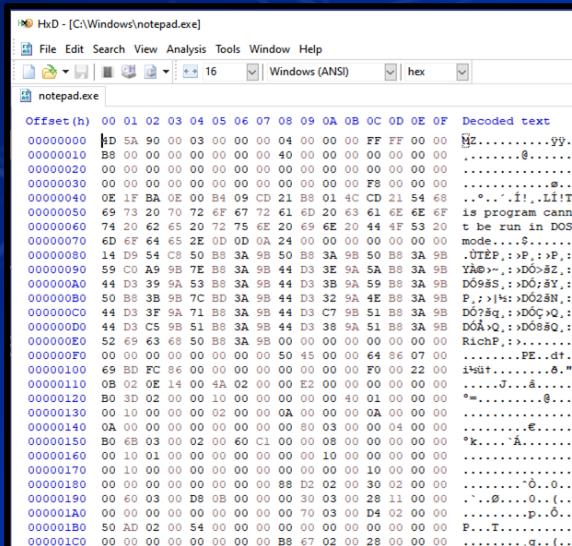
- Windows implementation of shared libraries
- Prevents redundant storage commonly used code

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.

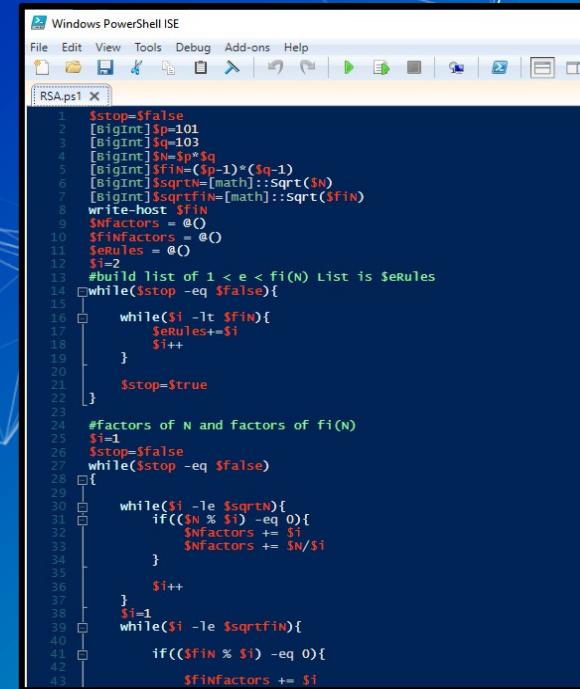


The screenshot shows the HxD hex editor interface. The title bar reads "HxD - [C:\Windows\notepad.exe]". The menu bar includes File, Edit, Search, View, Analysis, Tools, Window, Help. The toolbar has icons for Open, Save, Find, Replace, Copy, Paste, Cut, Delete, Undo, Redo, and a zoom dropdown set to 16. The status bar shows "Windows (ANSI)" and "hex". The main window displays memory dump details with columns for Offset(h), Decoded text, and Hex dump. The offset column ranges from 00000000 to 00001C0. The decoded text column shows assembly-like mnemonics and opcodes. The hex dump column shows the raw binary data. A scroll bar is visible on the right.

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

PowerShell Script (.ps1)

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

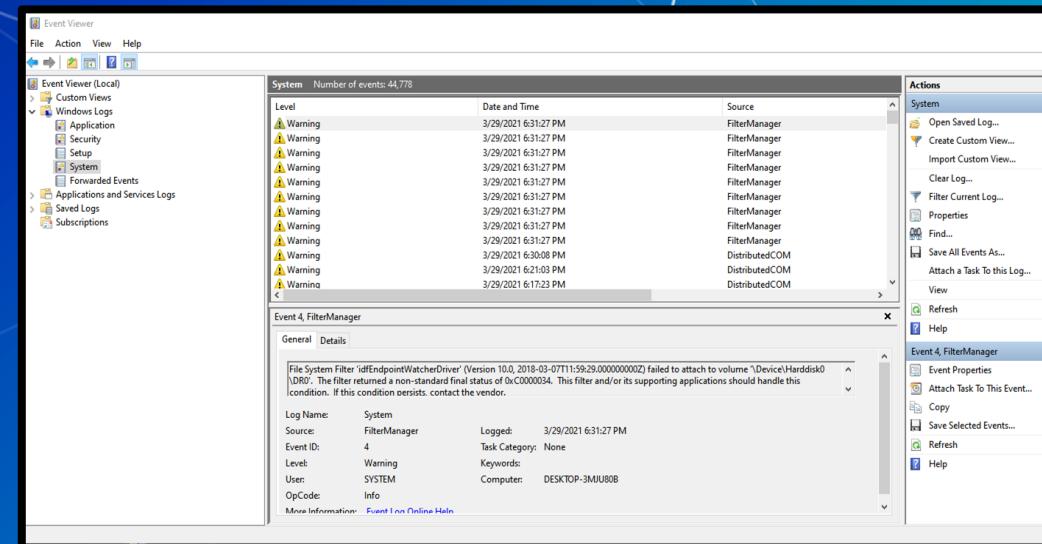


The screenshot shows the Windows PowerShell Integrated Scripting Environment (ISE) window titled "RSA.ps1". The code in the editor is a PowerShell script named RSA.ps1, which performs calculations related to RSA encryption. It includes variables like \$p, \$q, \$n, \$phi, and \$e, and uses loops to find factors of \$n and calculate \$phi.

```
$stop=$false
$[bigint]$p=101
$[bigint]$q=103
$[bigint]$n=$p*$q
$[bigint]$fin=(($p-1)*($q-1))
$[bigint]$sqrtN=[math]::sqrt($n)
$[bigint]$sqrtFin=[math]::sqrt($fin)
write-host $fin
$nfactors = @()
$finfactors = @()
$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
            $finfactors += $fin/$i
        }
        $i++
    }
    $i=1
    while($i -le $sqrtfin){
        if($fin % $i) -eq 0{
            $finfactors += $i
        }
        $i++
    }
}
```

Event Log (.evtx)

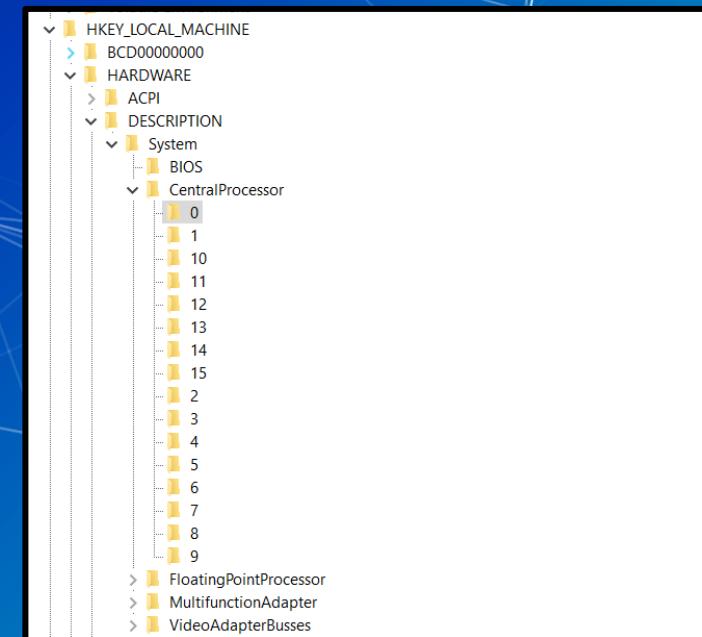
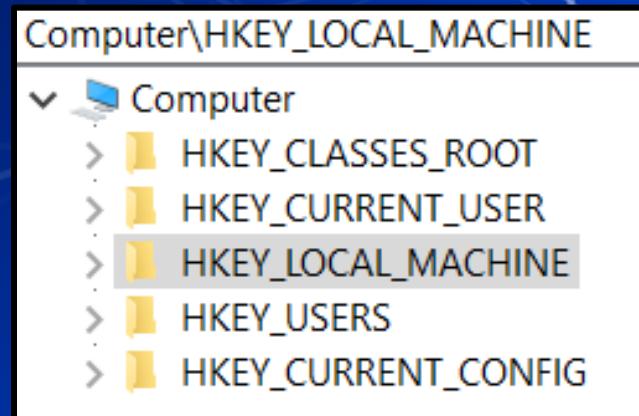
- Stores Windows Logs
- Located C:\Windows\System32\winevt\Logs\
- Event viewer used to view logs



The Registry

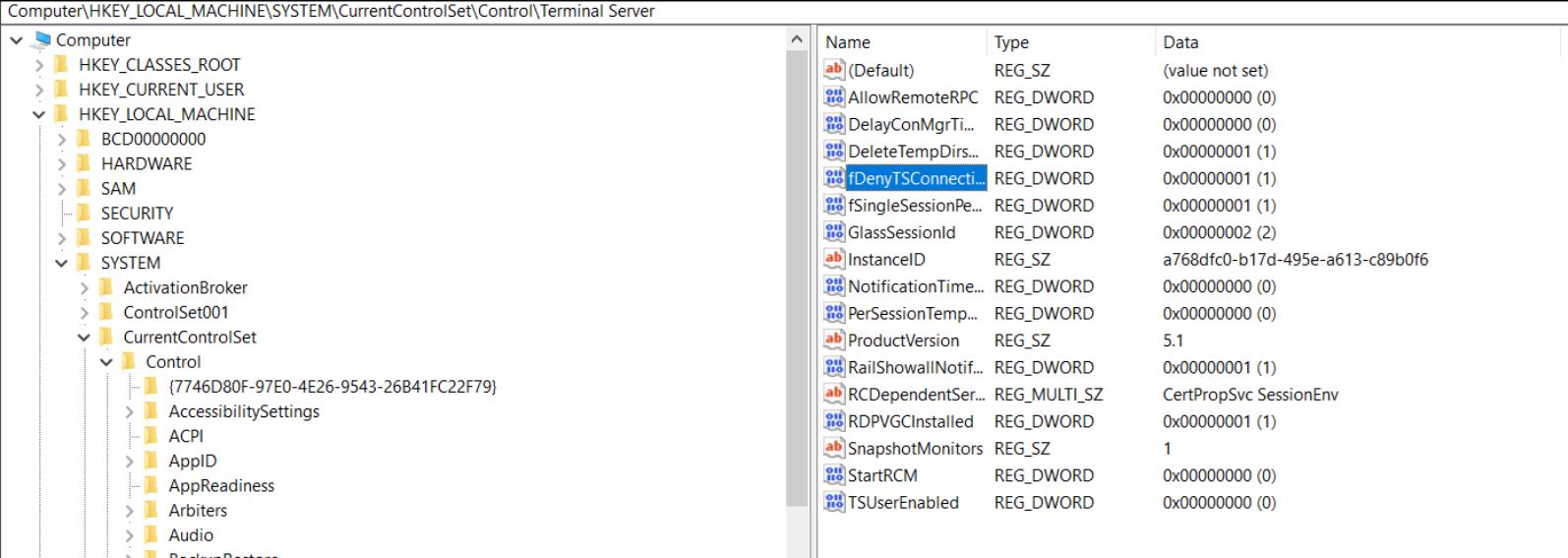
Registry

- Hierarchical database
 - Stores low-level settings



Registry cont.

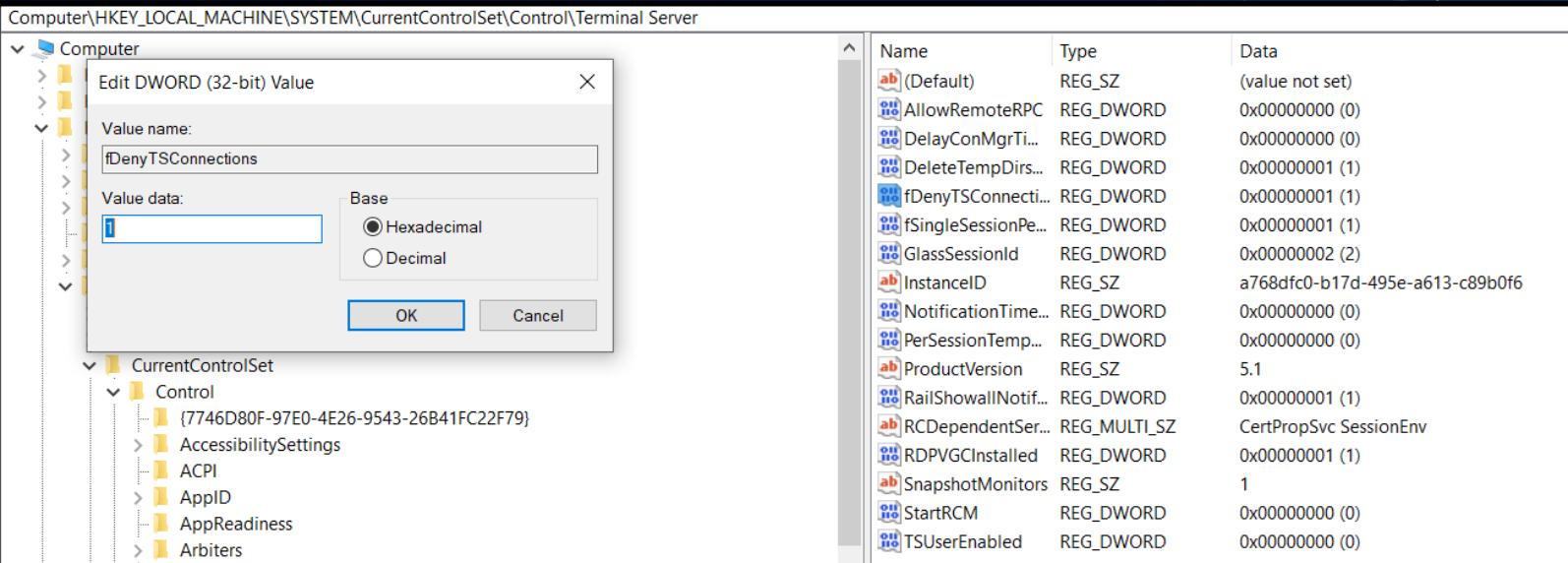
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server



Name	Type	Data
(Default)	REG_SZ	(value not set)
AllowRemoteRPC	REG_DWORD	0x00000000 (0)
DelayConMgrTi...	REG_DWORD	0x00000000 (0)
DeleteTempDirs...	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



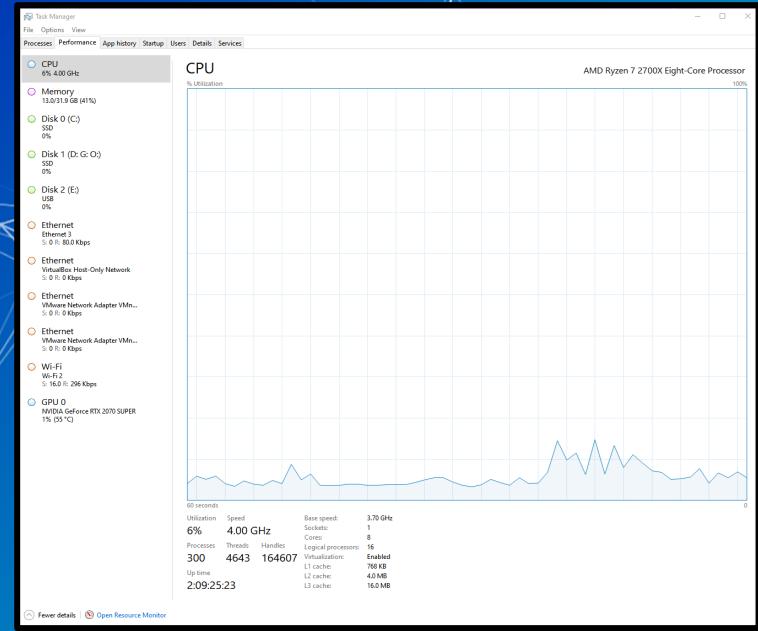
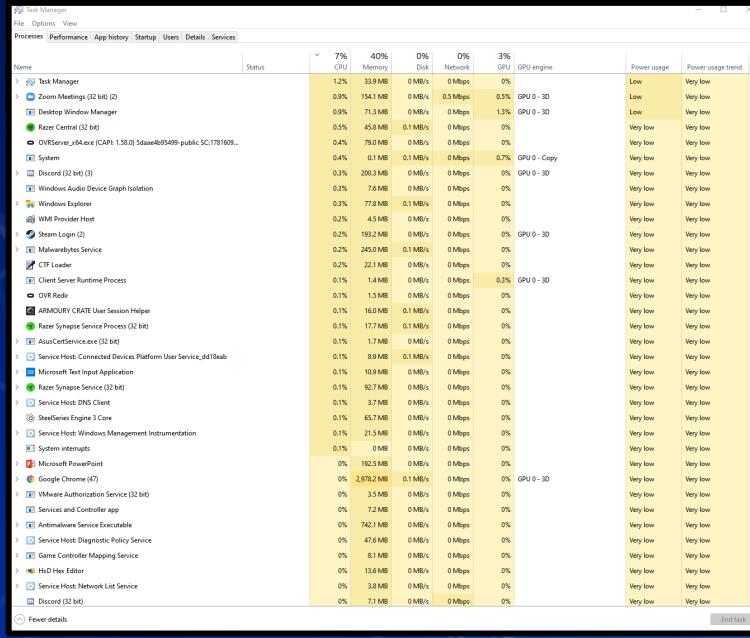
The screenshot shows the Windows Registry Editor interface. On the left, the navigation pane displays the registry path: Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server. A sub-menu is open under 'Computer' with the title 'Edit DWORD (32-bit) Value'. Inside this menu, the 'Value name:' field contains 'fDenyTSConnections' and the 'Value data:' field contains the value '1'. The 'Base' dropdown is set to 'Hexadecimal'. At the bottom of the menu are 'OK' and 'Cancel' buttons. The right pane lists various registry keys under 'Control'. The 'fDenyTSConnections' key is highlighted in blue. The table below provides a detailed view of the registry entries:

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)

Task Manager

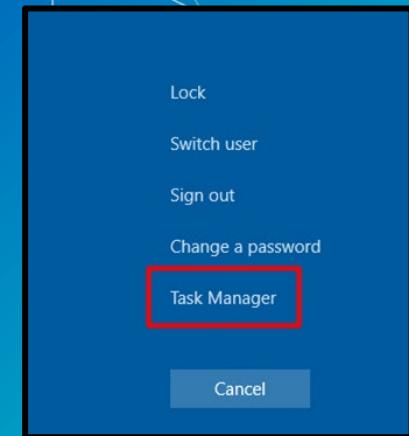
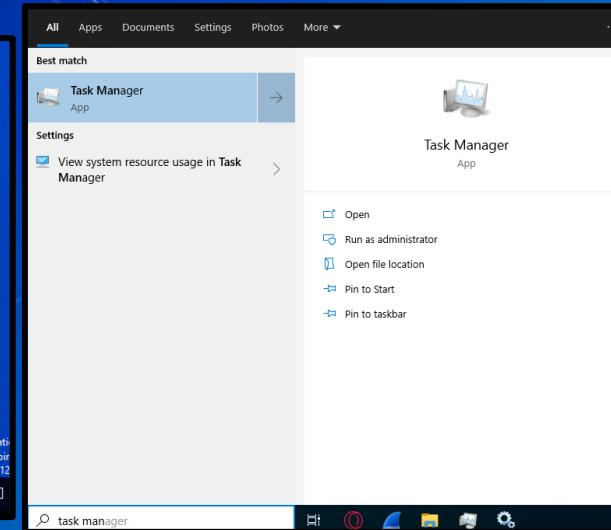
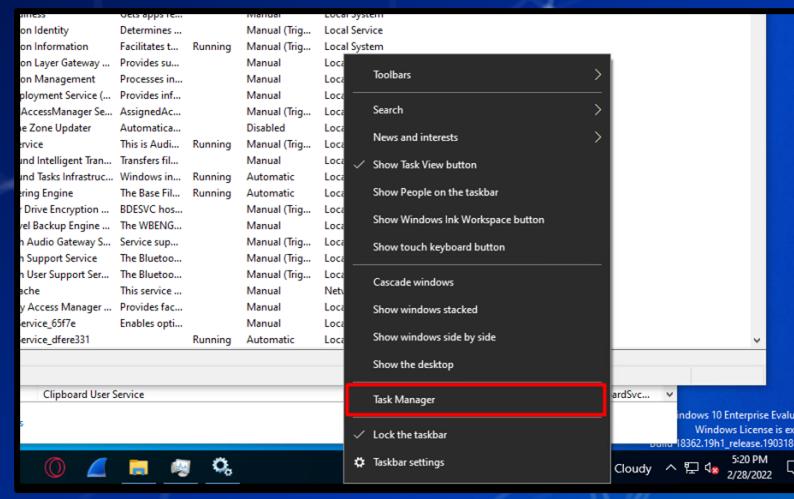
Task Manager

Provides high-level view of what is running



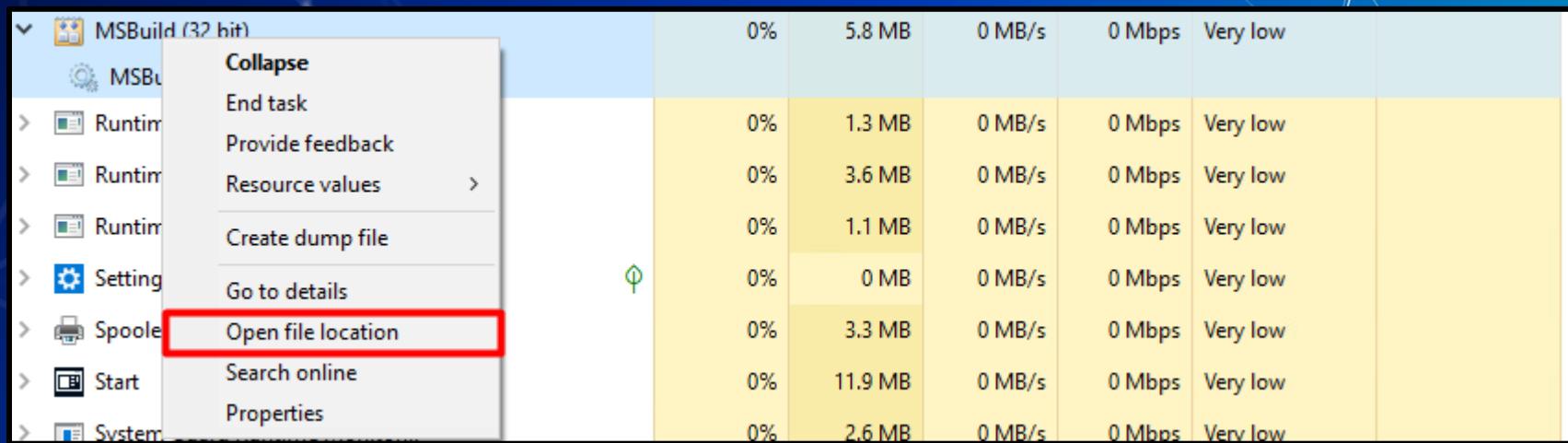
Task Manager cont.

■ How to open it?



Task Manager cont.

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

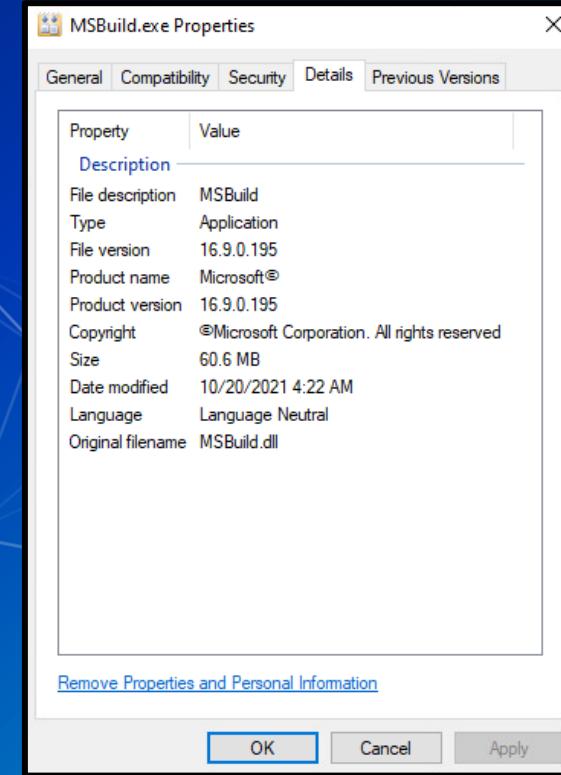
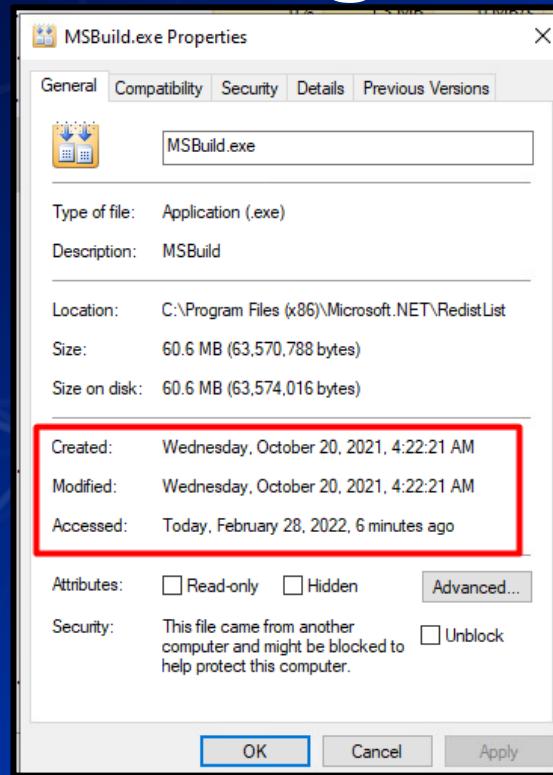


Task Manager cont.

- Show the properties of an executable

Task	CPU	Memory	Network	Processor	Priority	Background	Details
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	Collapse						
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		

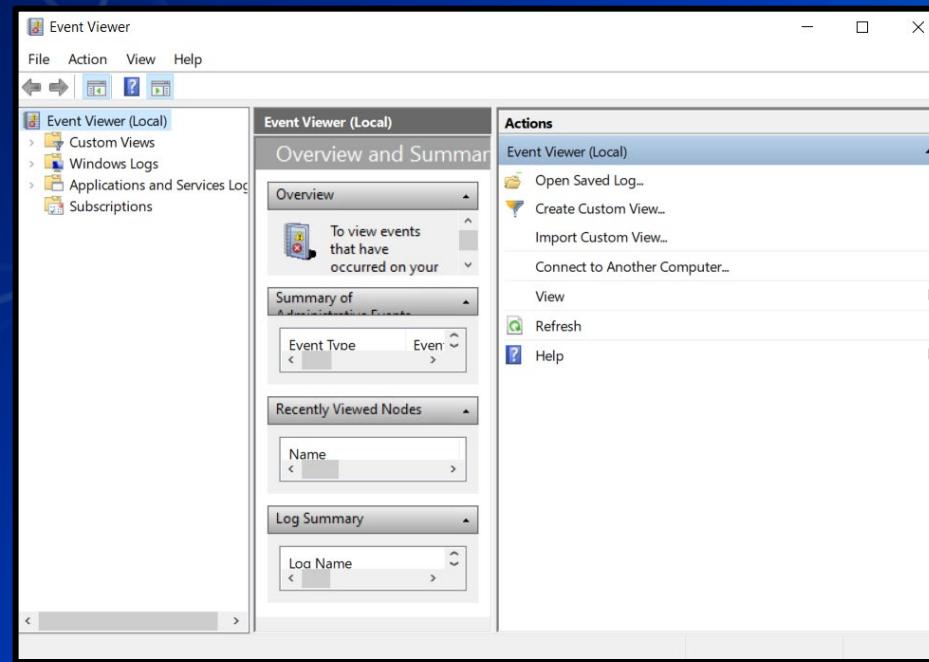
Task Manager cont.



Event Viewer

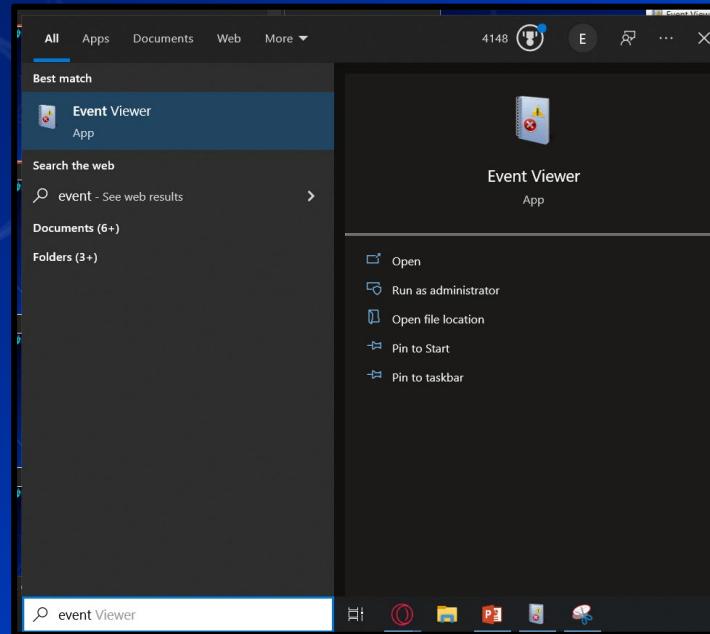
Event Viewer

■ Log viewer for Windows



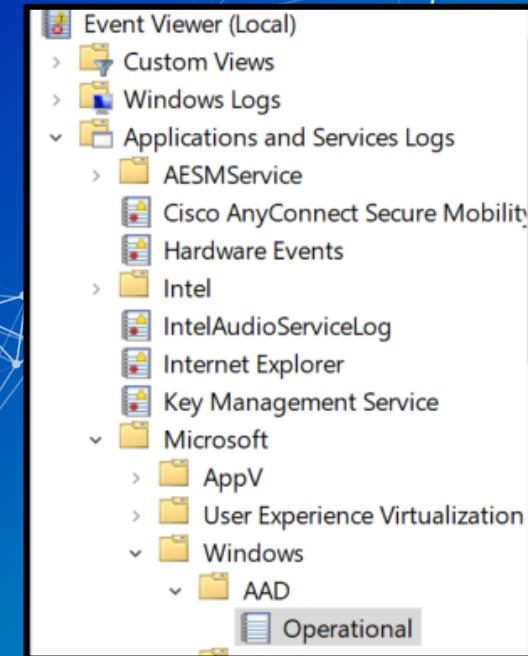
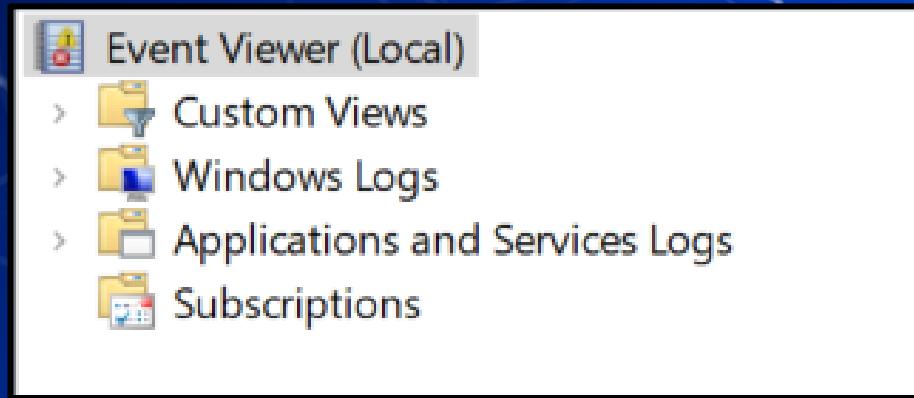
Event Viewer

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



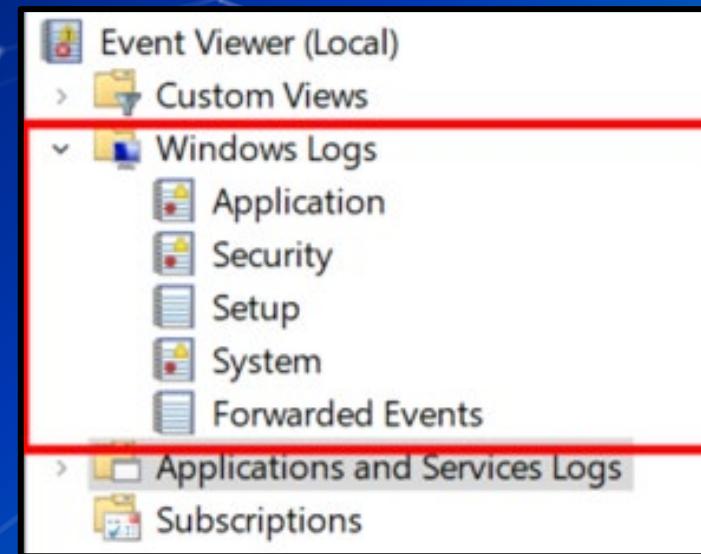
Event Viewer cont.

- Logs are stored in a hierarchical structure



Event Viewer cont.

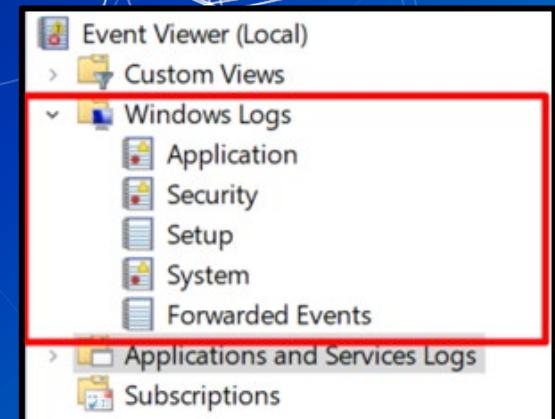
- Windows activities are stored within the "Windows Logs" folder



Event Viewer cont.

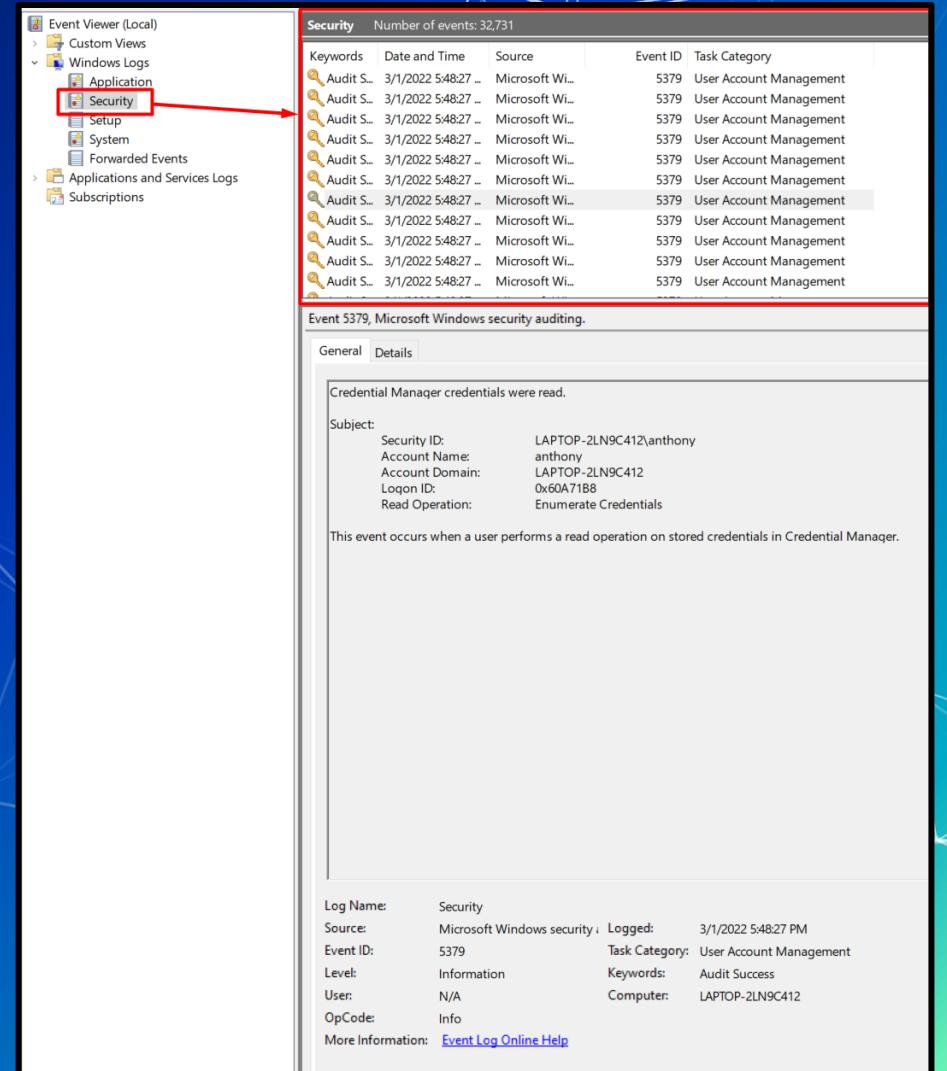
- Windows Logs are divided into 5 categories

- 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
Event ID:	4624
Level:	Information
User:	N/A
OpCode:	Info
Logged:	2/28/2022 4:53:53 PM
Task Category:	Logon
Keywords:	Audit Success
Computer:	LAPTOP-2LN9C412
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

Encyclopedia

- All Event IDs
- Audit Policy

Go To Event ID: 4624 | Go

Security Log | Quick Reference Chart

Windows Security Log Events

Sources:

- 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	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 (!) 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:	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:

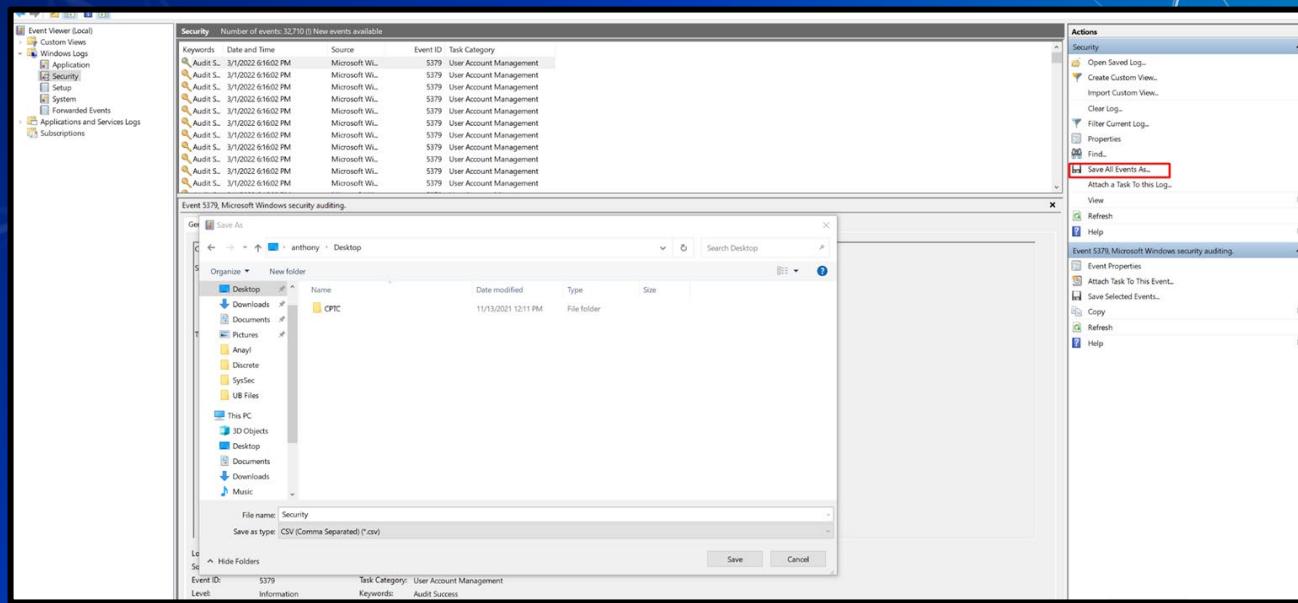
Process ID:	0x470
Process Name:	C:\Windows\System32\services.exe

Network Information:

Log Name:	Security
Source:	Microsoft Windows security
Event ID:	4624
Level:	Information
User:	N/A
OpCode:	Info
Keywords:	Audit Success
Computer:	LAPTOP-2LN9C412
Logged:	3/1/2022 6:13:59 PM
Task Category:	Logon
More Information:	Event Log Online Help

Event Viewer cont.

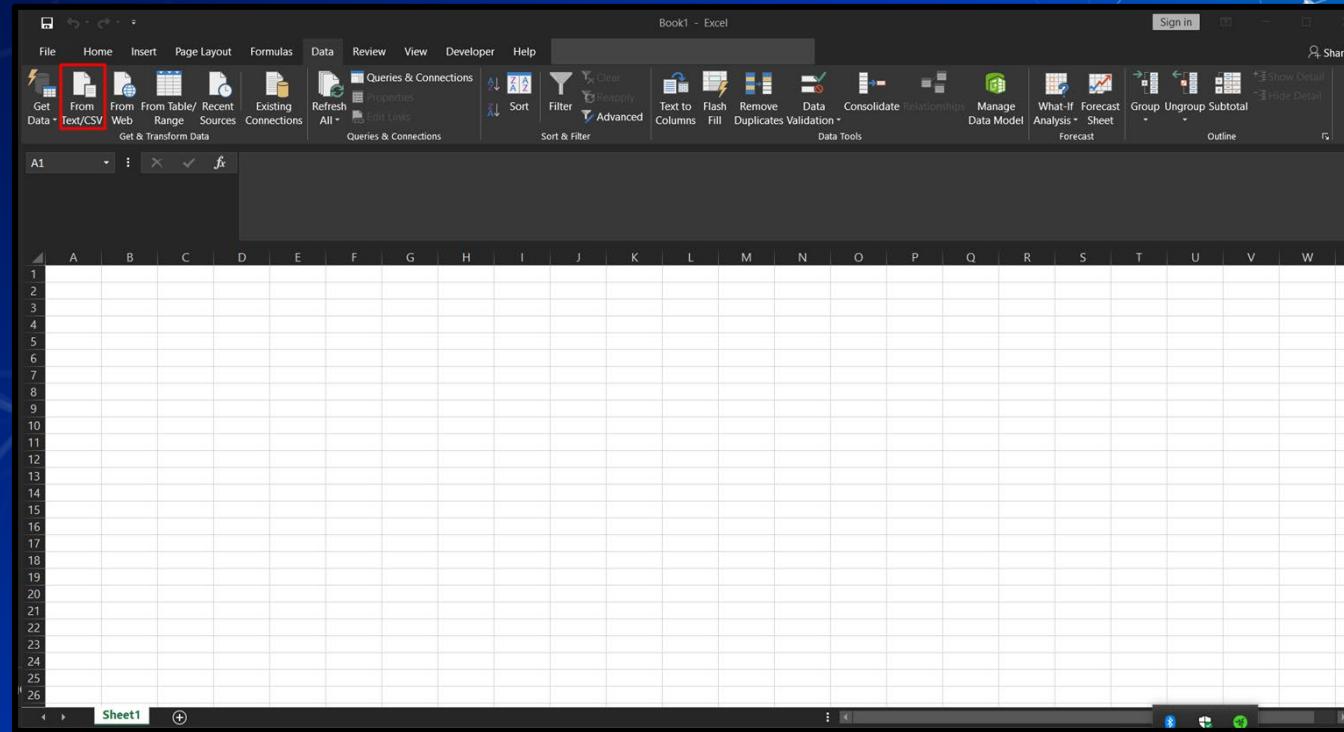
- Event viewer sucks when trying to search logs in bulk.
- We can extract logs to a CSV file



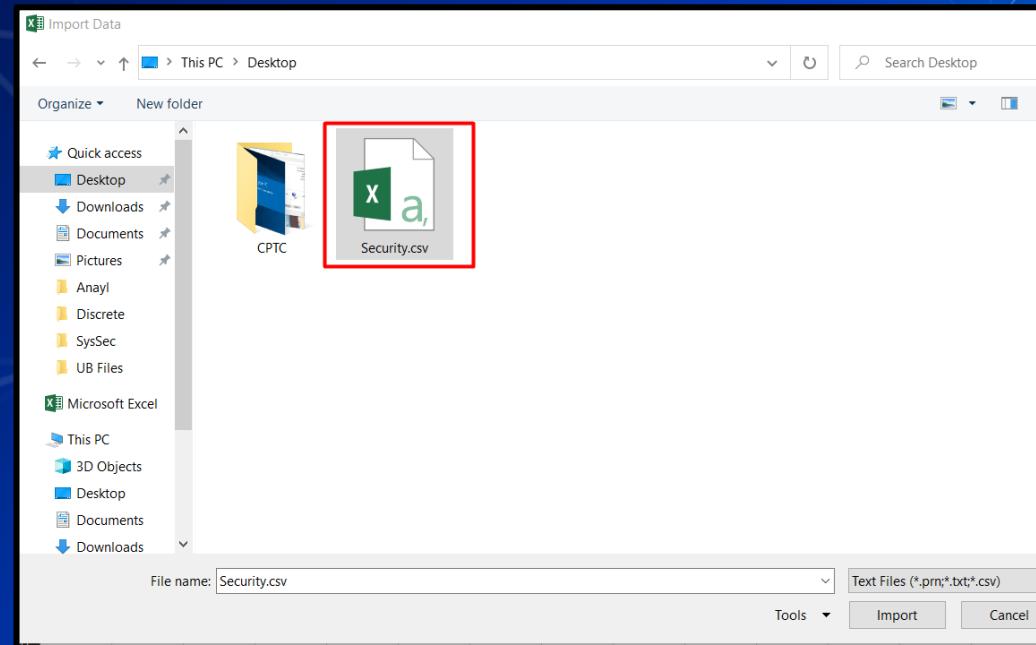
Event Viewer cont.

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

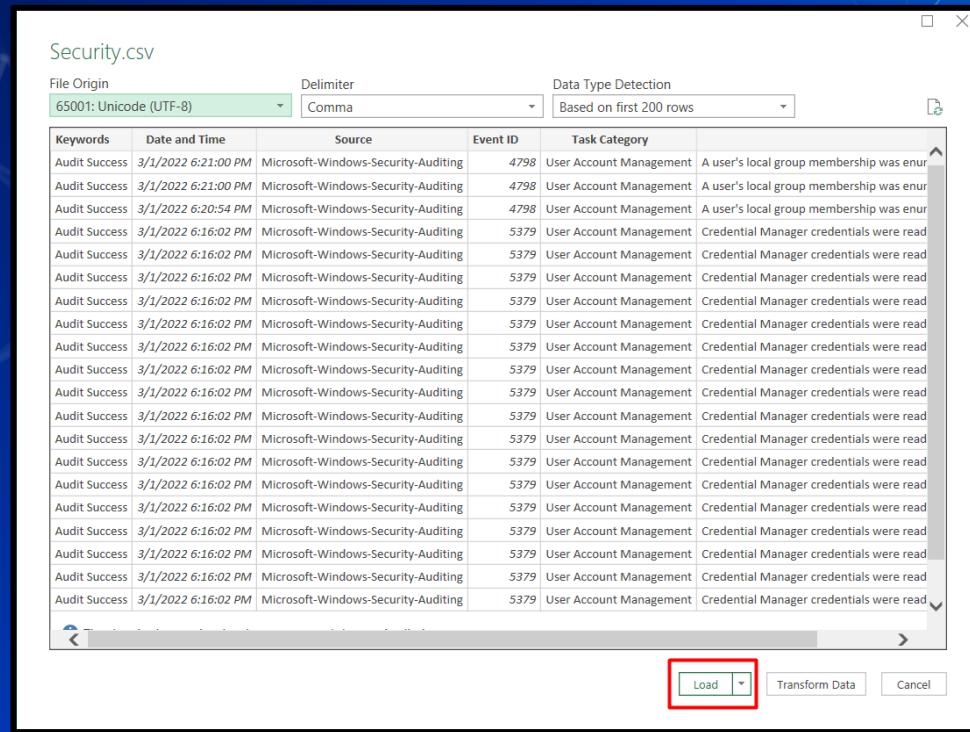
Importing Logs in Excel



Importing Logs in Excel



Importing Logs in Excel





Logs in Excel

Logs in Excel

Within Excel we can search logs using filters.



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?

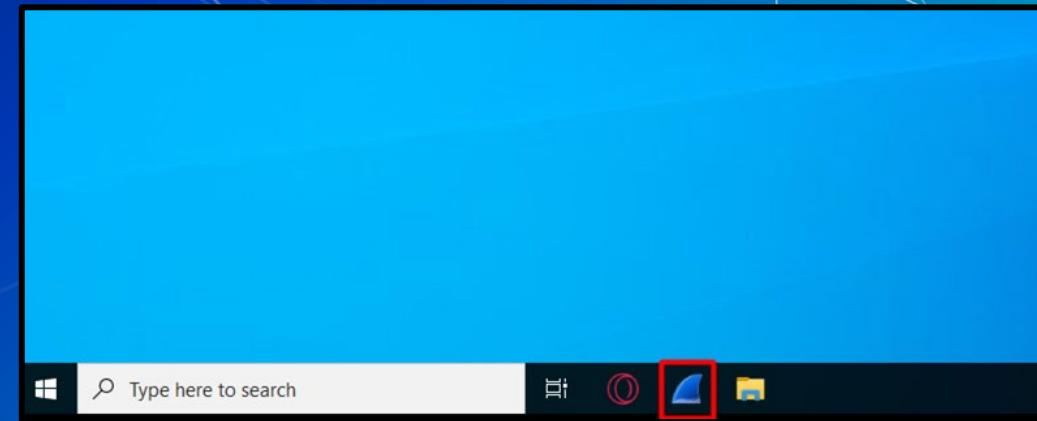
Network Forensics

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



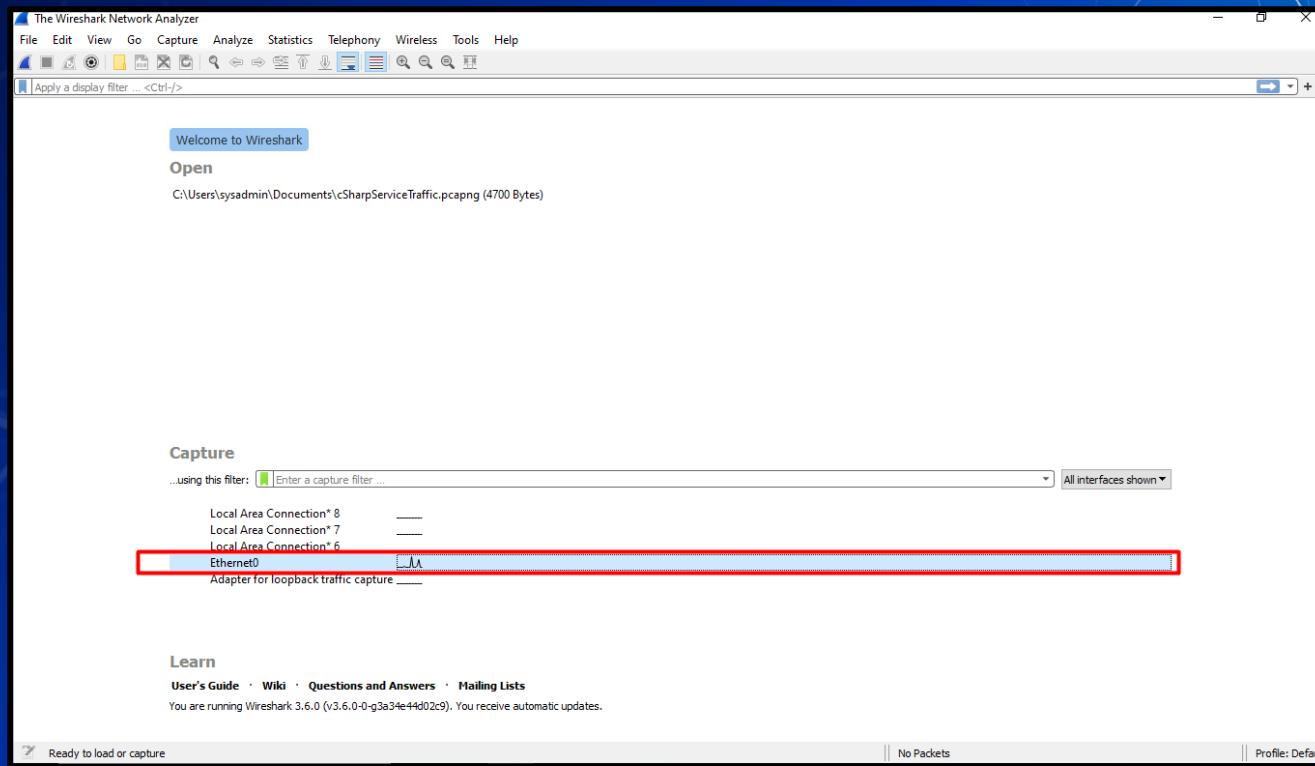
In Class Activity

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 (AppXVC)
Stopped	AssignedAccessM...	AssignedAccessManager Service
Running	AudioEndpointBuilder	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	BattleEye Service
Running	BFE	Base Filtering Engine
Stopped	BITS	Background Intelligent Transfer Ser...
Stopped	BluetoothUserService...	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	cphs	Intel(R) Content Protection HECC 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	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>

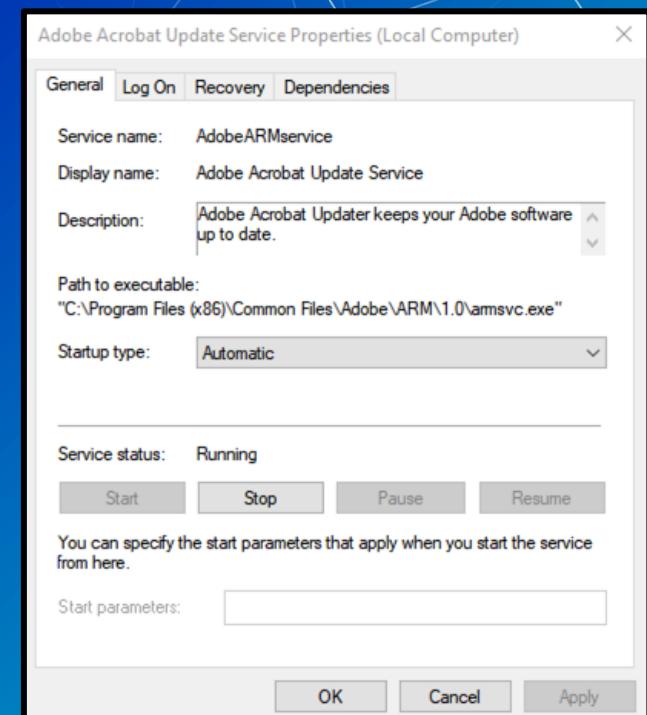
WMI & Services

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

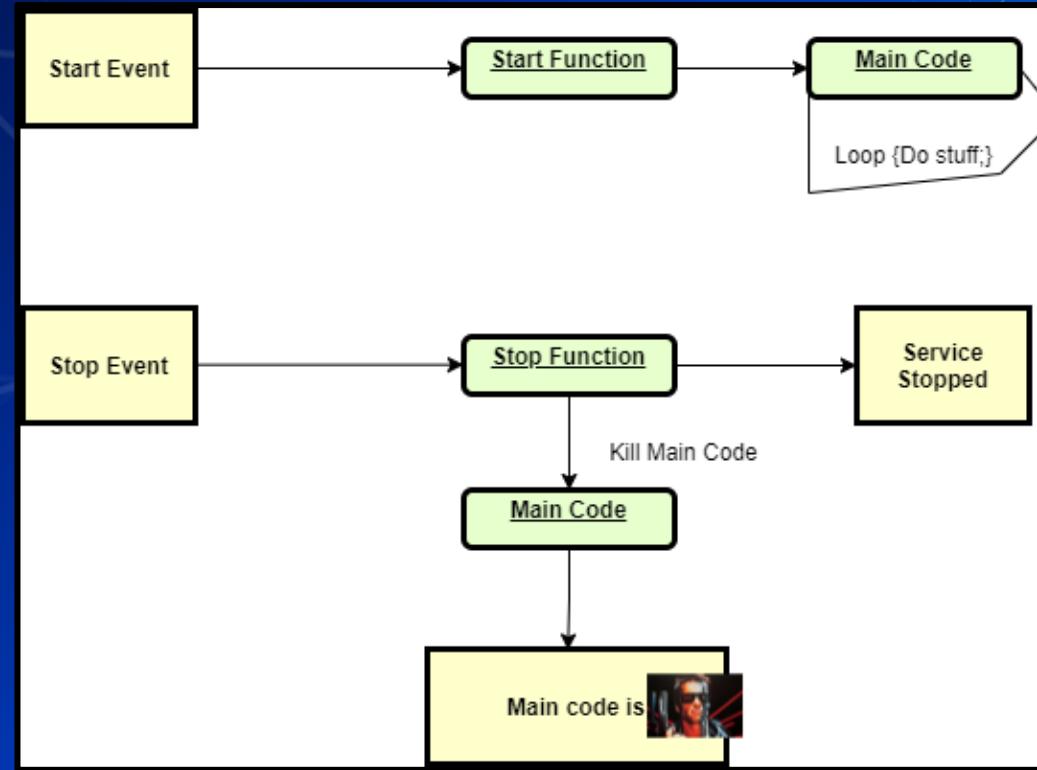
- Behind the scenes to keep things working
- 4 startup types
 - Automatic (Delayed Start)
 - Automatic
 - Manual
 - Disabled



Services

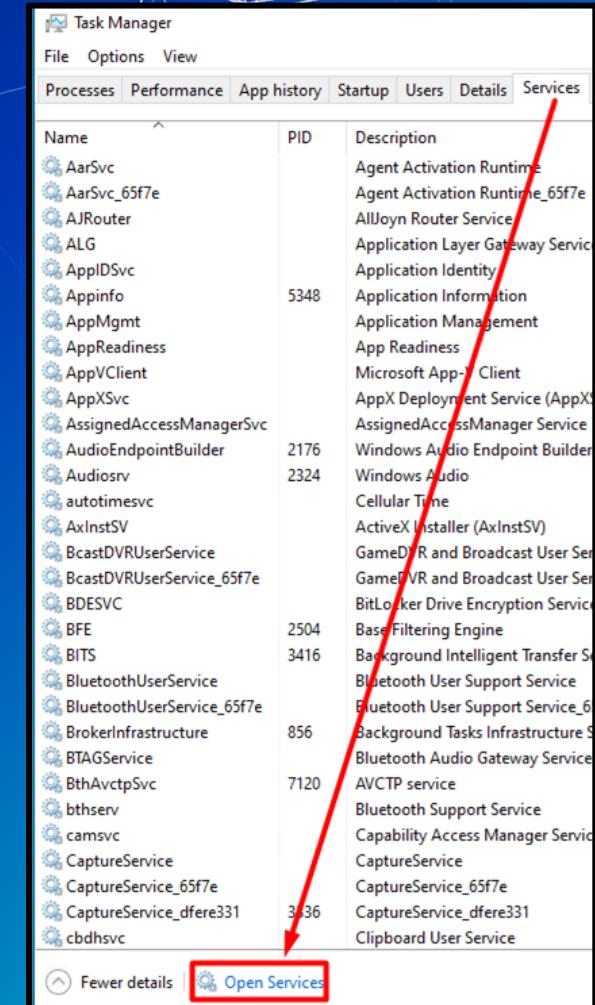
- Can run as nt authority \system
 - nt authority \system != root
 - Is more powerful than an "administrator"
- Active even when no user is signed in
- May be hosted by the service host (svchost.exe)
- May have executables that are designated to be services
- Follow a defined service model

Service Model



How to list services?

- Open Task Manager and navigate to services tab

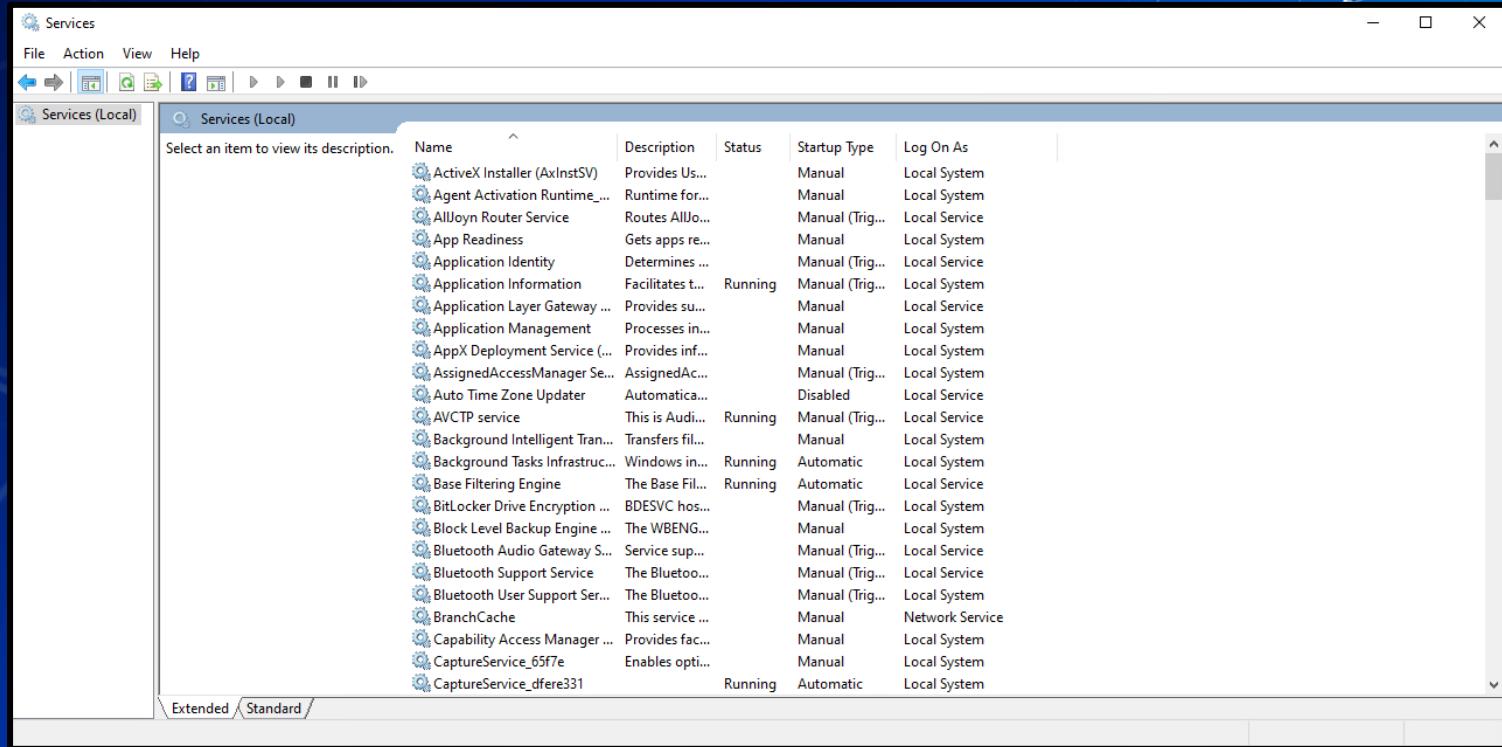


The screenshot shows the Windows Task Manager window with the "Services" tab selected. The table lists various system services with their names, Process IDs (PID), and descriptions. A red arrow points from the top right towards the "Open Services" button at the bottom right of the window.

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		GameDVR 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 standard navigation buttons. Below the toolbar is a search bar and a link to "Services (Local)". A message "Select an item to view its description." is displayed above the table. The main area is a table with columns: Name, Description, Status, Startup Type, and Log On As. The table lists numerous system services, such as ActiveX Installer, Agent Activation Runtime, AllJoyn Router Service, App Readiness, Application Identity, Application Information, Application Layer Gateway, Application Management, AppX Deployment Service, AssignedAccessManager, Auto Time Zone Updater, AVCTP service, Background Intelligent Trasnfer, Background Tasks Infrastructure, Base Filtering Engine, BitLocker Drive Encryption, Block Level Backup Engine, Bluetooth Audio Gateway, Bluetooth Support Service, Bluetooth User Support Service, BranchCache, Capability Access Manager, CaptureService_65f7e, and CaptureService_dffere331. Most services are set to Manual startup type and Local System log on. Some services like Background Intelligent Trasnfer and Background Tasks Infrastructure are set to Automatic startup type. The status column shows several services as Running.

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 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_dffere331	Running	Automatic	Local System	

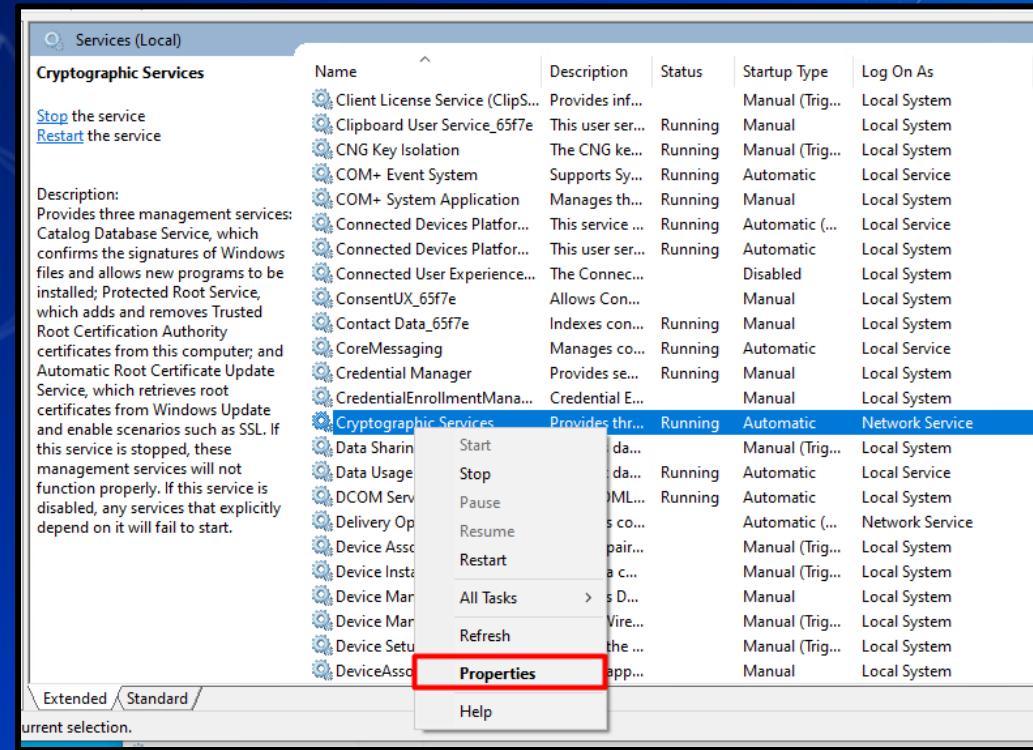
Extended Standard

Services List

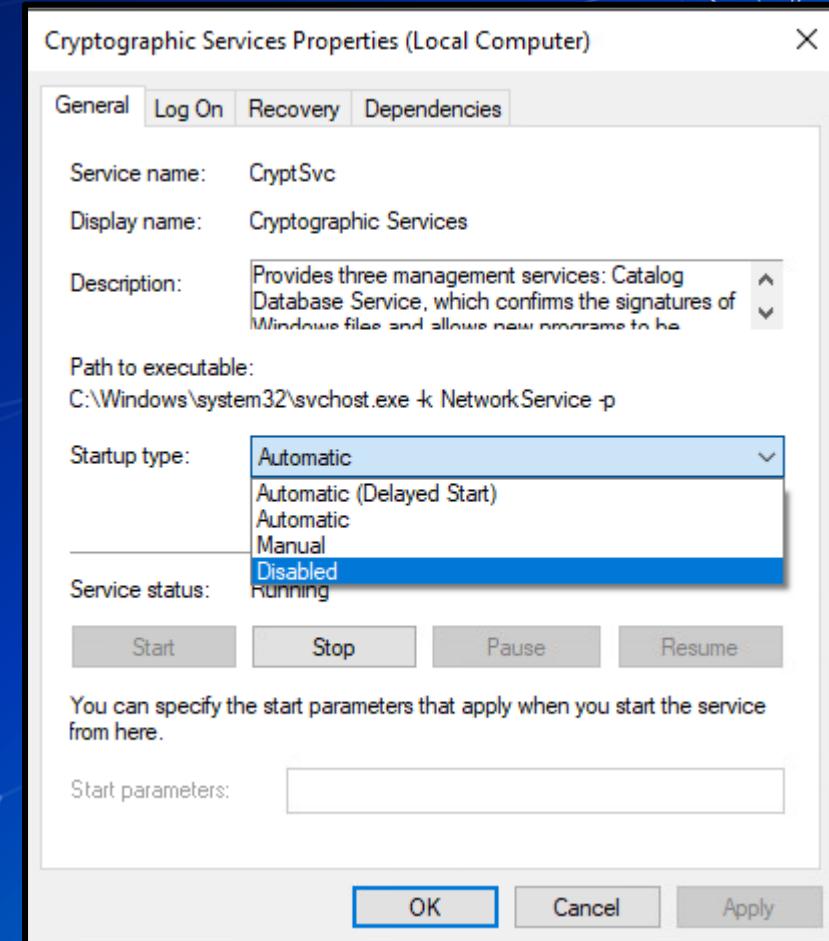
Services (Local)					
Cryptographic Services					
Stop the service Restart the service					
Description: Provides three management services: Catalog Database Service, which confirms the signatures of Windows files and allows new programs to be installed; Protected Root Service, which adds and removes 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	

Extended Standard

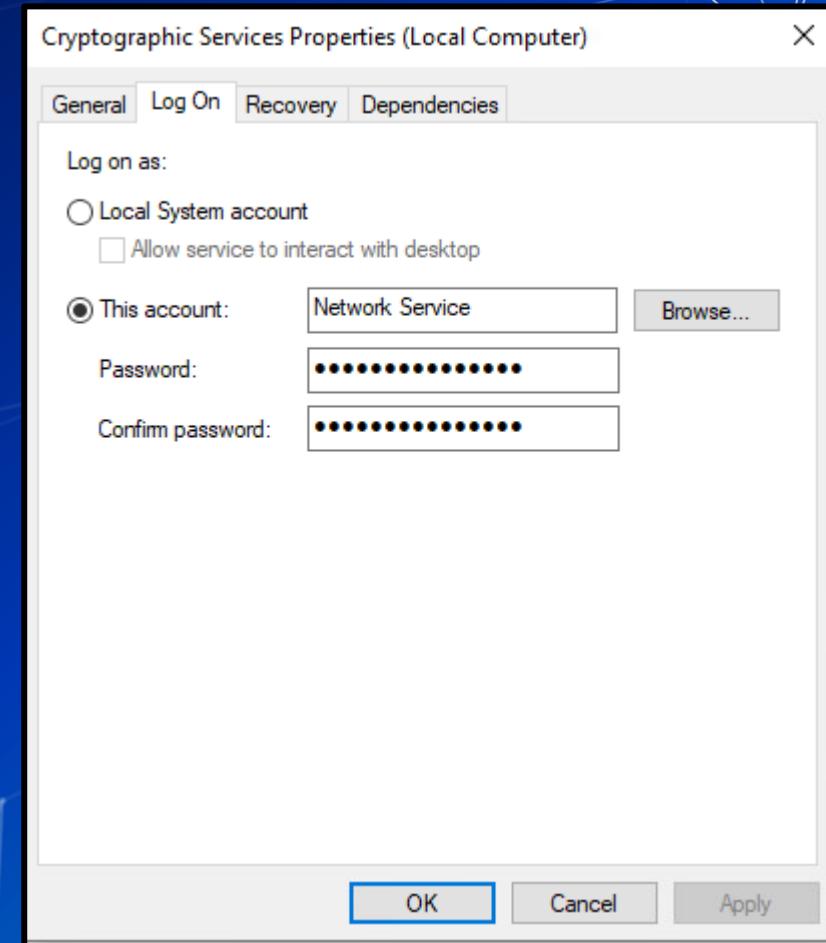
Services List



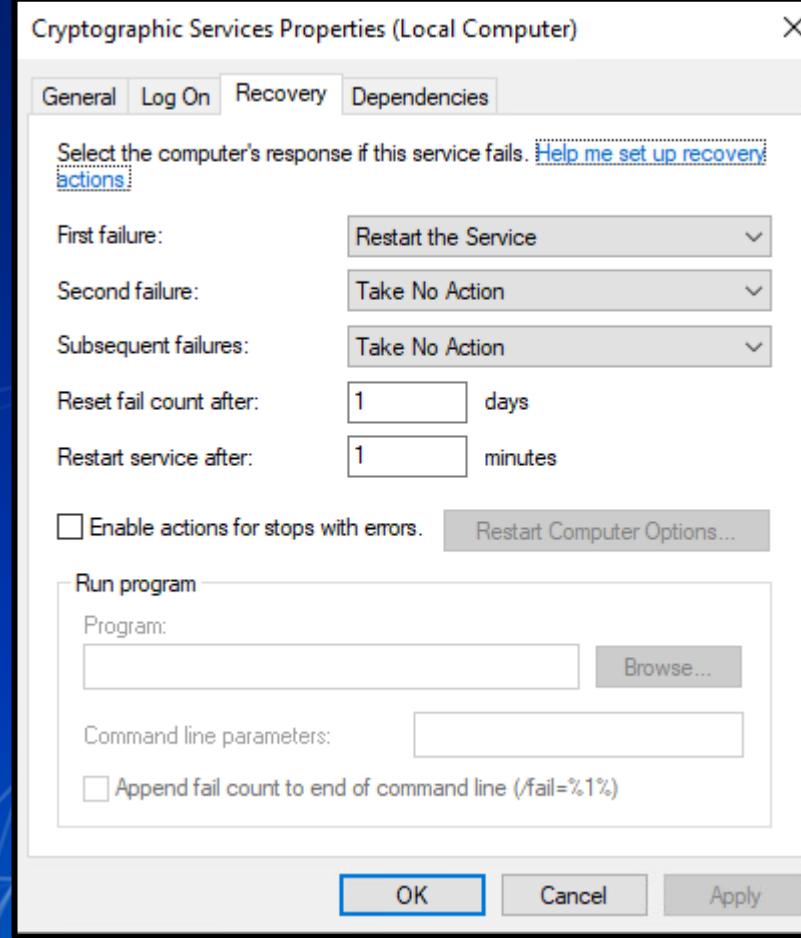
Services List



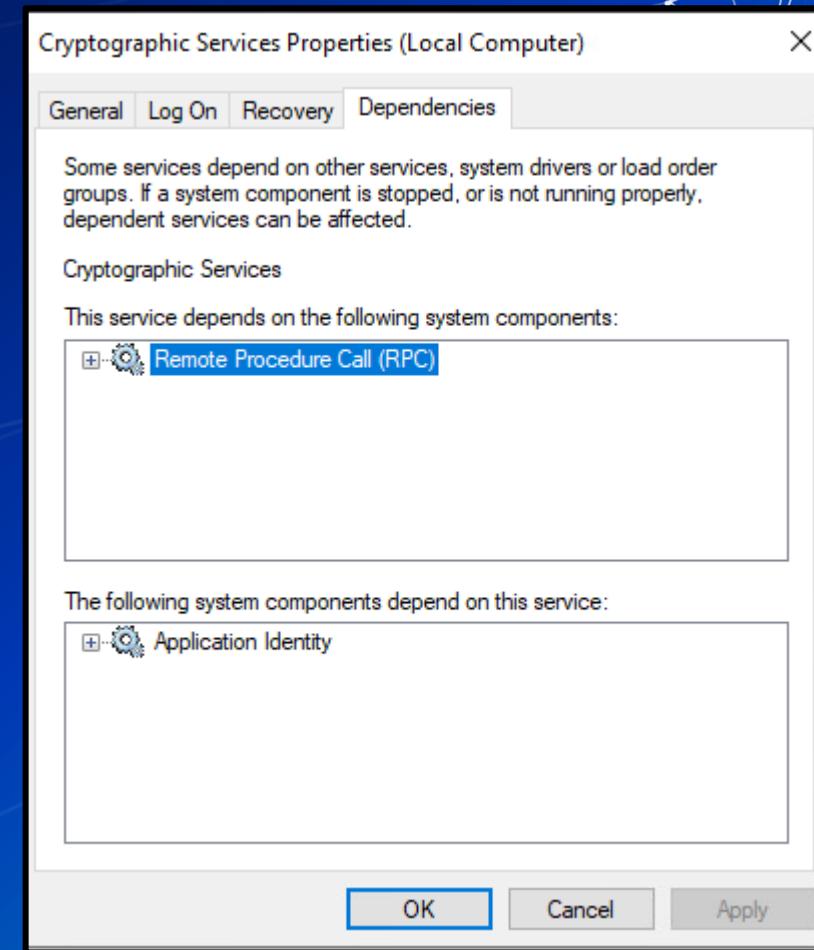
Services List



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

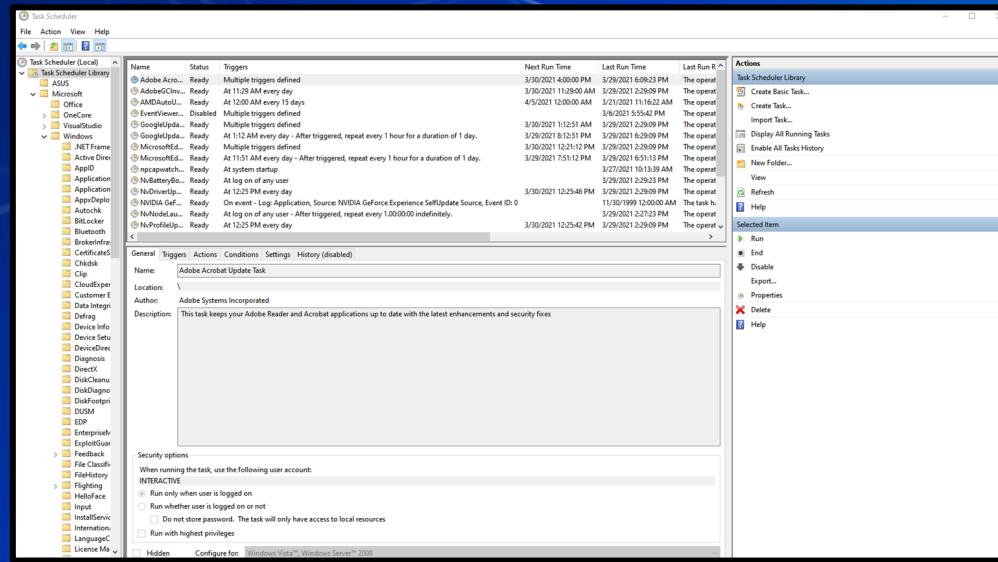
- Registry Editor is a GUI way of viewing registry
 - **Get-ItemProperty** can be used as well
 - <https://tinyurl.com/9hbeh72f>
- Two directories for running at sign on
 - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

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
>	MicrosoftEdge	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	
>	(Default)	REG_SZ	(value not set)
>	RtkAudUService	REG_SZ	"C:\Windows\System32\DriverStore\FileRepository_...
>	SecurityHealth	REG_EXPAND_SZ	
>	SteelSeriesGG	REG_SZ	"C:\Program Files\SteelSeries\GG\SteelSeriesGG.ex...

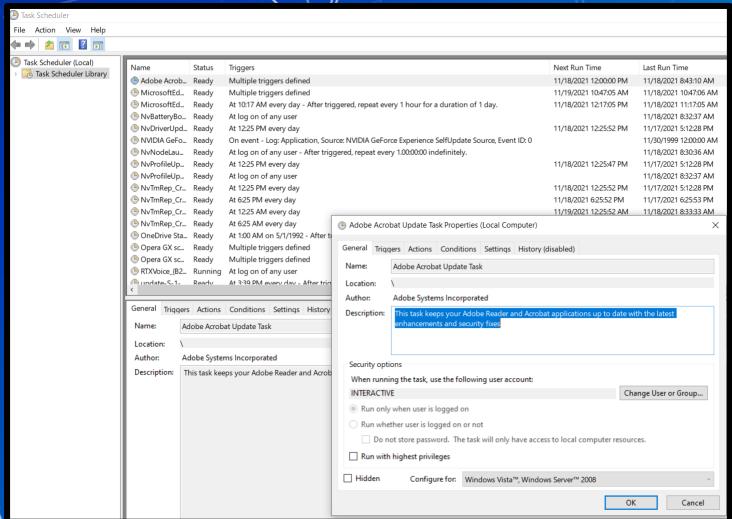
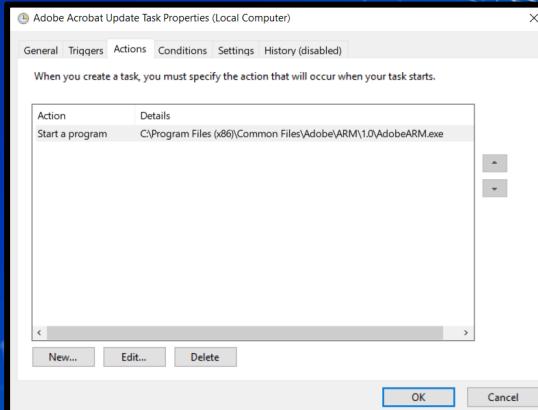
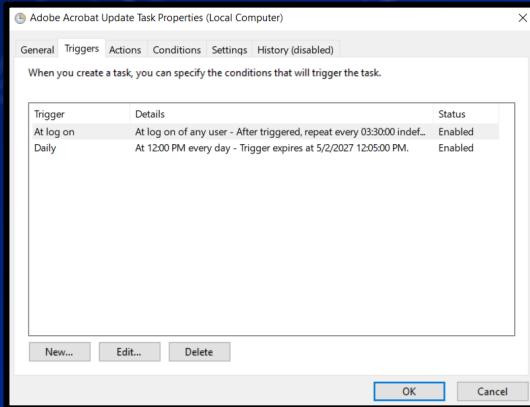
Scheduled Tasks

- 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?



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

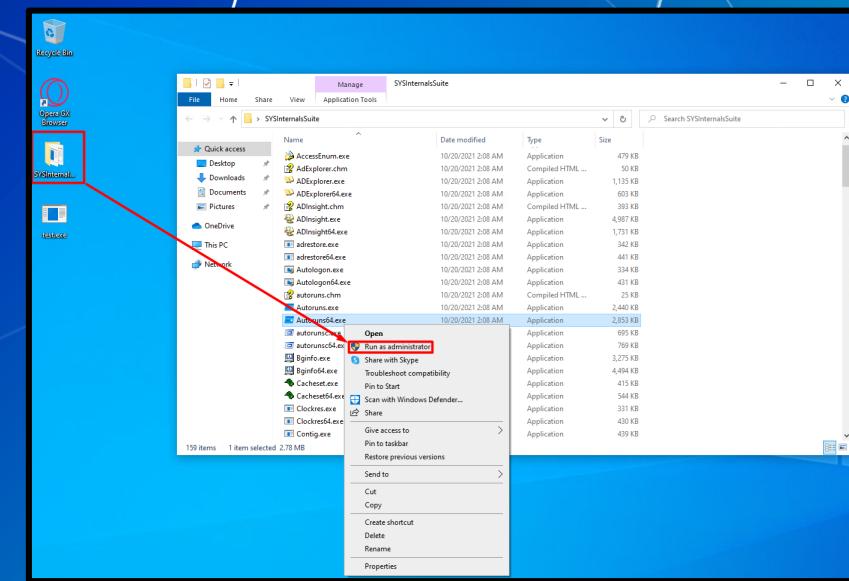
- Group policies can soften the security posture of a device
 - Disable anti-virus
 - Turn off or flood logs
 - Disable firewalls
 - And more!
- Group Policies can be used to establish registry based persistence
- Malicious group policies are very dangerous

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 – Combating Persistence

Categories of persistence

Autonyms - Sysinternals: www.sysinternals.com [Administrator] [DESKTOP-7A15TS1\sysadmin]						
File		Search	Entry	User	Options	Category
Autonyms Entry	Description	Publisher	Image Path	Timestamp	Virus Total	
↳ 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...	(Not Verified)	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Wed Apr 21 13:46:46 2021		
↳ Npcapwatchdog			C:\Program Files\Npcap\CheckStatus.bat	Thu Nov 18 13:58:11 2021		
↳ OneDrive Standalone Update Task-5-1-5-21-1961932216-26321...	Standalone Updater	(Verified) Microsoft Corporation	C:\Users\sysadmin\AppData\Local\Microsoft\OneDrive\standaloneUpdater.exe	Thu Nov 4 10:00:01 2021		
↳ Opera GX scheduled assistant Autoupdate 1637272882	Opera GX 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 1634717190	Keeps Opera up to date	(Verified) Opera Software AS	C:\Users\sysadmin\AppData\Local\Programs\Opera GX\launcher.exe	Thu Nov 4 10:00:01 2021		
↳ VMwareToolUpdator	Windows PowerShell	(Verified) Microsoft Windows	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Mon Mar 12 14:46:56 2019		
Services						
↳ Autonyms CurrentControlSet\Services						
↳ msbuild	Microsoft Edge Update Service (msbuild...)	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Nov 18 16:41:54 2021		
↳ msbuildupdate	Microsoft Edge Update Service (msbuild...)	(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\95.0.1020.59\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.exe	Wed Oct 20 01:22:21 2021		
↳ NetTcpPortSharing	Net Tcp Port Sharing Service: Provides abi...	(Verified) Microsoft Corporation	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSMSvcHost.exe	Fri Dec 6 22:03:03 2019		
↳ VgAuthService	Vmware Alias Manager and Ticket Service...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\VGAuthService.exe	Sat Apr 14 09:42:20 2018		
↳ VMSvc	Vmware Helper Service: Helps VMw...	(Verified) VMware, Inc.	C:\Windows\system32\vm3dservice.exe	Mon Feb 22 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\vmacthlp.exe	Sat Apr 14 09:43:46 2018		
↳ VMwareCAFCommAmpListener	Vmware CAF AMQP Communication Ser...	(Not Verified)	C:\Program Files\VMware\VMware Tools\VMware CAF\pmme\bin\CommAmpListener.exe	Sat Apr 14 09:24:46 2018		
↳ VMwareCAFManagementAgentHost	Vmware CAF Management Agent Service...	(Not Verified)	C:\Program Files\VMware\VMware Tools\VMware CAF\pmme\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 09:58:58 2018		
Drivers						
↳ HKLM\Serial\CurrentControlSet\Services						
↳ iklPS55_GPIOD	Intel(R) Serial I/O GPIO Controller Driver: I...	(Verified) Intel Corporation - Client...	C:\Windows\System32\drivers\iklPS55_GPIOD.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 12 14:46:53 2019		
↳ vmbnmp	vmBnmp: VMware SVGA 3D Minipor...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vmBnmp.sys	Wed Apr 21 11:59:41 2021		
↳ vmbnmp-debug	vmbnmp-debug: VMware SVGA 3D Minip...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vmBnmp-debug.sys	Sat Apr 14 10:02:02 2018		
↳ vmbnmp-stats	vmbnmp-stats: VMware SVGA 3D Minipor...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vmBnmp-stats.sys	Sat Apr 14 10:02:02 2018		
↳ vmbnmp-jeeder	vmbnmp-jeeder: VMware SVGA 3D Minip...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vmBnmp_jeeder.sys	Sat Apr 14 10:02:02 2018		
↳ vmd	vmd: VMware VMCI Bus Driver: VMware PCI...	(Verified) VMware, Inc.	C:\Windows\System32\drivers\vmci.sys	Wed Nov 29 09:10:32 2017		
↳ vmbgfs	Vmware Hot Guest Client Redirector: Im...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vmhgfs.sys	Sat Apr 14 09:55:48 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		
↳ vmrwdsck	Vmware Physical Disk Helper: VMware Ph...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vmrwdsck.sys	Sat Apr 14 09:55:04 2018		
↳ vrmouse	Vmware USB Pointing Device: VMware Po...	(Verified) VMware, Inc.	C:\Windows\System32\drivers\vmrmouse.sys	Sat Apr 14 09:57:32 2018		
↳ vnetWFP	vnetWFP: Guest Introspection Network Fil...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vnnetWFP.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\vssock.sys	Wed Nov 29 09:10:32 2017		
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Font Drivers						
↳ MSBuild	Size: 62,080 K	Time: Wed Oct 20 01:22:21 2021				
	(Not Verified) ©Microsoft Corporat...	16.9.0.195				
	C:\Program Files (x86)\Microsoft .NET\Redist\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	(Verified) Microsoft Corporation	C:\Users\sysadmin\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe	Thu Nov 18 13:56:11 2021		
	Opera GX scheduled assistant Autoupdate 1637272882	(Verified) Open Software AS	C:\Users\sysadmin\AppData\Local\Programs\Opera GX\launcher.exe	Thu Nov 4 10:00:11 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		
	Keep Opera up to date.	(Verified) Microsoft Windows	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Mon Mar 18 21:46:56 2019		
Services						
HKL\SYSTEM\CurrentControlSet\Services						
	edgeupdate	Microsoft Edge Update Service (edgeupdate...)	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Update\MicrosoftEdgeUpdate.exe	Thu Nov 18 16:41:54 2021	
	edgeupdateatom	Microsoft Edge Update Service (edgeupdate...)	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Update\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021	
	MicrosoftEdgeElevationService	Microsoft Edge Elevation Service (Microso...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\95.0.1020.51\msedge_elevation_service.exe	Thu Nov 18 13:56:29 2021	
	MSBuild	MSBuild Provides Just-in-time compilati...	(Not Verified) Microsoft Corpor...	C:\Program Files (x86)\Microsoft .NET\Redist\list\MSBuild.exe	Wed Oct 20 01:22:21 2021	
	NetLsIoSharing	Net Ls Io Sharing Service: Provides ab...	(Verified) Microsoft Corporation	C:\Windows\Microsoft.NET\Framework64\v4.0.3019\SMSSvcHost.exe	Fri Dec 6 22:03:03 2019	
	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	
	vMSOService	VMware SVGA Helper Service: Helps VMw...	(Verified) VMware, Inc.	C:\Windows\system32\vmwservice.exe	Mon Feb 22 02:55:32 2021	
	VMTools	VMware Tools: Provides support for sync...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Sat Apr 14 09:58:32 2018	
	VMwarePhysicalDiskHelperService	VMware Physical Disk Helper Service: Ena...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmchilp.exe	Sat Apr 14 09:54:36 2018	
	VMwareCAFComAmpListener	VMware CAF AMP Communication Servic...	(Not Verified)	C:\Program Files\VMware\VMware CAF\pmc\bin\CommAmpListener.exe	Sat Apr 14 09:52:46 2018	
	VMwareCAFManagementAgentHost	VMware CAF Management Agent Service: ...	(Not Verified)	C:\Program Files\VMware\VMware Tools\CAF\pmc\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	
Drivers						
HKL\SYSTEM\CurrentControlSet\Services						
	iaLPSI_GIO	Intel(R) Serial IO GPIO Controller Driver: ...	(Verified) Intel Corporation - Client	C:\Windows\System32\drivers\iaLPSI_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 Host Client Redirector: ...	(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\vhmmemctl.sys	Sat Apr 14 09:55:46 2018	
	vmmouse	VMware Pointing Device: VMware Pointin...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vhmmouse.sys	Sat Apr 14 09:56:16 2018	
	vmreadsd	VMware Physical Disk Helper: VMware Ph...	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vmreadsd.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\vnethWF.sys	Sat Apr 14 10:00:44 2018	
	vsepfilt	vsepfilt: Guest Inspection Driver	(Verified) VMware, Inc.	C:\Windows\System32\DRIVERS\vsepfilt.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	
HKL\SOFTWA...						
HKL\SOFTWA...	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	

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/a7jpzmst>
 - <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?