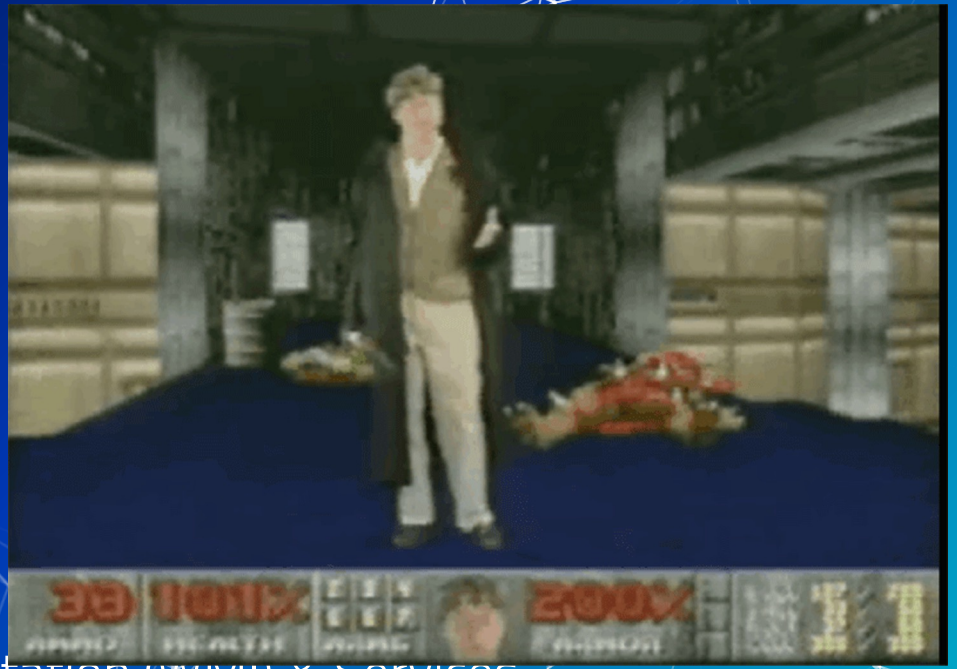
NetDef

Windows Threat Hunting

UBNetDef, Spring 2023
Week 6

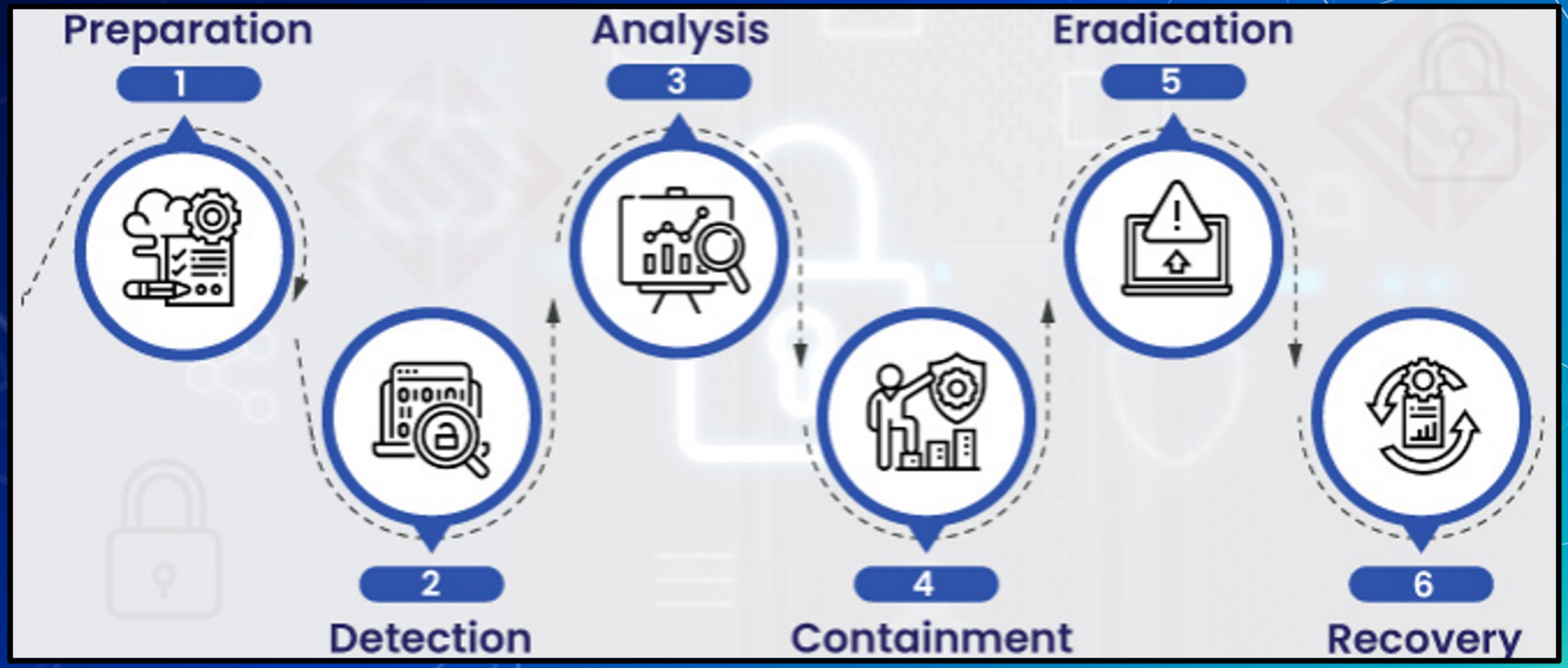
Presenter:
Anthony Magrene & Griffin Refol

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



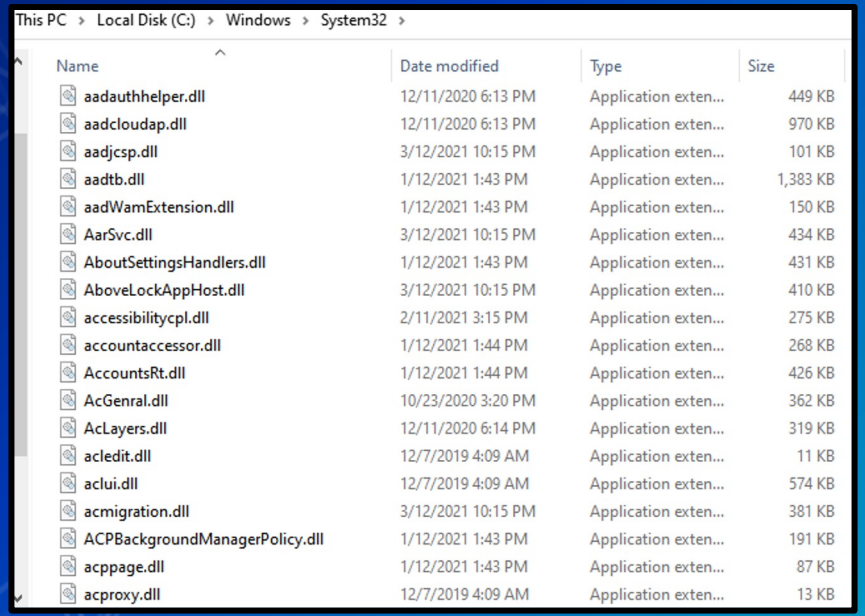
NetDef

Windows Concepts

Notable File Types

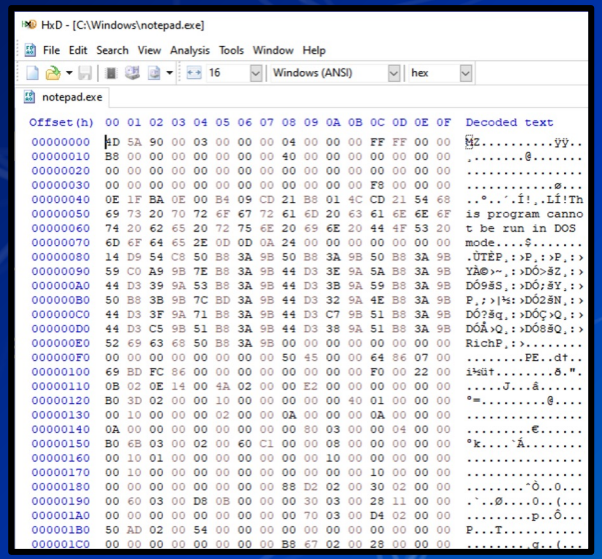
Dynamic Link Library (.dll)

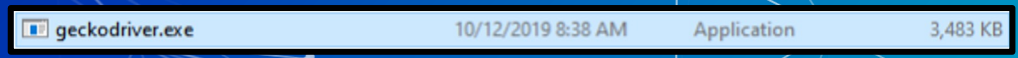
- Windows implementation of shared libraries
- Prevents redundant storage commonly used code



Portable Executable (.exe)

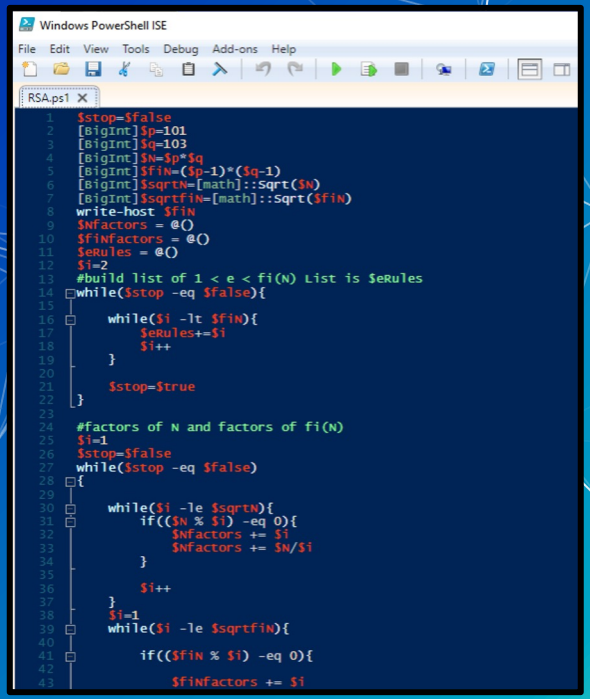
- Machine code that is executed by the operating system
- May be written using high-level languages
  - GO, C++, C, Ruby etc.





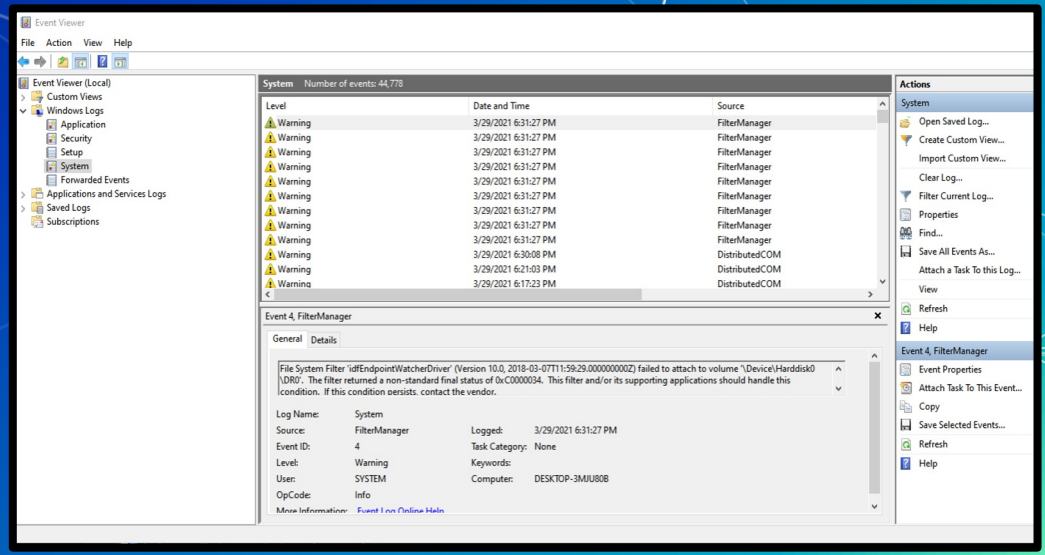
PowerShell Script (.ps1)

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



Event Log (.evtx)

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

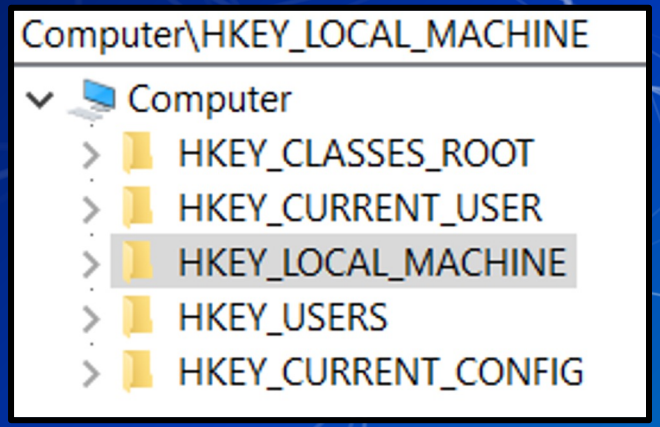


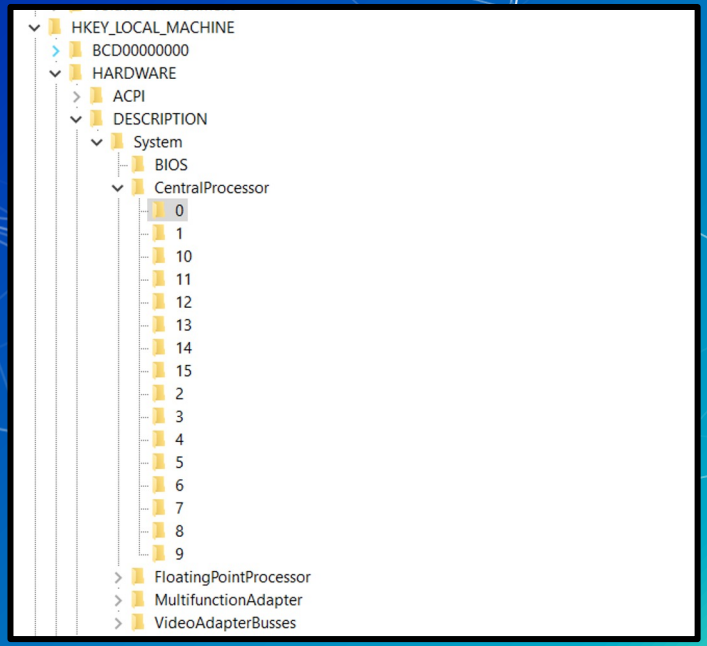
NetDef

The Registry

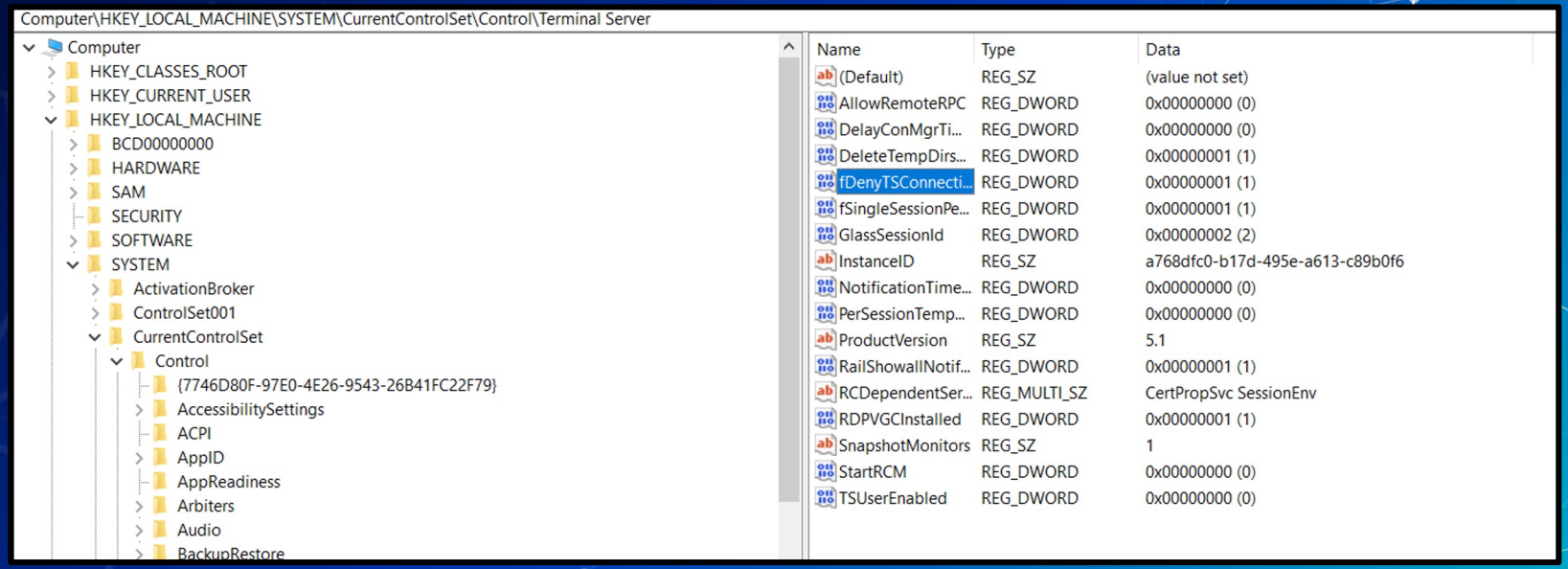
Registry

- Hierarchical database
  - Stores low-level settings

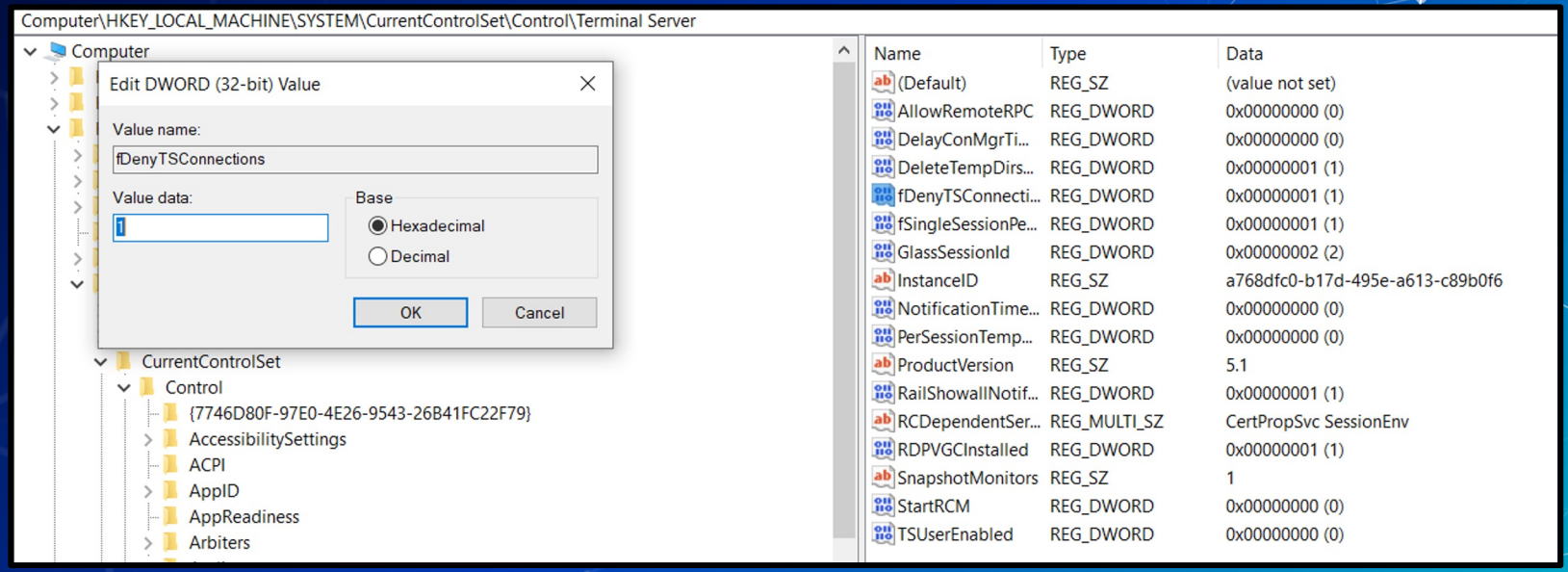




Registry cont.



Registry cont.

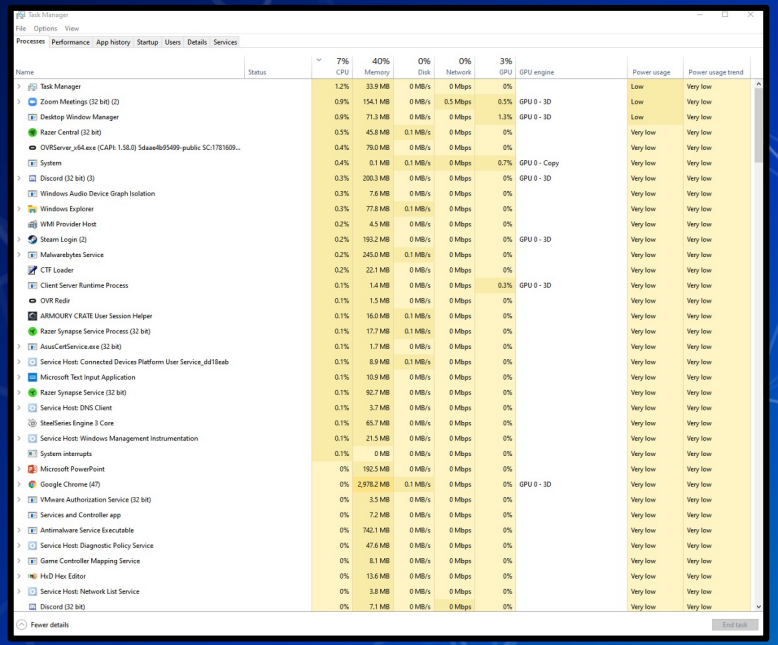


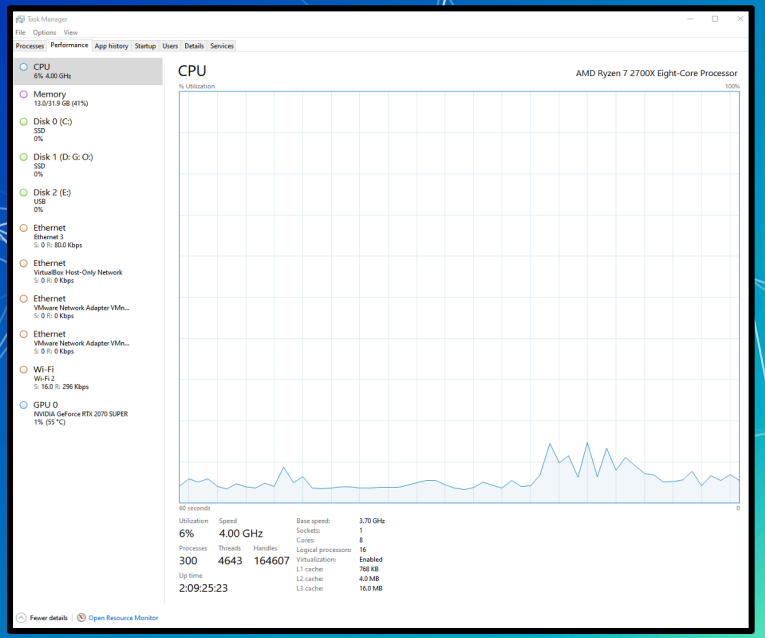
NetDef

Task Manager

Task Manager

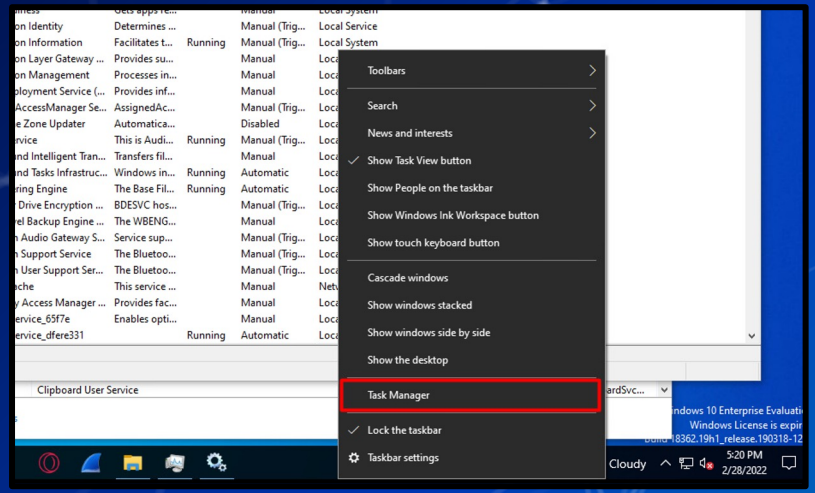
- Provides high-level view of what is running

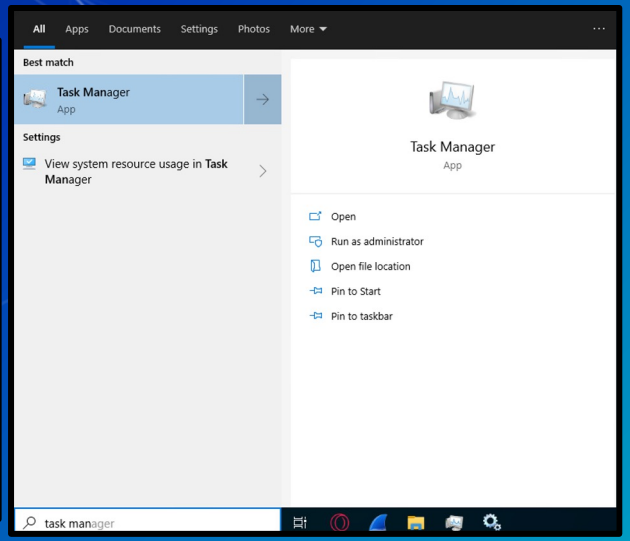


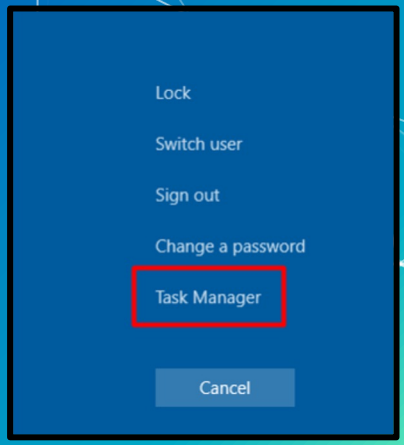


Task Manager cont.

- How to open it?

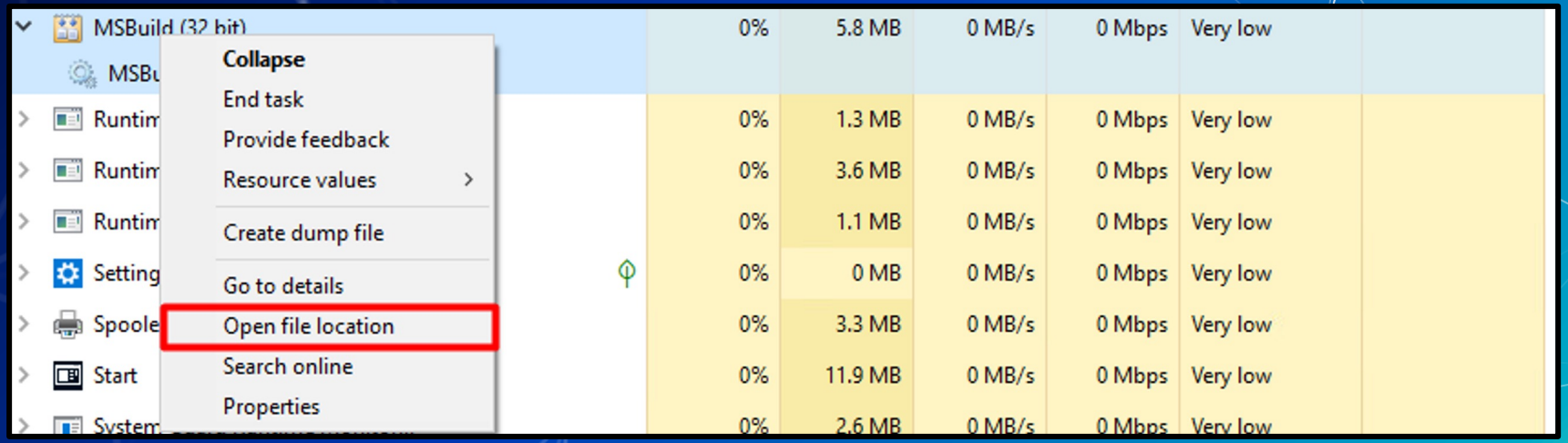






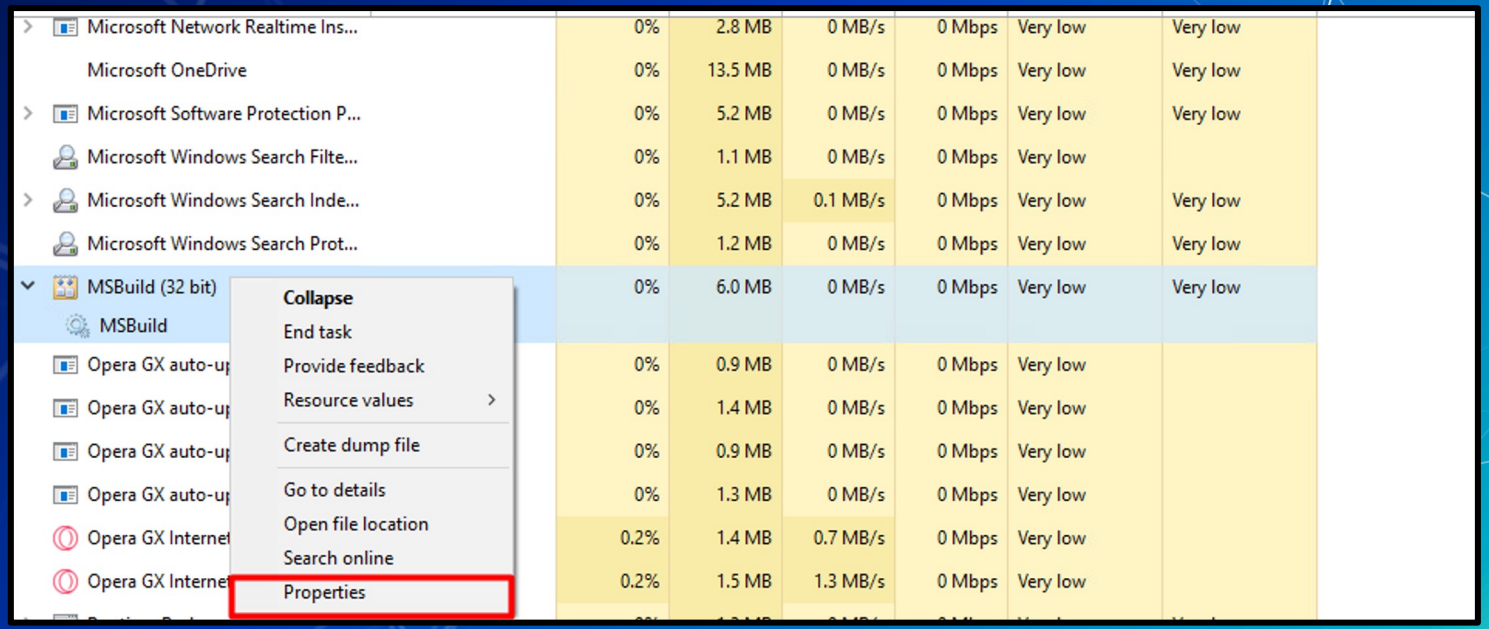
Task Manager cont.

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

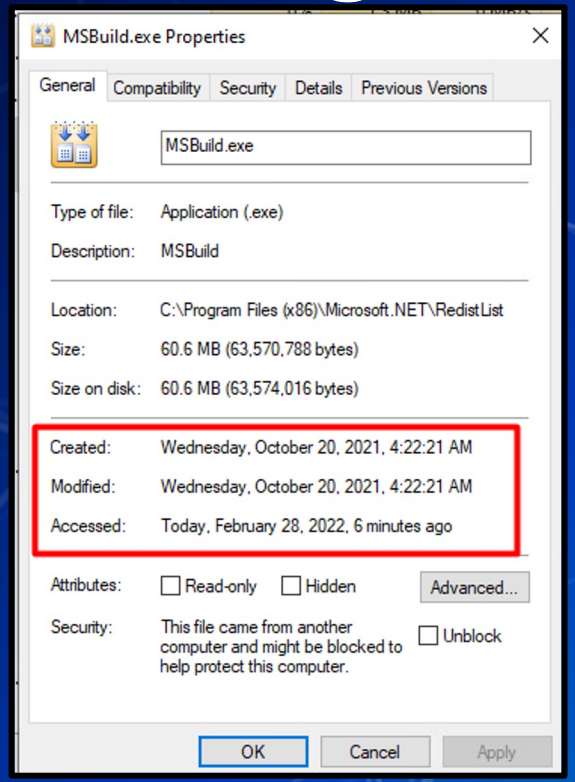


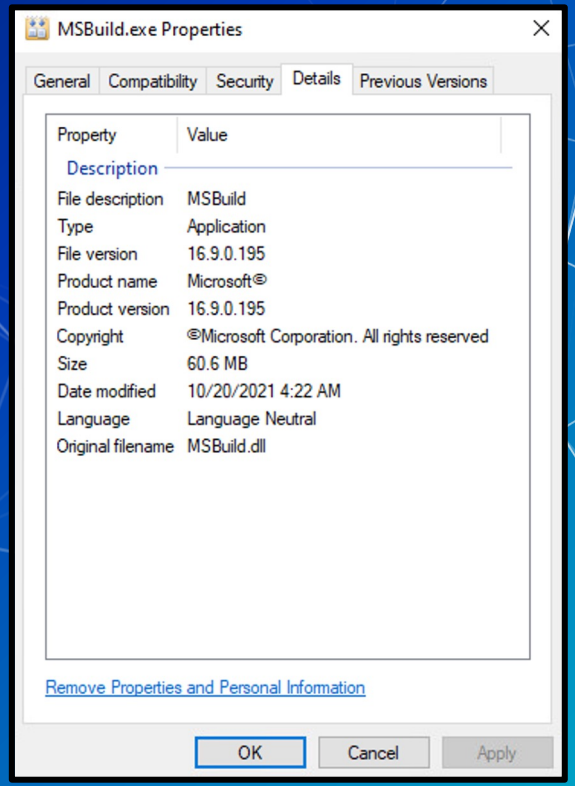
Task Manager cont.

- Show the properties of an executable



Task Manager cont.



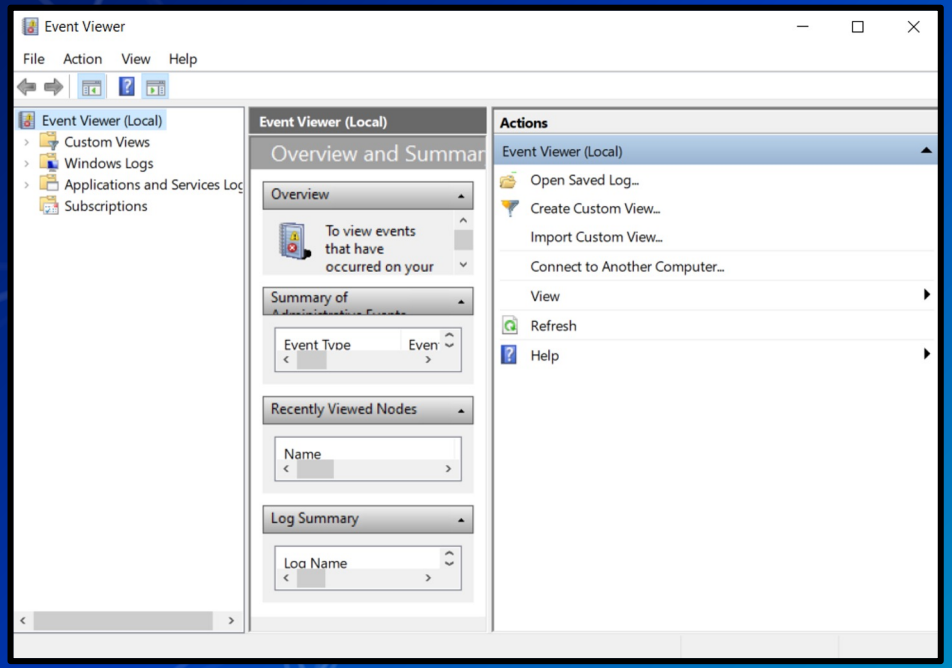


NetDef

Event Viewer

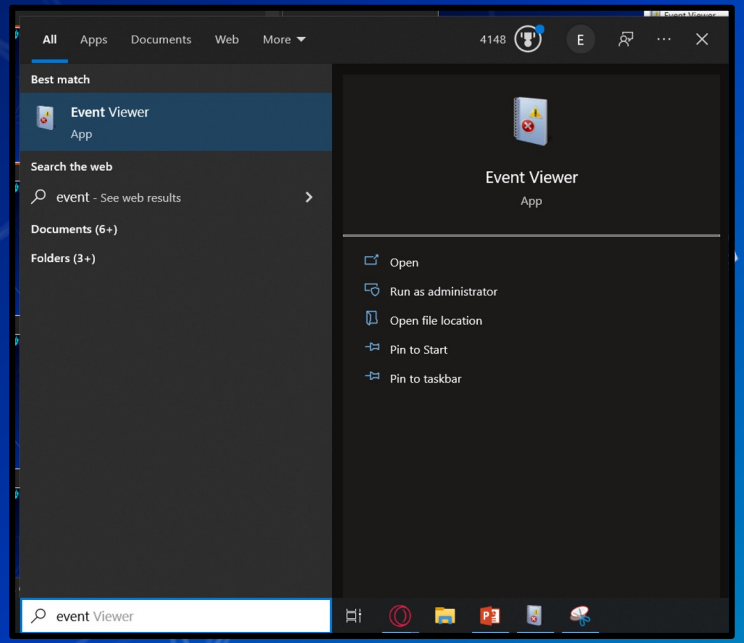
Event Viewer

- Log viewer for Windows



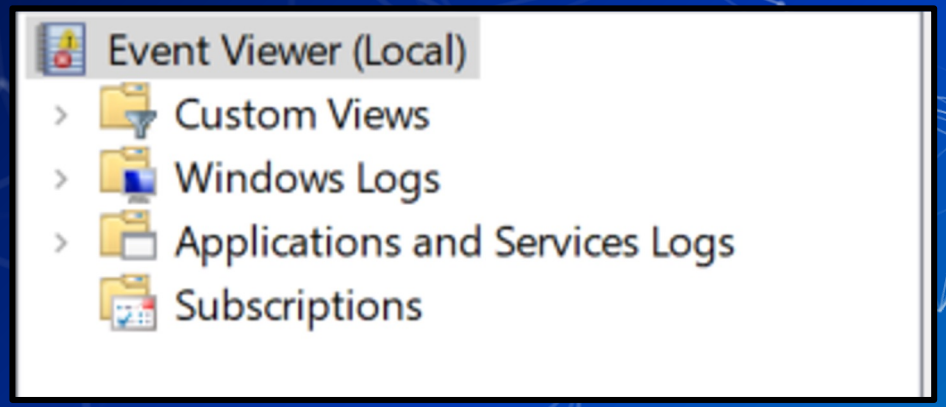
Event Viewer

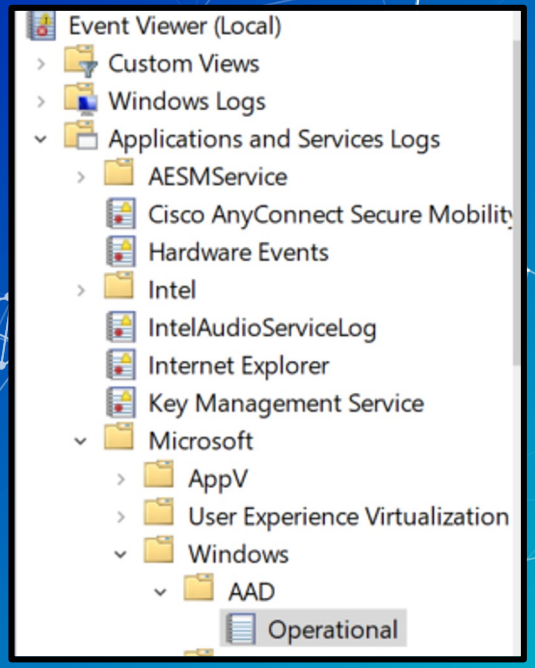
- Can be opened by searching for “event” and clicking open



Event Viewer cont.

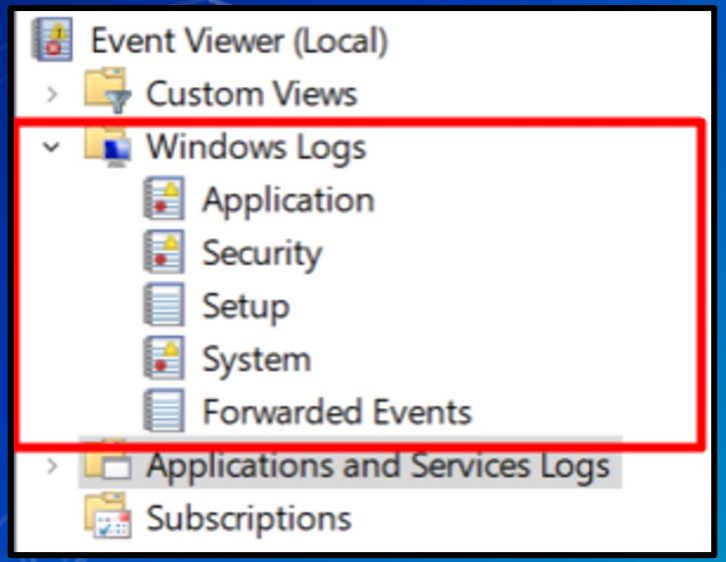
- Logs are stored in a hierarchical structure



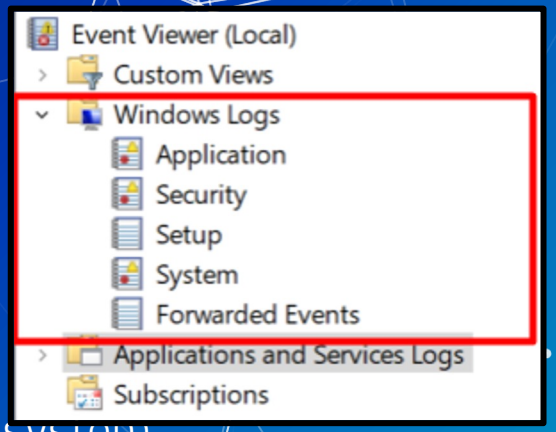


Event Viewer cont.

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



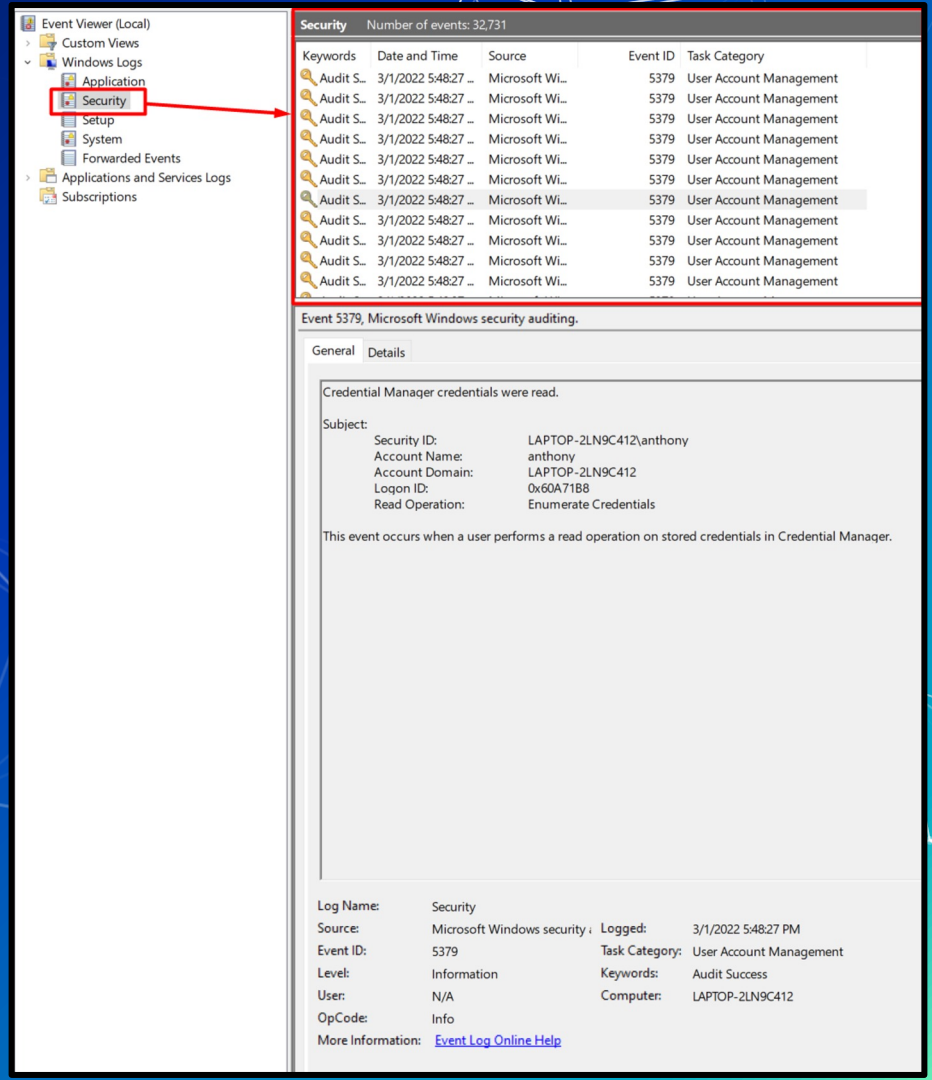
Event Viewer cont.



- 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



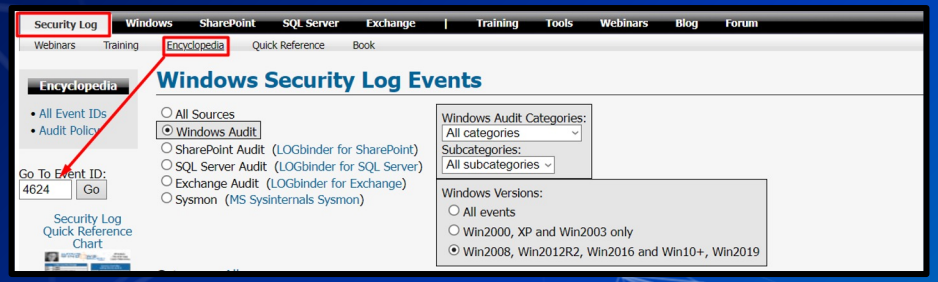
Event Viewer cont.

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

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.



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.

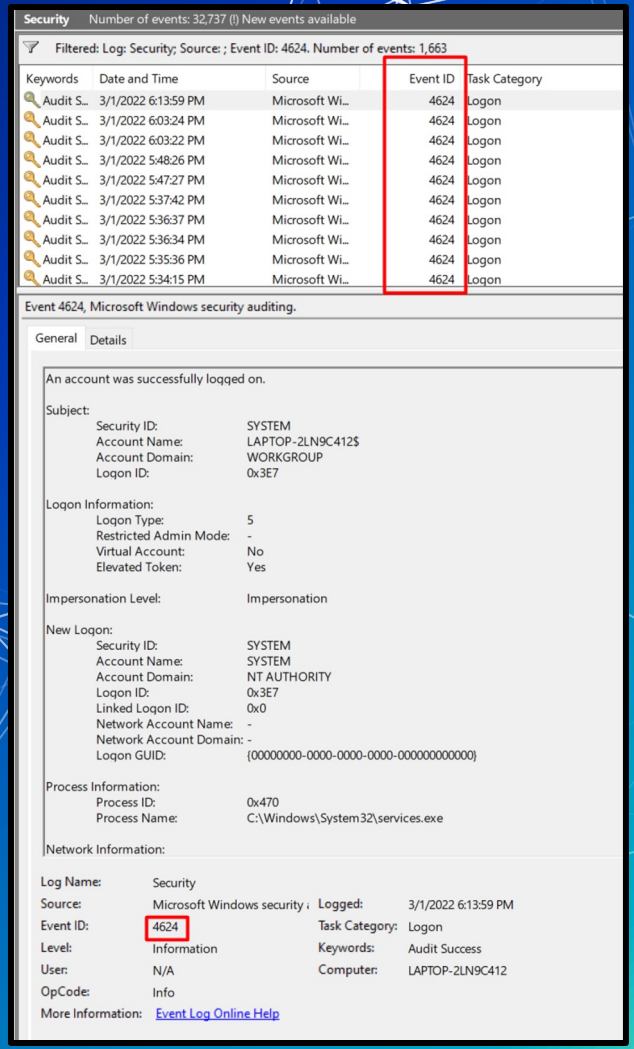
Win2012 adds the Impersonation Level field as shown in the example.

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 • Logon
Type	Success
Corresponding events in Windows 2003 and before	528 , 540

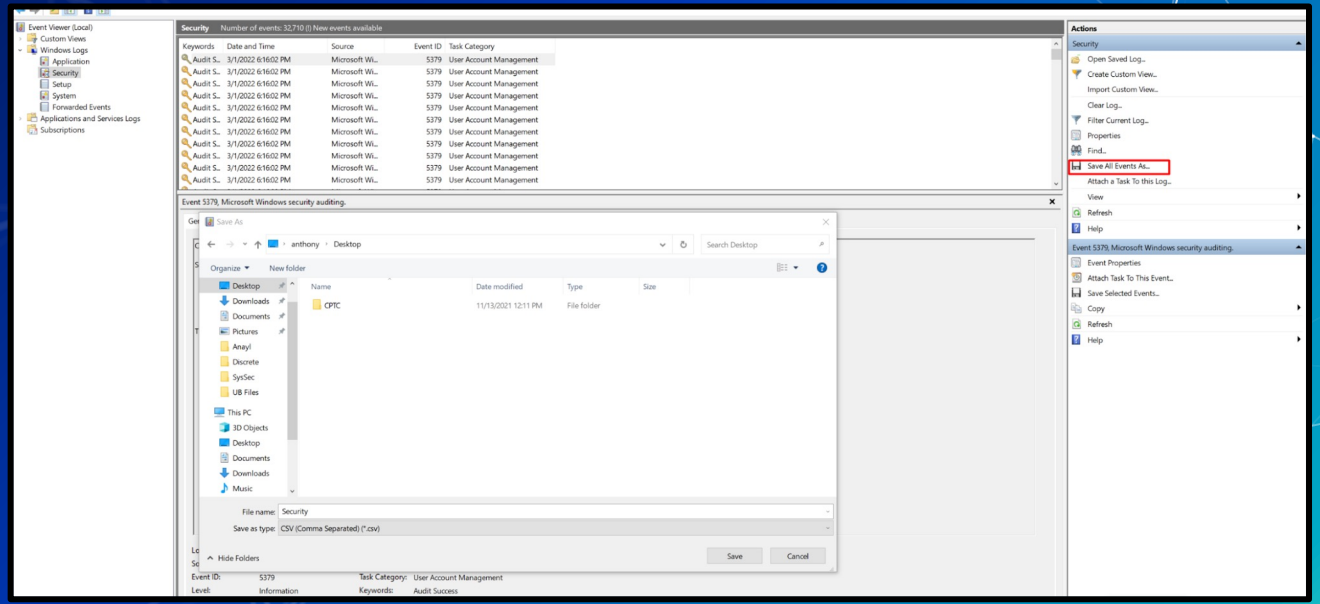
Discussions on Event ID 4624

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



Event Viewer cont.

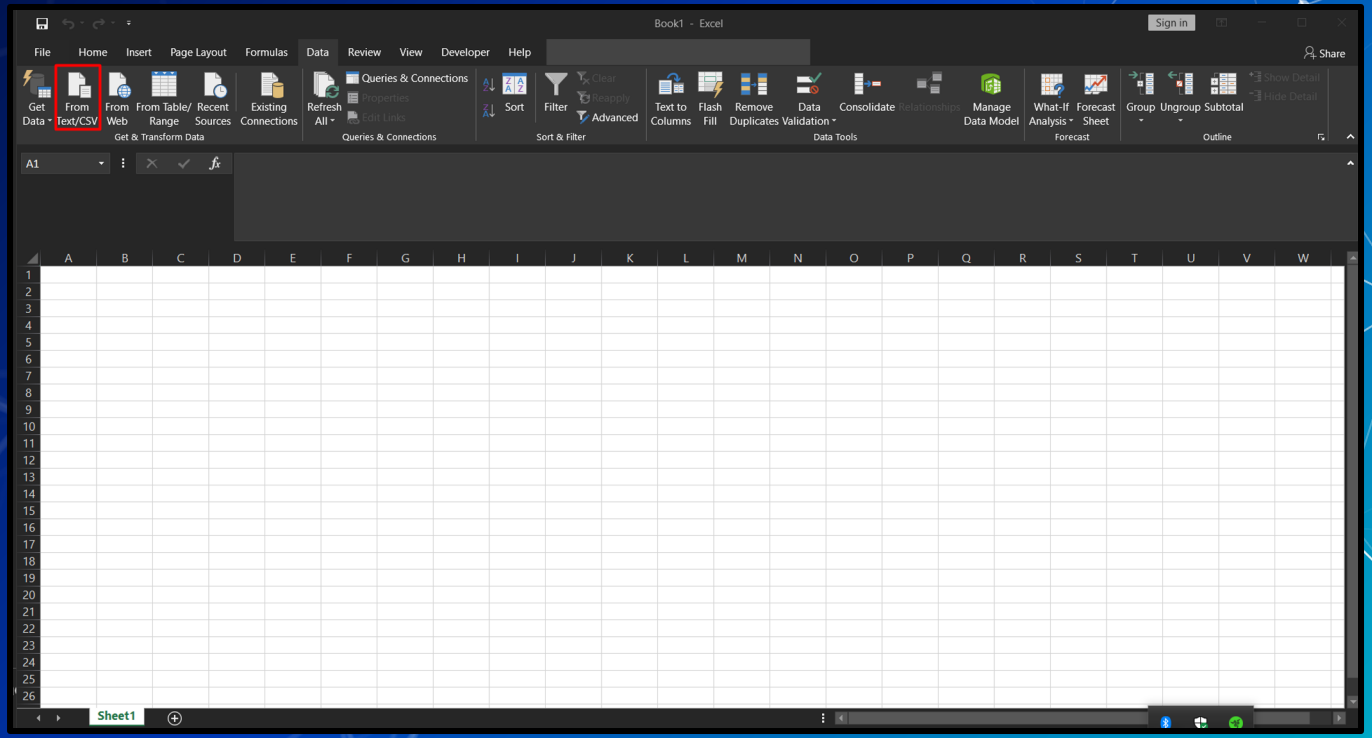
- Event viewer sucks when trying to search logs in bulk.
- We can extract logs to a CSV file



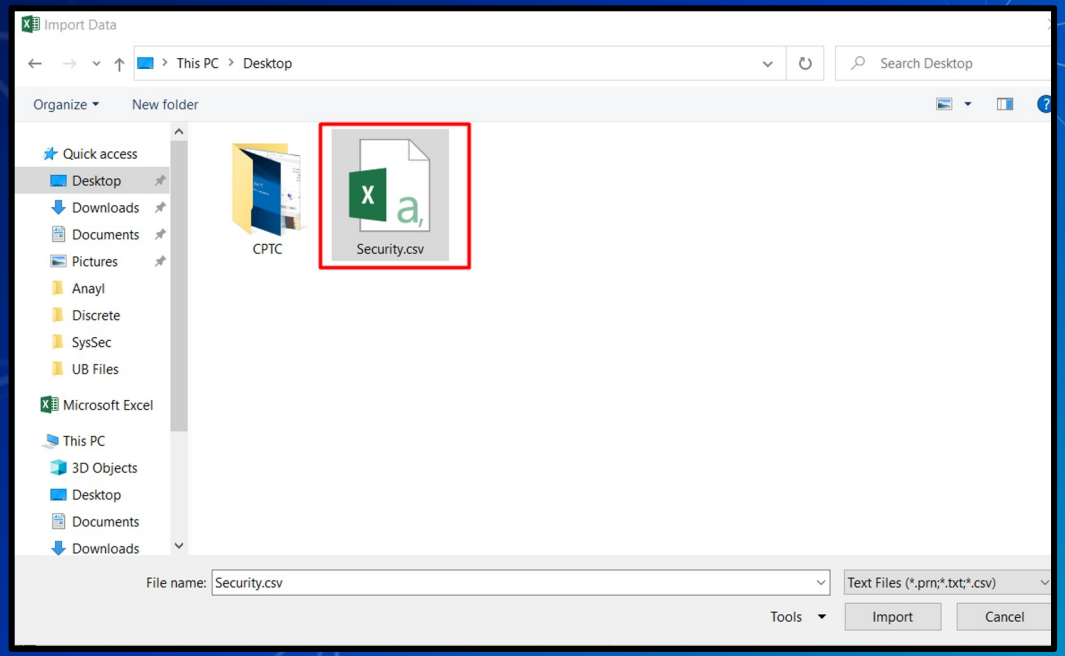
Event Viewer cont.

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

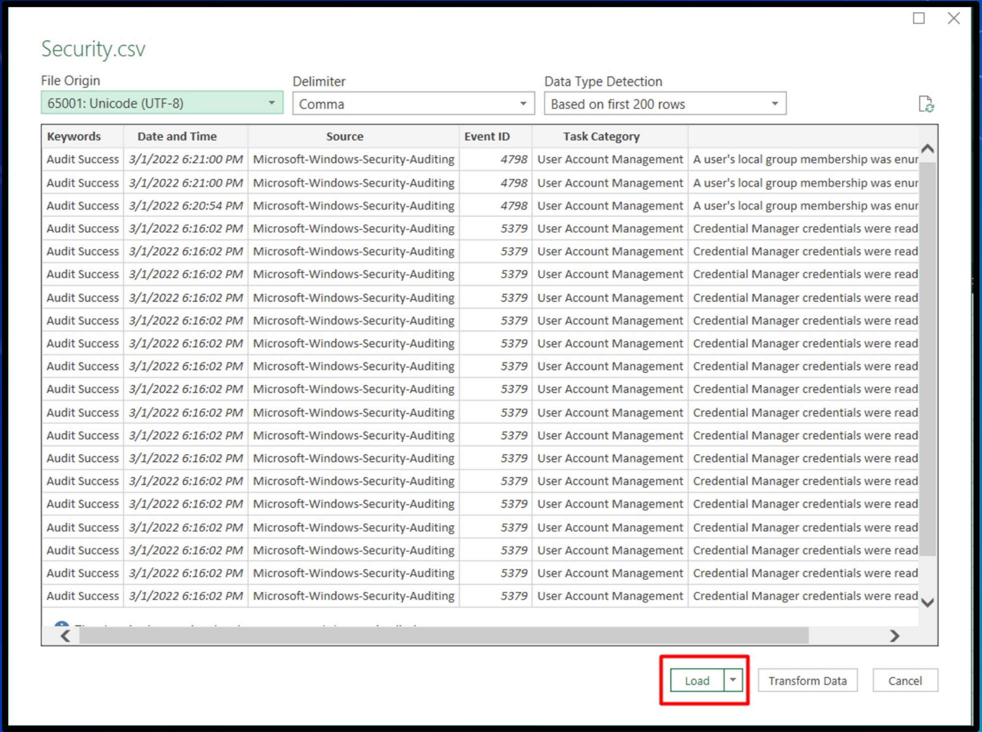
Importing Logs in Excel



Importing Logs in Excel



Importing Logs in Excel



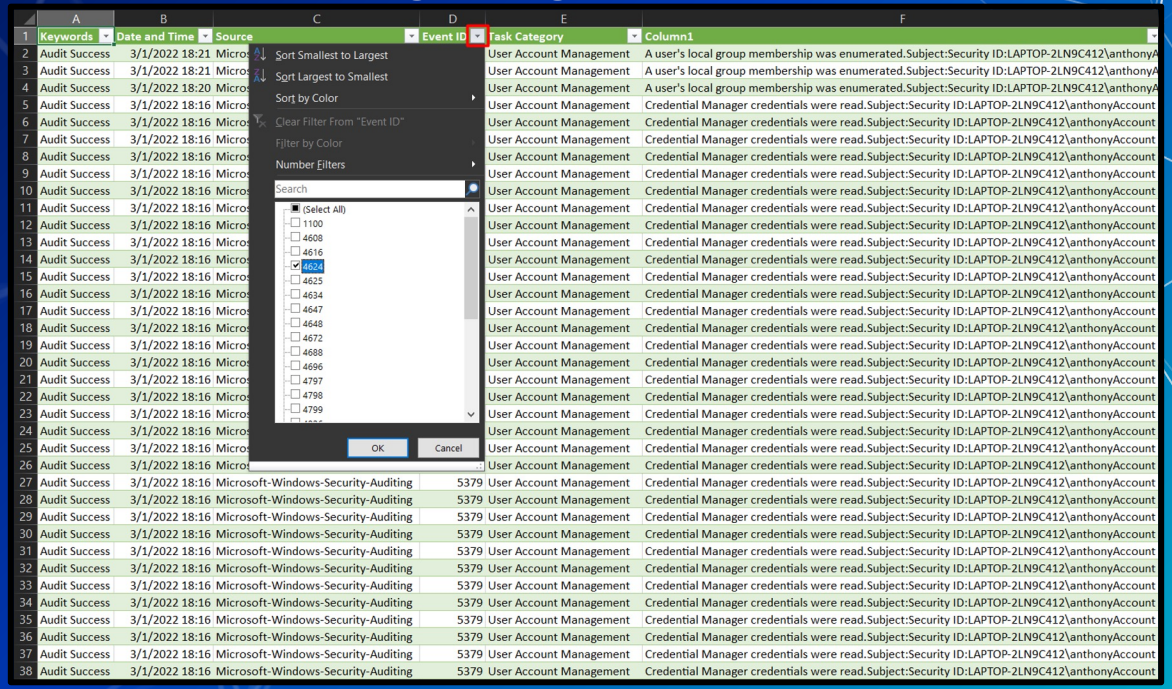
Keywords	Date and Time	Source	Event ID	Task Category	
Audit Success	3/1/2022 6:21:00 PM	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enur
Audit Success	3/1/2022 6:21:00 PM	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's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

Logs in Excel

	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-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enumerated.Subject:Security ID:LAPTOP-2LN9C412\anthony
3	Audit Success	3/1/2022 18:21	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enumerated.Subject:Security ID:LAPTOP-2LN9C412\anthony
4	Audit Success	3/1/2022 18:20	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was enumerated.Subject:Security ID:LAPTOP-2LN9C412\anthony
5	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
6	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
7	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
8	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
9	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
10	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
11	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
12	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
13	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
14	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
15	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
16	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
17	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
18	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
19	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
20	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
21	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
22	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
23	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
24	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
25	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
26	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
27	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
28	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
29	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
30	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
31	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
32	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
33	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
34	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
35	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
36	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
37	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
38	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
39	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun
40	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	5379	User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccoun

Logs in Excel

- Within Excel we can search logs using filters.



Logs in Excel

	A	B	C	D	E	F
1	Keywords	Date and Time	Source	Event ID	Task Category	Column1
81	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
83	Audit Success	3/1/2022 18:16	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
85	Audit Success	3/1/2022 18:13	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
87	Audit Success	3/1/2022 18:03	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
89	Audit Success	3/1/2022 18:03	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
185	Audit Success	3/1/2022 17:48	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
187	Audit Success	3/1/2022 17:47	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
206	Audit Success	3/1/2022 17:37	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
322	Audit Success	3/1/2022 17:36	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
494	Audit Success	3/1/2022 17:36	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
891	Audit Success	3/1/2022 17:35	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
903	Audit Success	3/1/2022 17:34	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
904	Audit Success	3/1/2022 17:34	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1476	Audit Success	3/1/2022 17:33	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1494	Audit Success	3/1/2022 17:33	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1500	Audit Success	3/1/2022 17:33	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1502	Audit Success	3/1/2022 17:33	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1503	Audit Success	3/1/2022 17:33	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1510	Audit Success	2/28/2022 22:41	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1512	Audit Success	2/28/2022 22:41	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1516	Audit Success	2/28/2022 22:41	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1524	Audit Success	2/28/2022 22:41	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1528	Audit Success	2/28/2022 22:41	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1529	Audit Success	2/28/2022 22:41	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1531	Audit Success	2/28/2022 22:41	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1537	Audit Success	2/28/2022 22:40	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1607	Audit Success	2/28/2022 22:40	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1609	Audit Success	2/28/2022 22:39	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1611	Audit Success	2/28/2022 22:39	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1614	Audit Success	2/28/2022 22:22	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1616	Audit Success	2/28/2022 22:08	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41
1618	Audit Success	2/28/2022 22:08	Microsoft-Windows-Security-Auditing	4624	Logon	An account was successfully logged on.Subject:Security ID:SYSTEMAccount Name:LAPTOP-2LN9C41

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.

NetDef

Questions?

NetDef

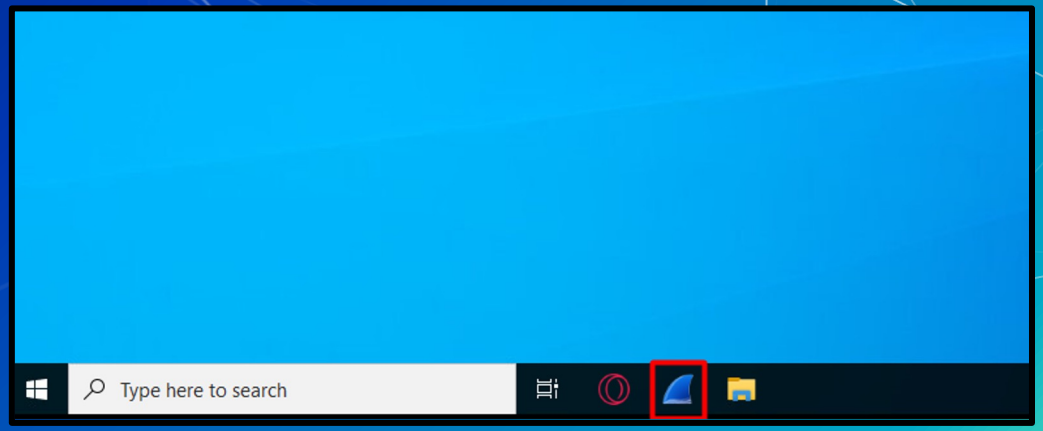
Network Forensics

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



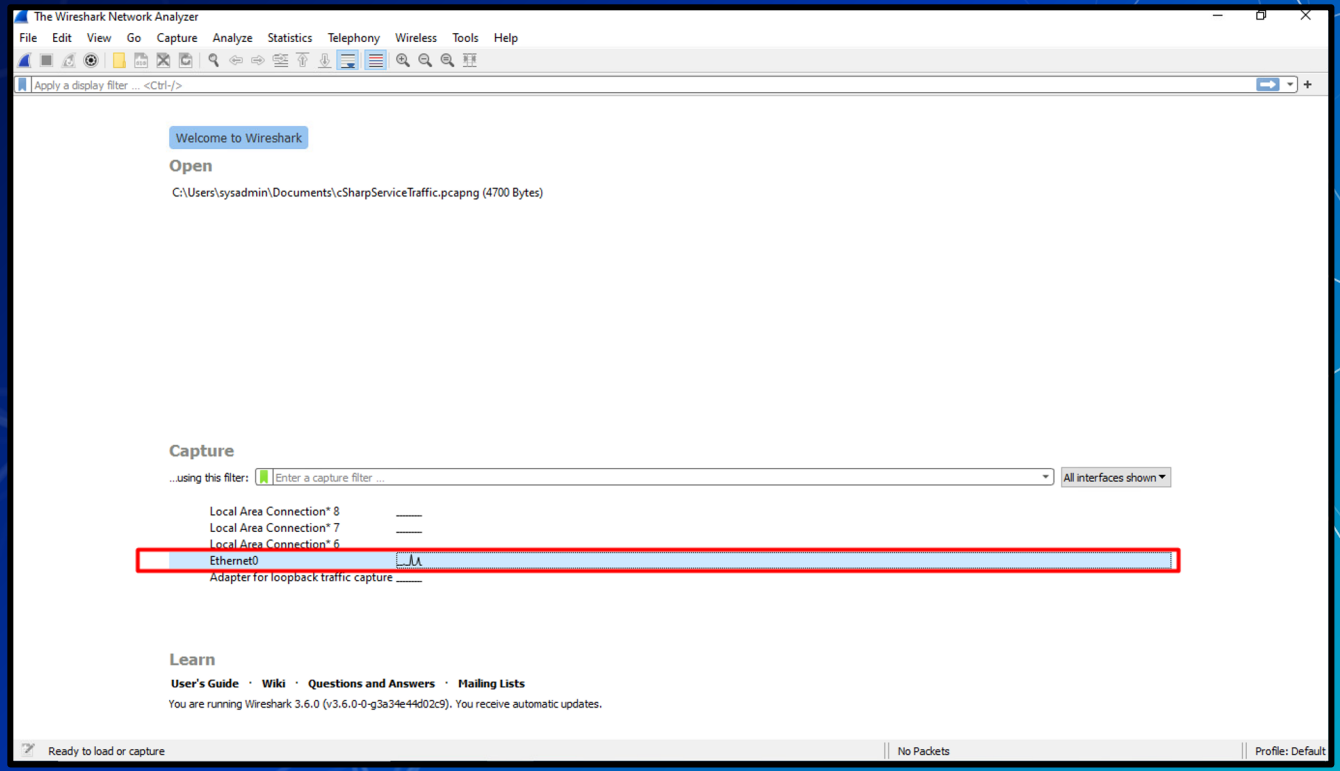
In Class Activity

WireShark

Hands on 0 - Wireshark

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

Network Forensics Hands-on



NetDef

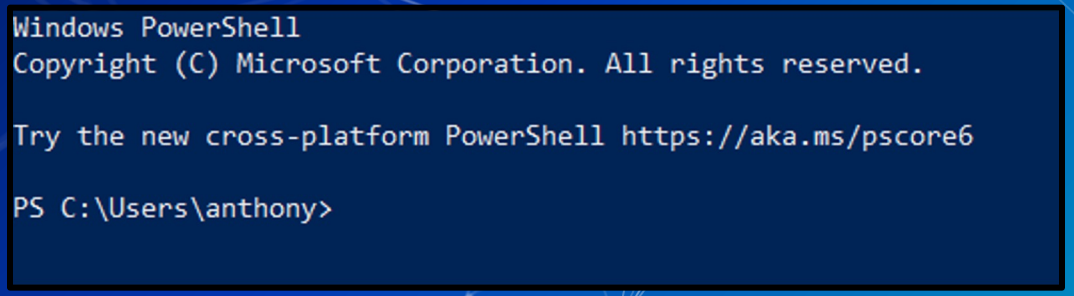
Break Slide

NetDef

PowerShell For IR

PowerShell

- Automation and configuration tool
- https://docs.microsoft.com/en-us/powershell/



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.”

NetDef

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  autotimesvc        Cellular Time
Stopped  AxInstSV           ActiveX Installer (AxInstSV)
Stopped  BcastDVRUserSer... 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_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 HECI Se...
Running  cplspcon           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  BcastDVRUserSer... 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`?

NetDef

Break Slide

NetDef

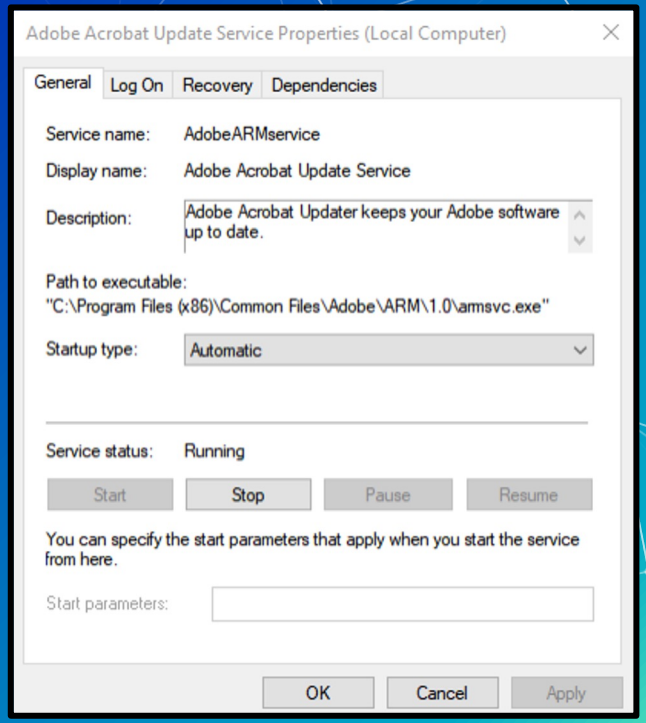
WMI & Services

Windows Management Instrumentation (WMI)

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

Services

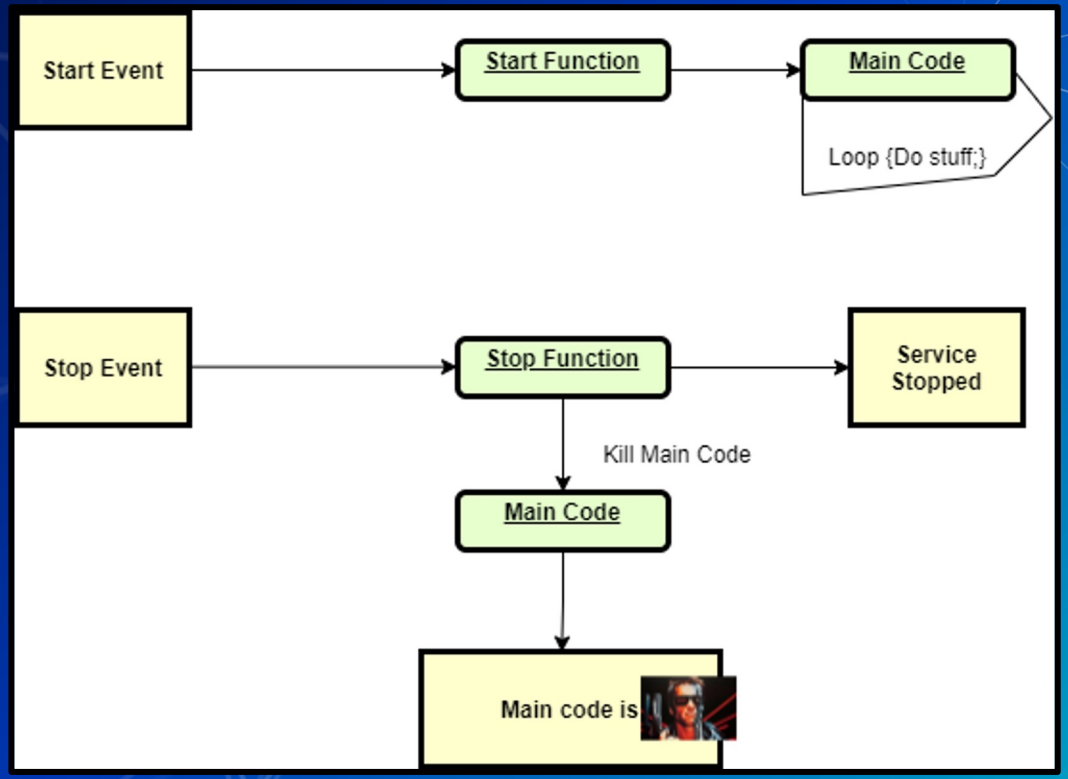
- Behind the scenes to keep things working
- 4 startup types
  - Automatic (Delayed Start)
  - Automatic
  - Manual
  - Disabled



Services

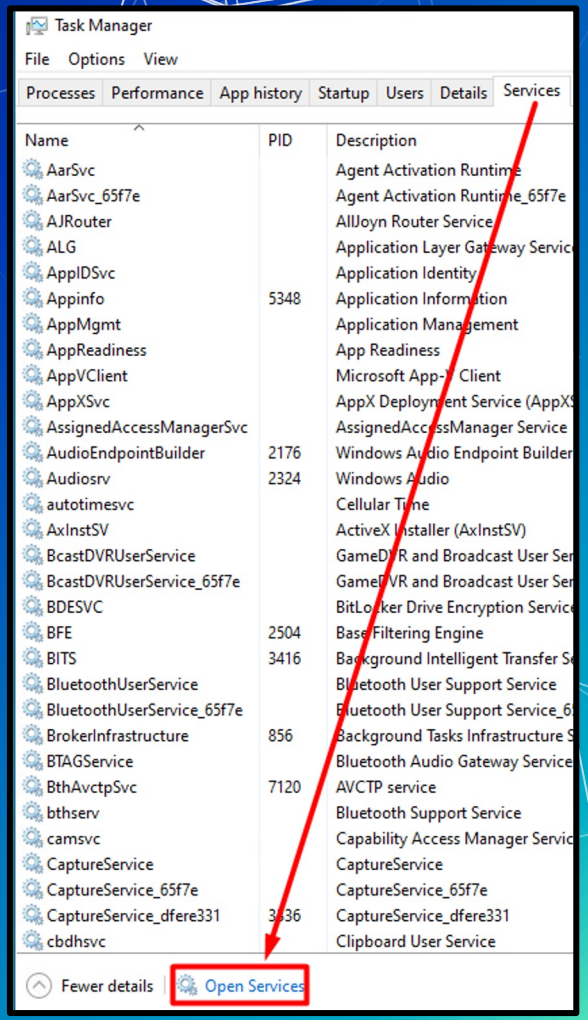
- Can run as `nt authority \system`
  - `nt authority \system` != `root`
  - Is more powerful than an “administrator”
- Active even when no user is signed in
- May be hosted by the service host (svchost.exe)
- May executables that are designated to be services
- Follow a defined service model

Service Model

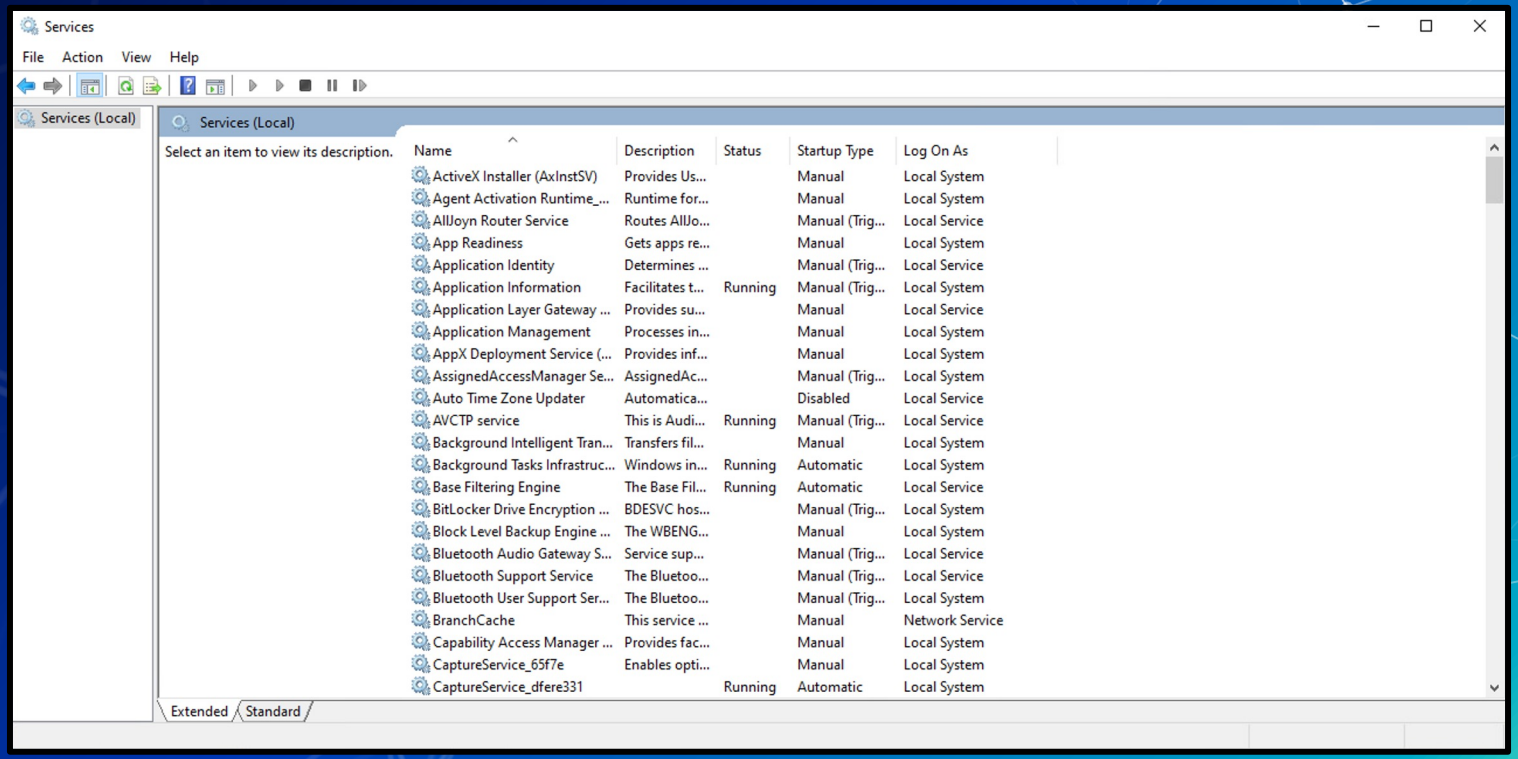


How to list services?

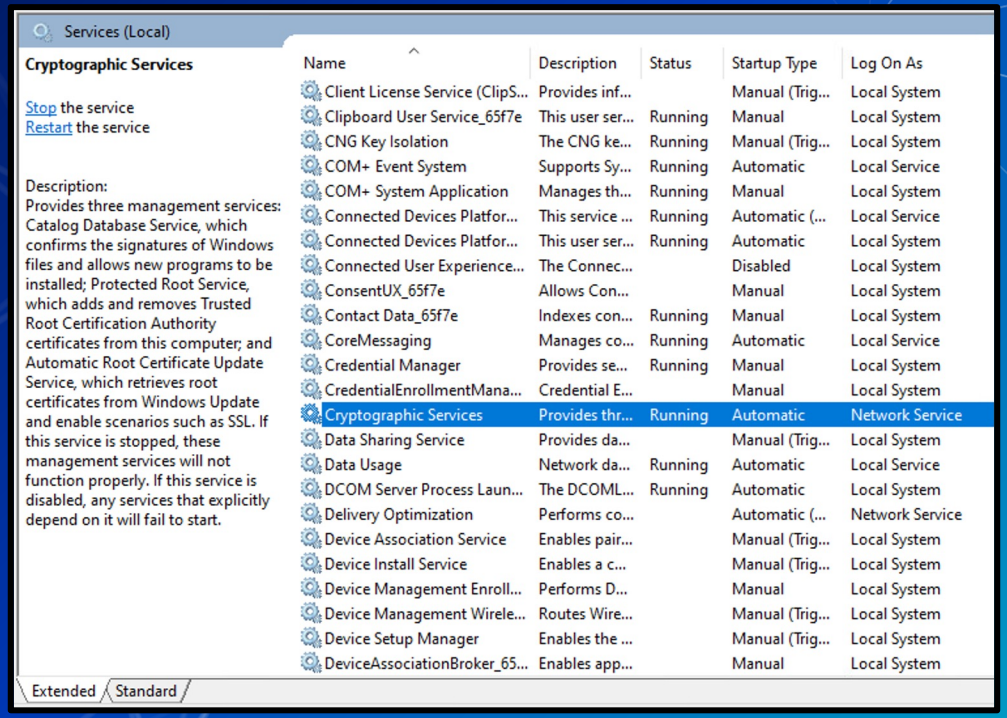
- Open Task Manager and navigate to services tab



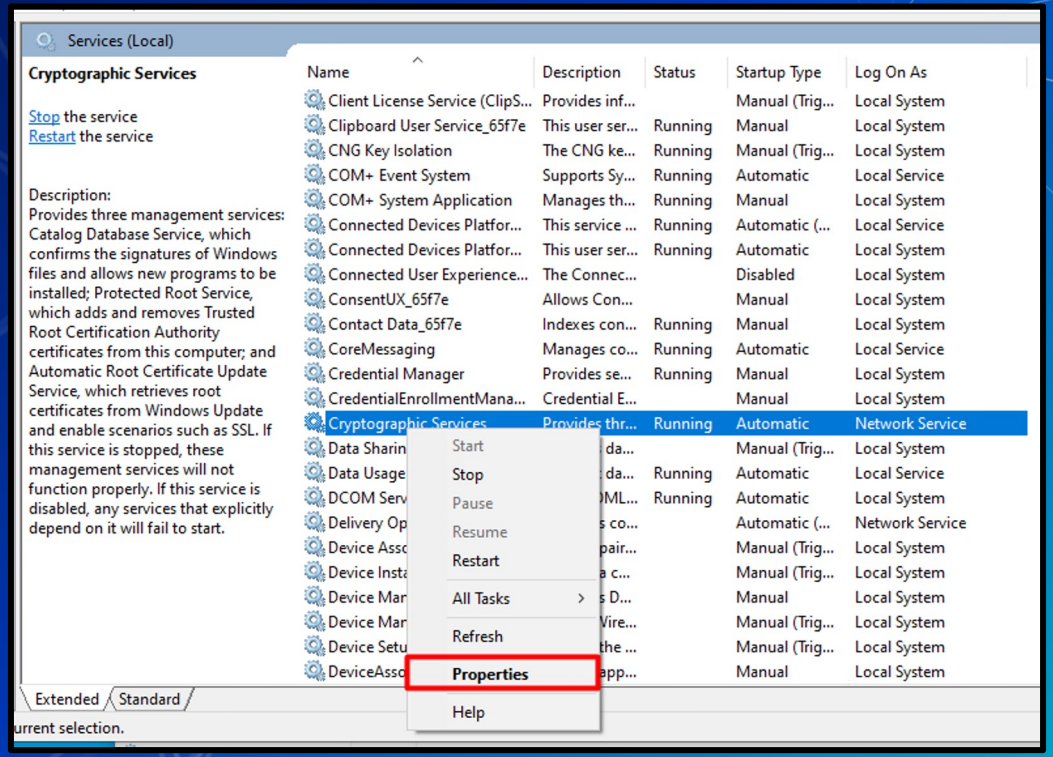
Services List



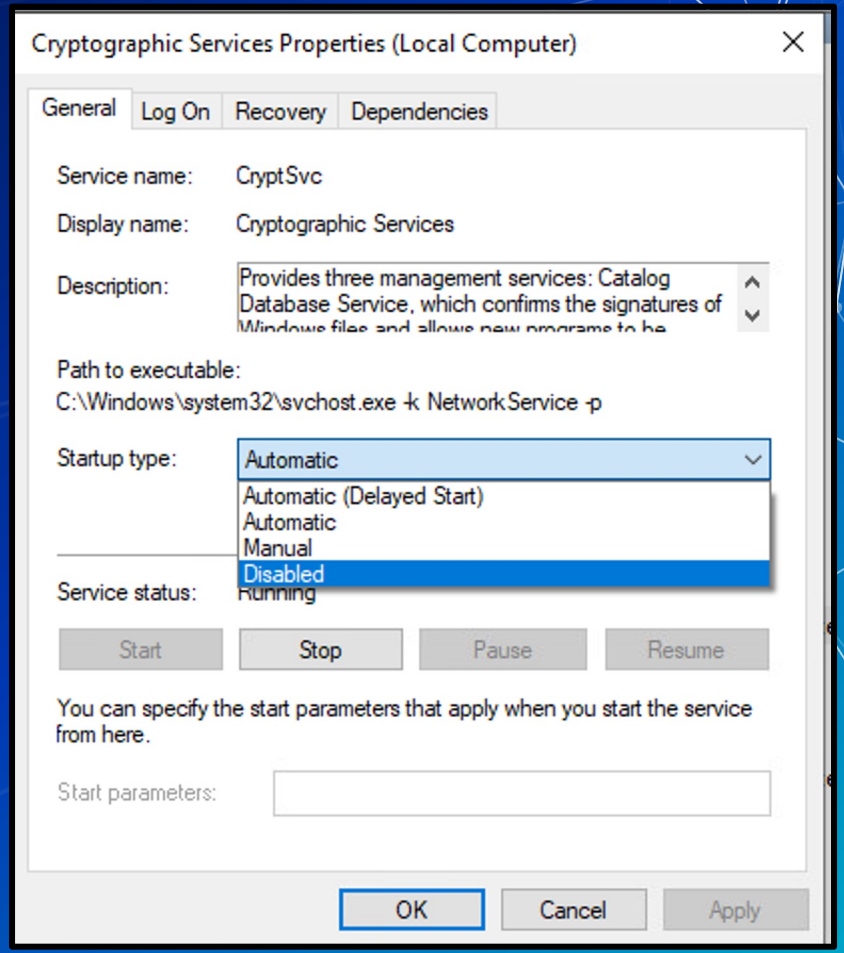
Services List



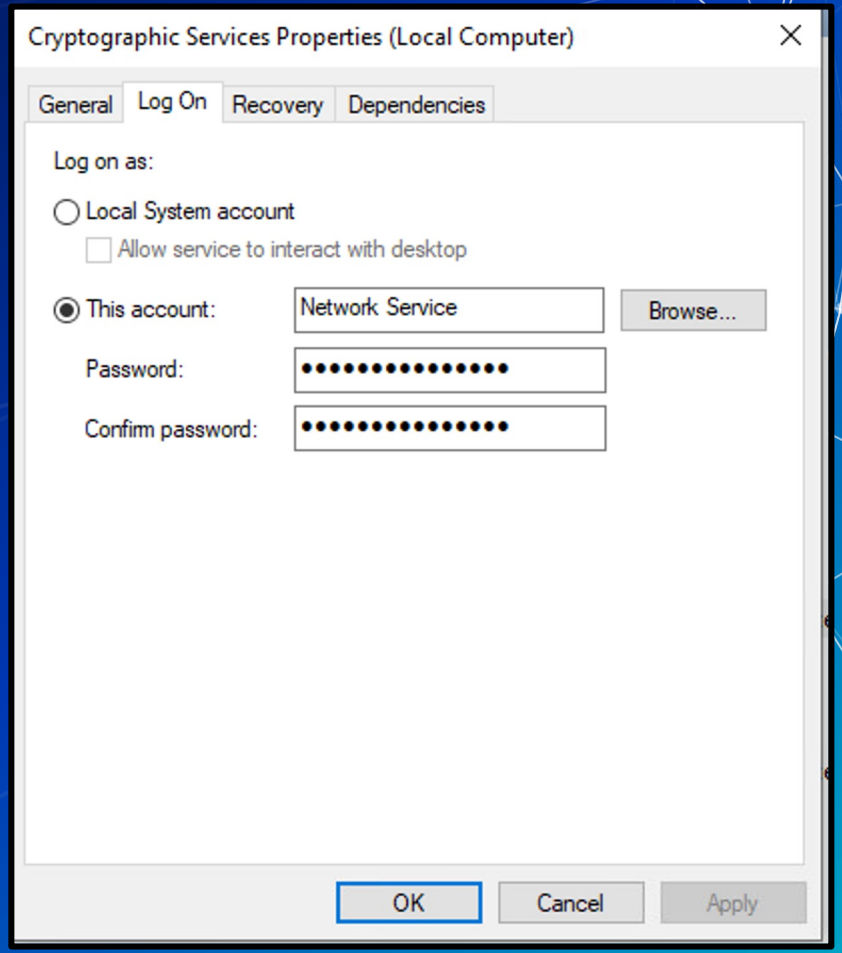
Services List



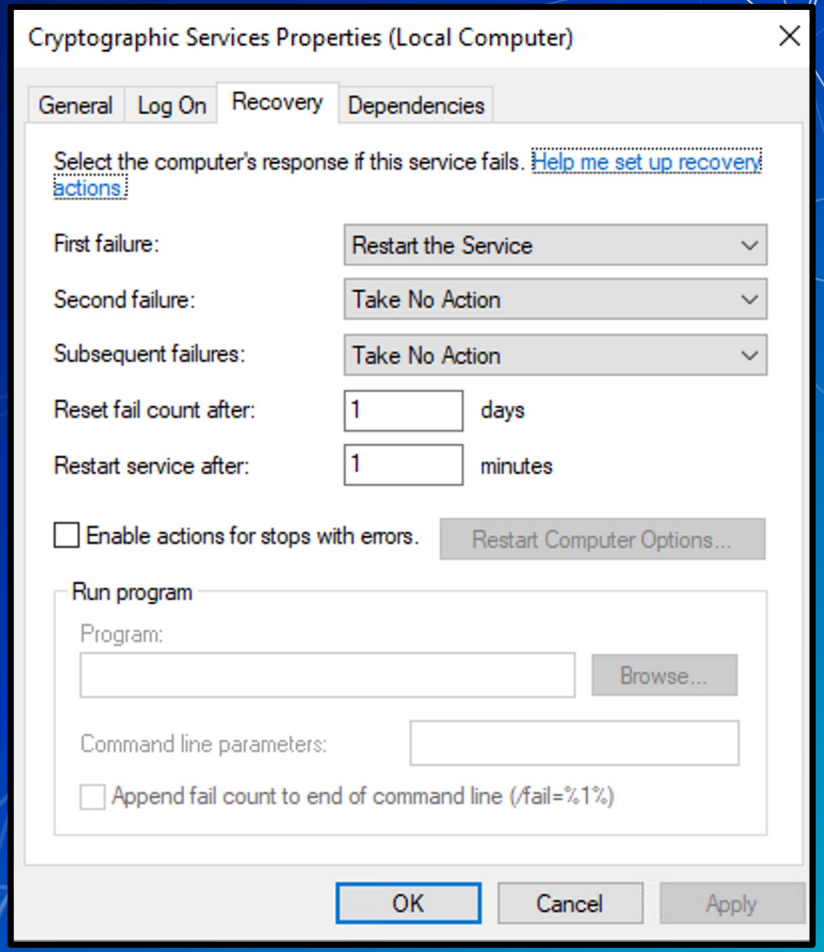
Services List



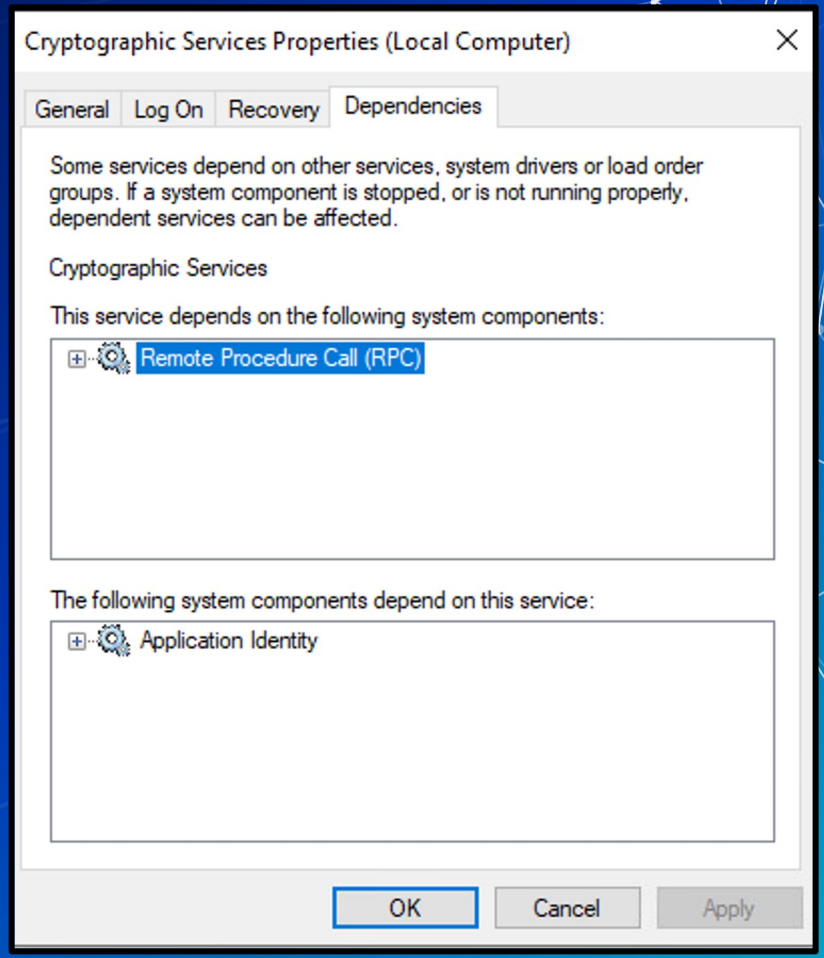
Services List



Services List



Services List



NetDef

In Class Activity

Find a Malicious Service

Hands on 3- Find a Malicious Service

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

Hands on 3- Delete a Malicious Service

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

NetDef

RESTART YOUR WINDOWS VM

Persistence

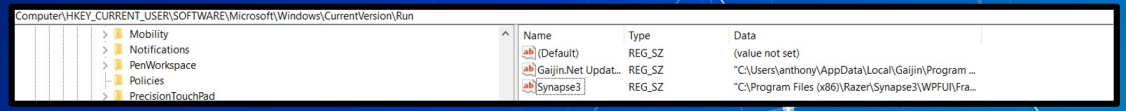
Persistence

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

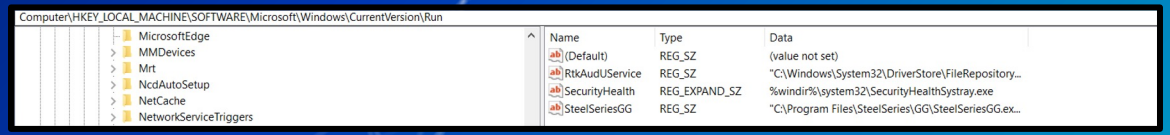
Persistence Methods

- 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

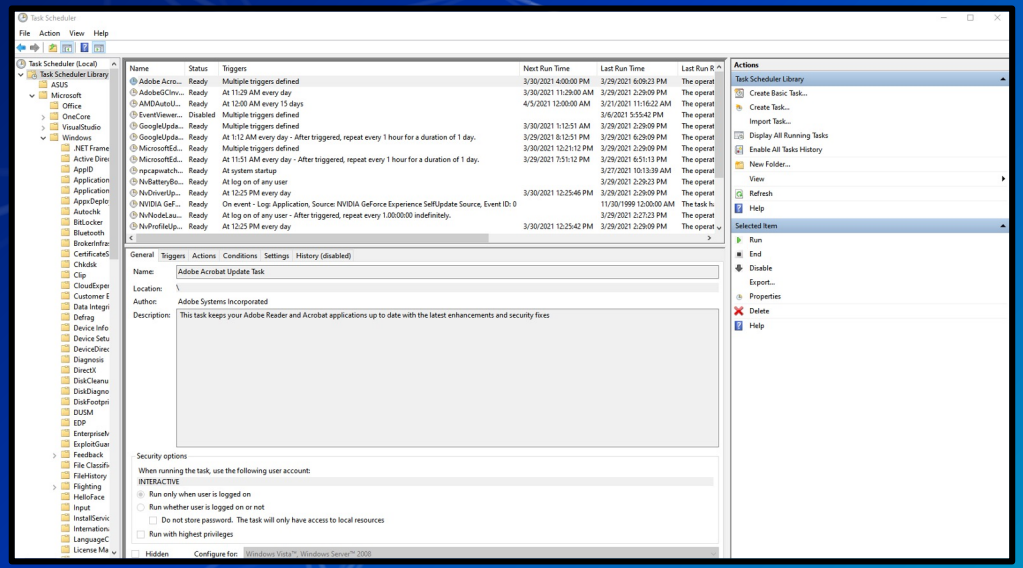


- Registry Editor is a GUI way of viewing registry
  - `Get-ItemProperty` can be used as well
    - https://tinyurl.com/9hbeh72f
- Two directories for running at sign on
  - `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`



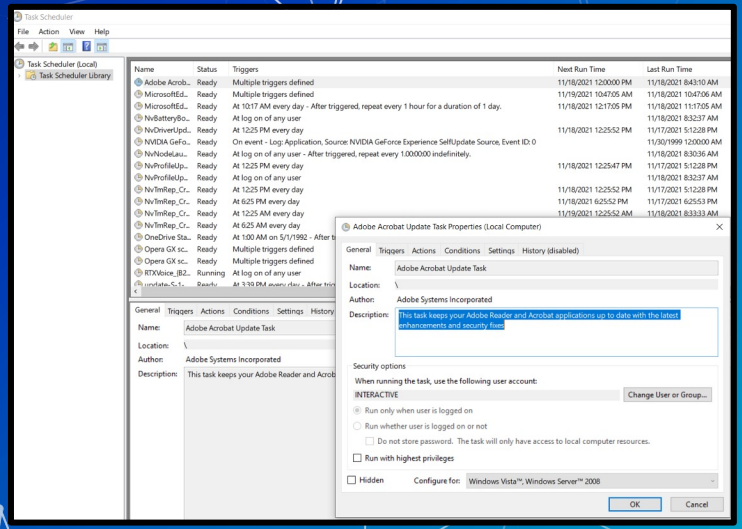
Scheduled Tasks

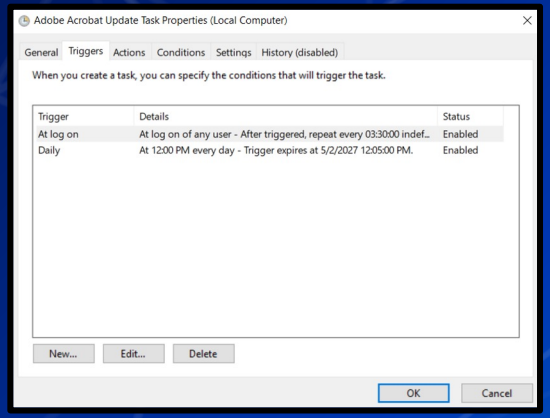
- Perform actions given specific triggers
- Stored in `C:\Windows\System32\Tasks` as xml files

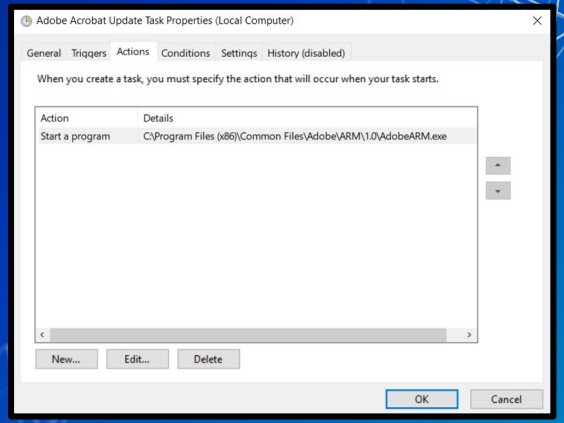


Scheduled Tasks cont.

- 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

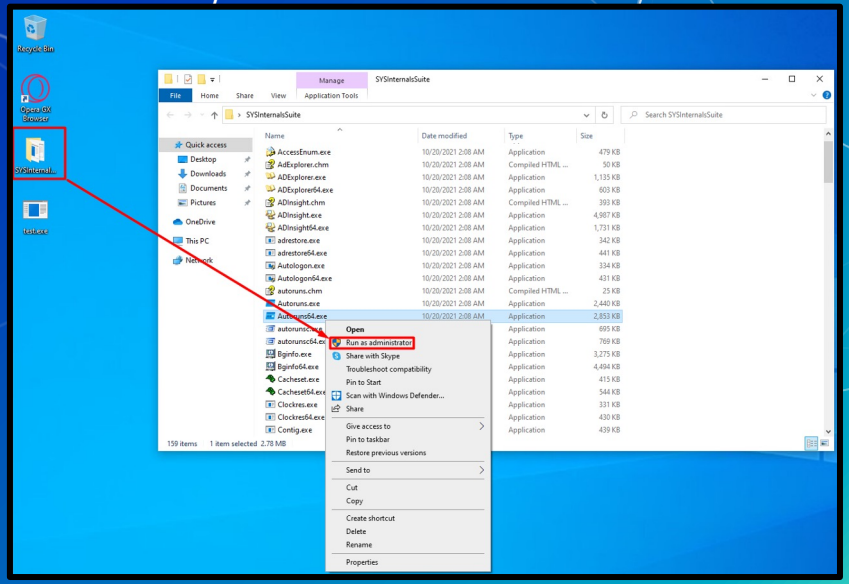
- Group policies can soften the security posture of a device
  - Disable anti-virus
  - Turn off or flood logs
  - Disable firewalls
  - And more!
- Group Policies can be used to establish registry based persistence
- Malicious group policies are very dangerous

Hands on 4 – Combatting Persistence

- Check services again
  - What do you notice?

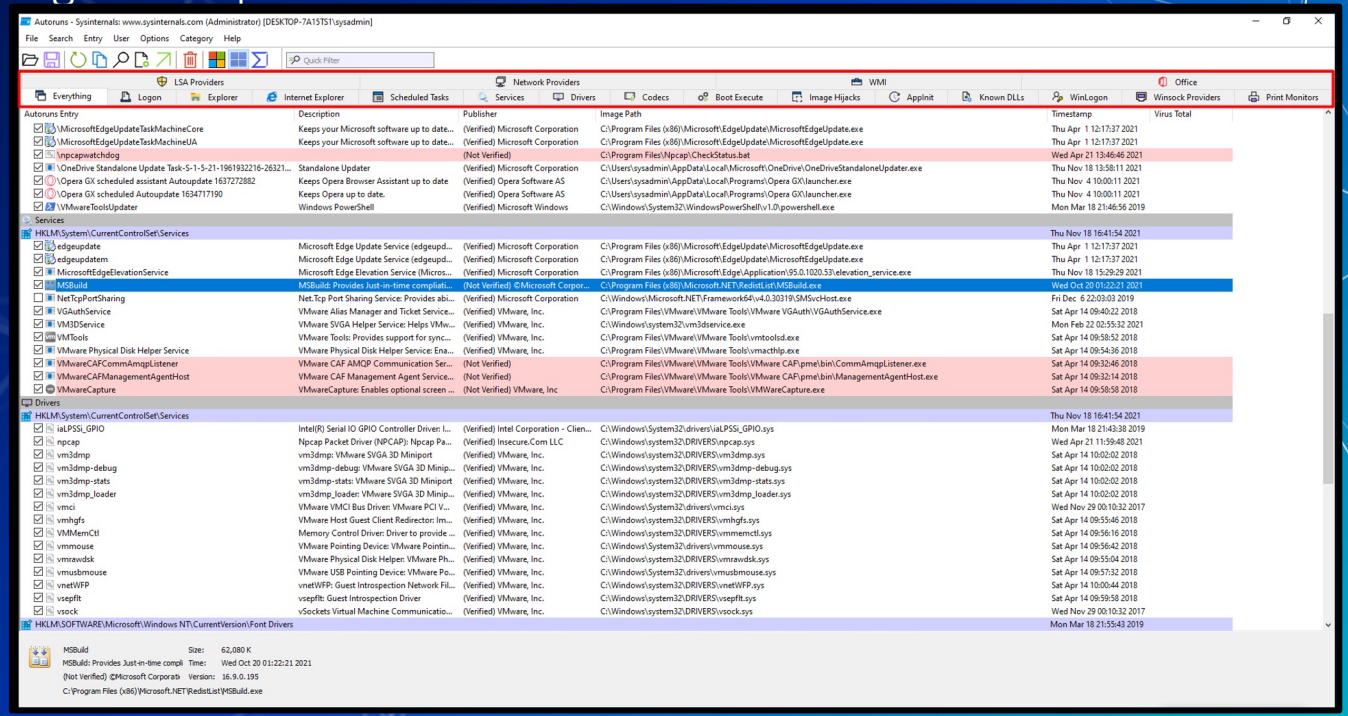
Hands on 4 – Combatting Persistence

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

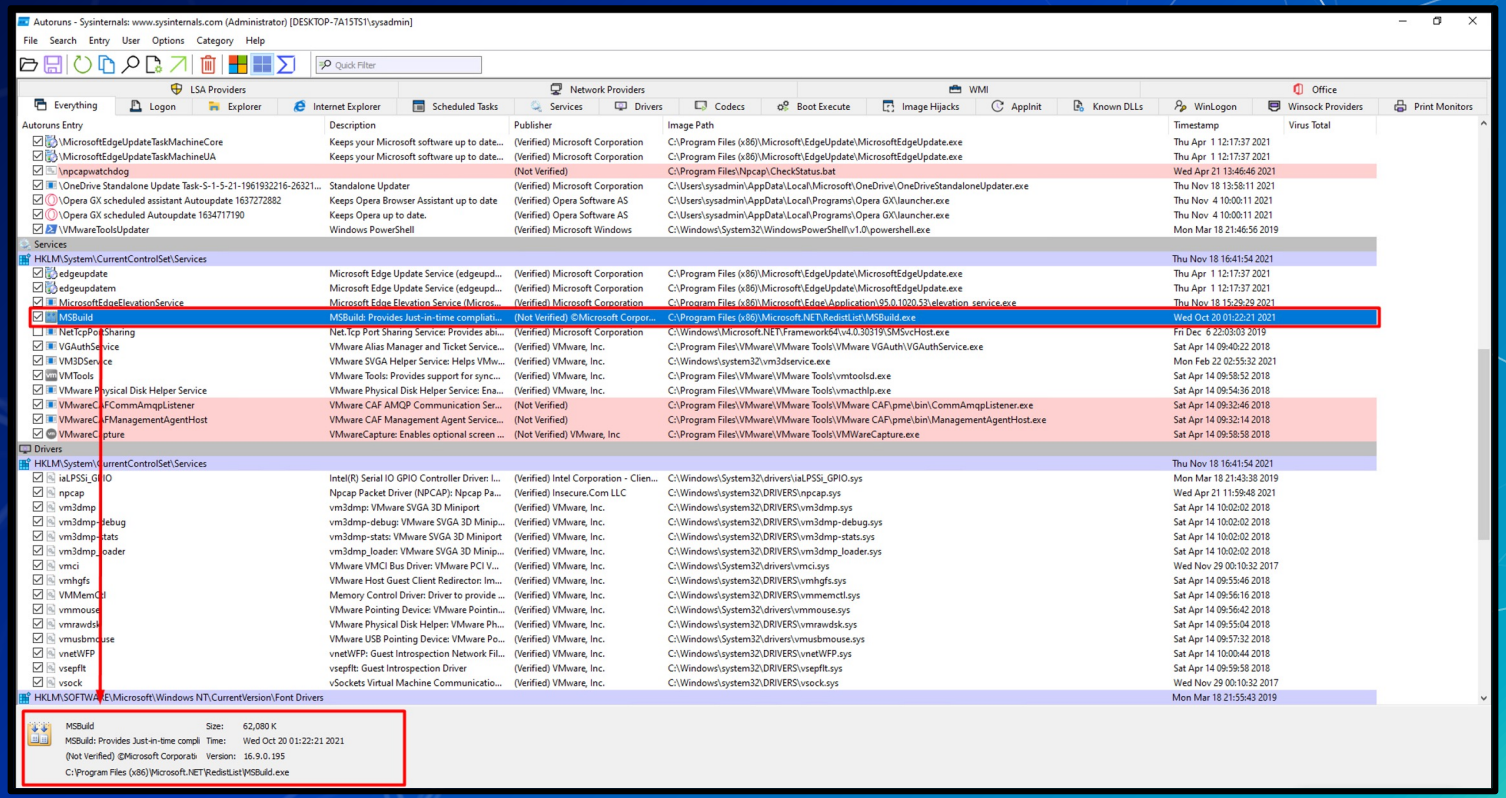


Hands on 4 – Combatting Persistence

- Categories of persistence



Hands on 4 – Combatting Persistence



Hands on 4 – Combatting Persistence

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

Homework Links

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

Additional Resources

- Abusing Windows Management Instrumentation (Black Hat)
  - https://tinyurl.com/a7jpzmsc
  - 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/

NetDef

Questions?