Windows Threat Hunting

UBNetDef, Fall 2023
Week 6

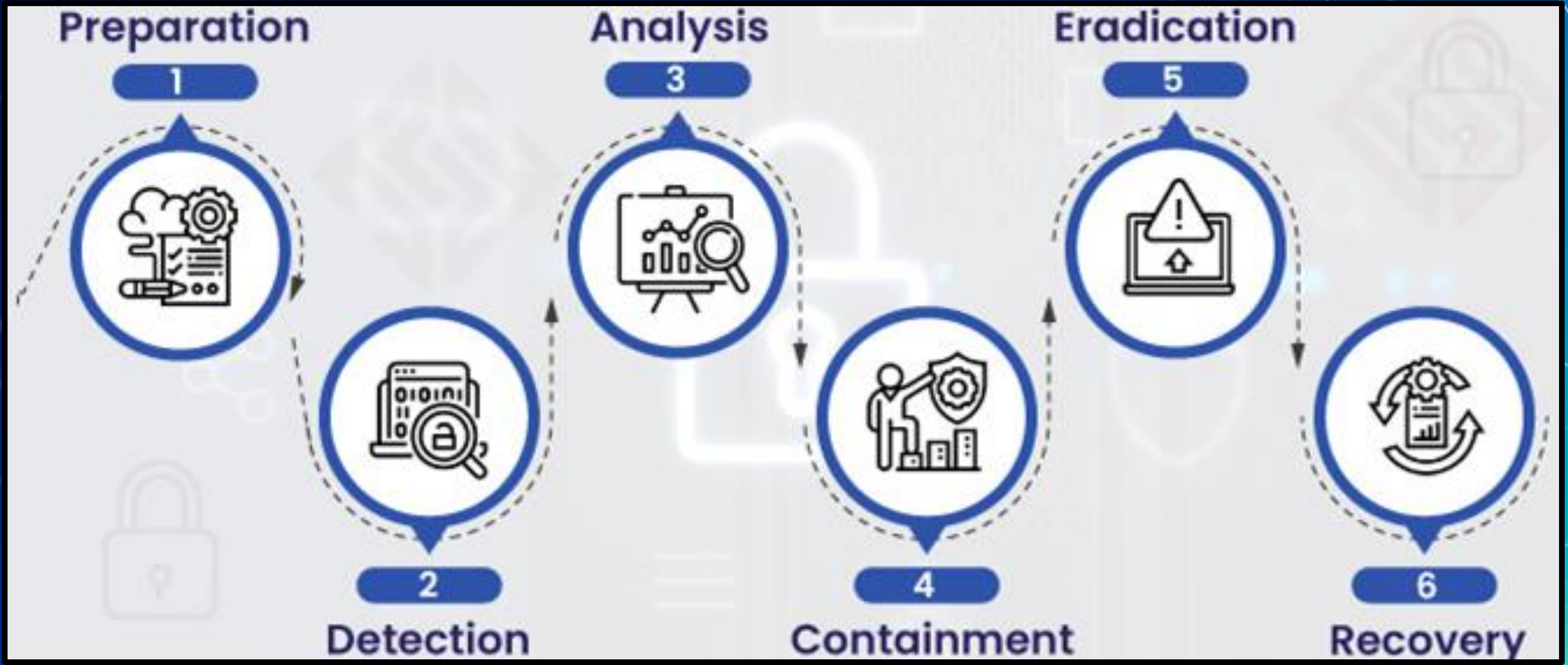
Presenter:
Anthony Magrene & Griffin Refol

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

NetDef

Incident Response



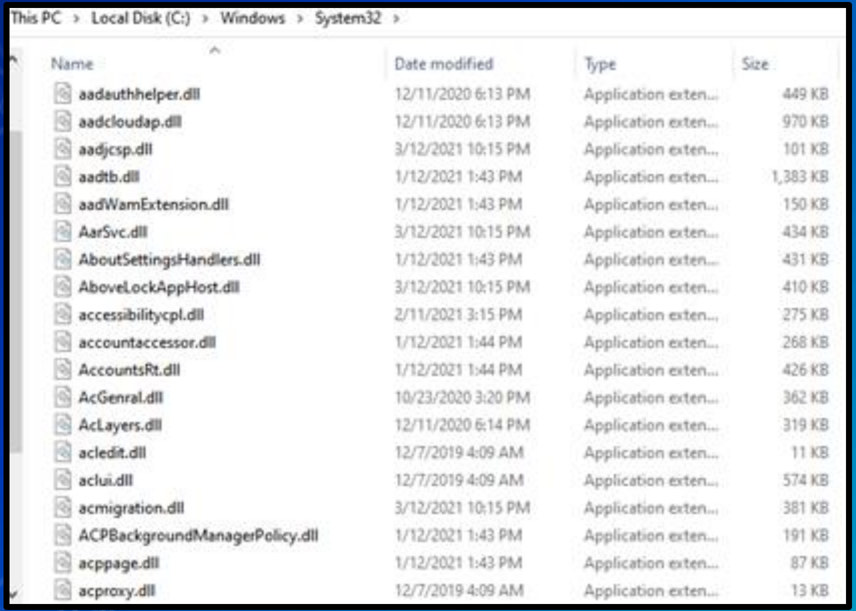
NetDef

Windows Concepts

Notable File Types

Dynamic Link Library (.dll)

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

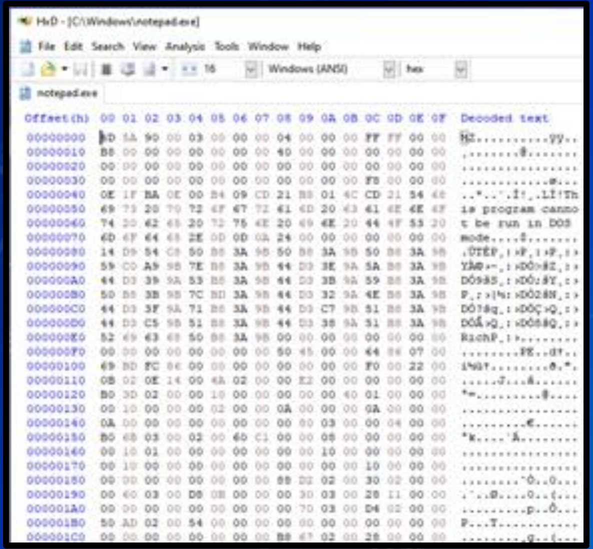


This PC › Local Disk (C:) › Windows › System32 ›

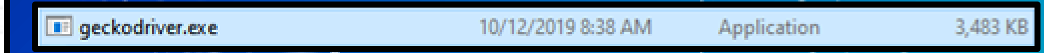
Name	Date modified	Type	Size
aadauthhelper.dll	12/11/2020 6:13 PM	Application exten...	449 KB
aadcloudap.dll	12/11/2020 6:13 PM	Application exten...	970 KB
aadjcsp.dll	3/12/2021 10:15 PM	Application exten...	101 KB
aadtb.dll	1/12/2021 1:43 PM	Application exten...	1,383 KB
aadWamExtension.dll	1/12/2021 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
AcGenral.dll	10/23/2020 3:20 PM	Application exten...	362 KB
AcLayers.dll	12/11/2020 6:14 PM	Application exten...	319 KB
acledit.dll	12/7/2019 4:09 AM	Application exten...	11 KB
aclui.dll	12/7/2019 4:09 AM	Application exten...	574 KB
acmigration.dll	3/12/2021 10:15 PM	Application exten...	381 KB
ACPBackgroundManagerPolicy.dll	1/12/2021 1:43 PM	Application exten...	191 KB
acppage.dll	1/12/2021 1:43 PM	Application exten...	87 KB
acproxy.dll	12/7/2019 4:09 AM	Application exten...	13 KB

Portable Executable (.exe)

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


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

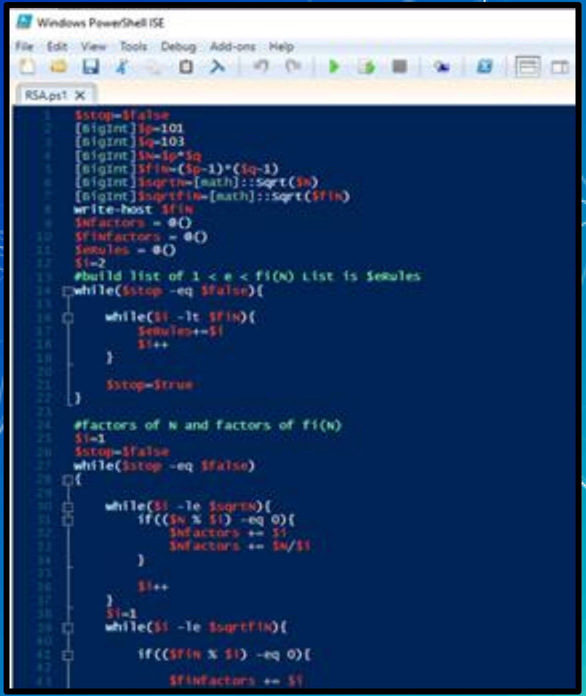
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 F8 00 00 00  ............ø...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  14 D9 54 C8 50 B8 3A 9B 50 B8 3A 9B 50 B8 3A 9B  .ÙTÈP¸:›P¸:›P¸:›
00000090  59 C0 A9 9B 7E B8 3A 9B 44 D3 3E 9A 5A B8 3A 9B  YÀ©›~¸:›DÓ>šZ¸:›
000000A0  44 D3 39 9A 53 B8 3A 9B 44 D3 3B 9A 59 B8 3A 9B  DÓ9šS¸:›DÓ;šY¸:›
000000B0  50 B8 3B 9B 7C BD 3A 9B 44 D3 32 9A 4E B8 3A 9B  P¸;›|½:›DÓ2šN¸:›
000000C0  44 D3 3F 9A 71 B8 3A 9B 44 D3 C7 9B 51 B8 3A 9B  DÓ?šq¸:›DÓÇ›Q¸:›
000000D0  44 D3 C5 9B 51 B8 3A 9B 44 D3 38 9A 51 B8 3A 9B  DÓÅ›Q¸:›DÓ8šQ¸:›
000000E0  52 69 63 68 50 B8 3A 9B 00 00 00 00 00 00 00 00  RichP¸:›........
000000F0  00 00 00 00 00 00 00 00 50 45 00 00 64 86 07 00  ........PE..d†..
00000100  69 BD FC 8C 00 00 00 00 00 00 00 00 F0 00 22 00  i½üŒ........ð.".
00000110  0B 02 0E 14 00 4A 02 00 00 E2 00 00 00 00 00 00  ......J...â.....
00000120  B0 3D 02 00 00 10 00 00 00 00 00 40 01 00 00 00  °=.........@....
00000130  00 10 00 00 00 02 00 00 0A 00 00 00 0A 00 00 00  ................
00000140  0A 00 00 00 00 00 00 00 00 80 03 00 00 04 00 00  .........€......
00000150  B0 6B 03 00 02 00 60 C1 00 00 08 00 00 00 00 00  °k....`Á........
00000160  00 10 01 00 00 00 00 00 00 00 10 00 00 00 00 00  ................
00000170  00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00  ................
00000180  00 00 00 00 00 00 00 00 88 D2 02 00 30 02 00 00  ........ˆÒ..0...
00000190  00 40 03 00 D8 0B 00 00 00 30 03 00 28 11 00 00  .@..Ø....0..(...
000001A0  00 00 00 00 00 00 00 00 00 70 03 00 D4 02 00 00  .........p..Ô...
000001B0  50 AD 02 00 54 00 00 00 00 00 00 00 00 00 00 00  P...T...........
000001C0  00 00 00 00 00 00 00 00 B8 47 02 00 28 00 00 00  ........¸G..(...
```



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

PowerShell Script (.ps1)

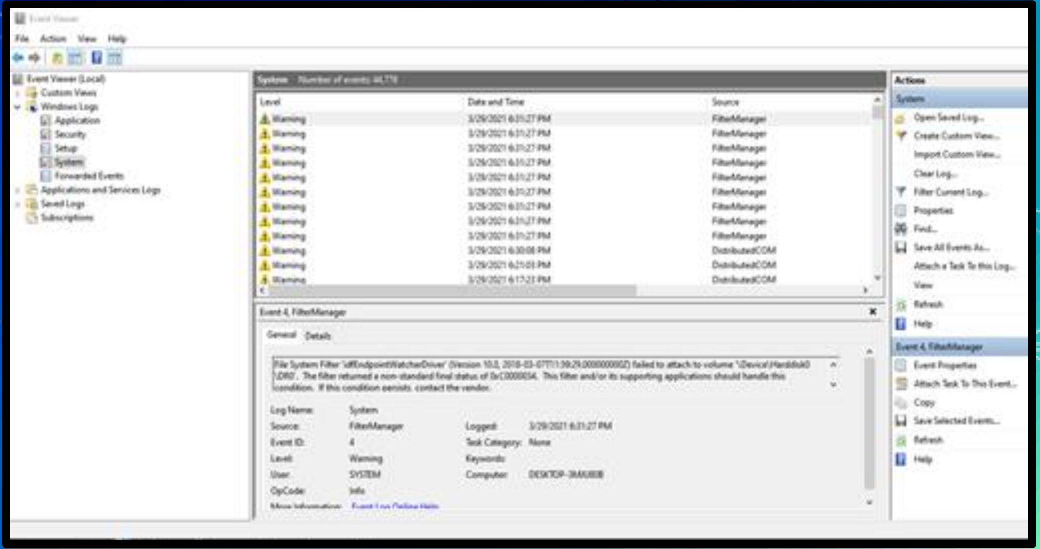
- PowerShell Integrated Scripting Environment (ISE)
- Extensive .NET integration



```
$stop=$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 = @()
$eRules = @()
$i=2
#build list of 1 < e < fi(N) List is $eRules
while($stop -eq $false){

    while($i -lt $fiN){
        $eRules+=$i
        $i++
    }

    $stop=$true
}

#factors of N and factors of fi(N)
$i=1
$stop=$false
while($stop -eq $false)
{

    while($i -le $sqrtN){
        if(($N % $i) -eq 0){
            $Nfactors += $i
            $Nfactors += $N/$i
        }

        $i++
    }
    $i=1
    while($i -le $sqrtfiN){

        if(($fiN % $i) -eq 0){

            $fiNfactors += $i
```

Event Log (.evtx)

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



System Number of events: 46,778

Level	Date and Time	Source
Warning	3/29/2021 6:31:27 PM	FilterManager
Warning	3/29/2021 6:31:27 PM	FilterManager
Warning	3/29/2021 6:31:27 PM	FilterManager
Warning	3/29/2021 6:31:27 PM	FilterManager
Warning	3/29/2021 6:31:27 PM	FilterManager
Warning	3/29/2021 6:31:27 PM	FilterManager
Warning	3/29/2021 6:31:27 PM	FilterManager
Warning	3/29/2021 6:31:27 PM	FilterManager
Warning	3/29/2021 6:31:27 PM	FilterManager
Warning	3/29/2021 6:30:08 PM	DistributedCOM
Warning	3/29/2021 6:21:03 PM	DistributedCOM
Warning	3/29/2021 6:17:23 PM	DistributedCOM

Event 4, FilterManager

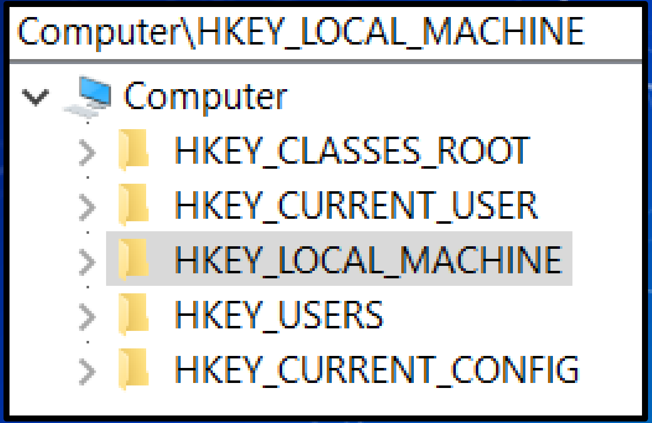
File System Filter 'sifEndpointWatcherDriver' (Version 10.0, 2018-03-07T11:39:29.000000000Z) failed to attach to volume '\Device\HarddiskVolume0\DR0'. The filter returned a non-standard final status of 0xC0000034. This filter and/or its supporting applications should handle this condition. If this condition persists, contact the vendor.

Log Name:	System		
Source:	FilterManager	Logged:	3/29/2021 6:31:27 PM
Event ID:	4	Task Category:	None
Level:	Warning	Keywords:	
User:	SYSTEM	Computer:	DESKTOP-3MAU80B
OpCode:	Info		

The Registry

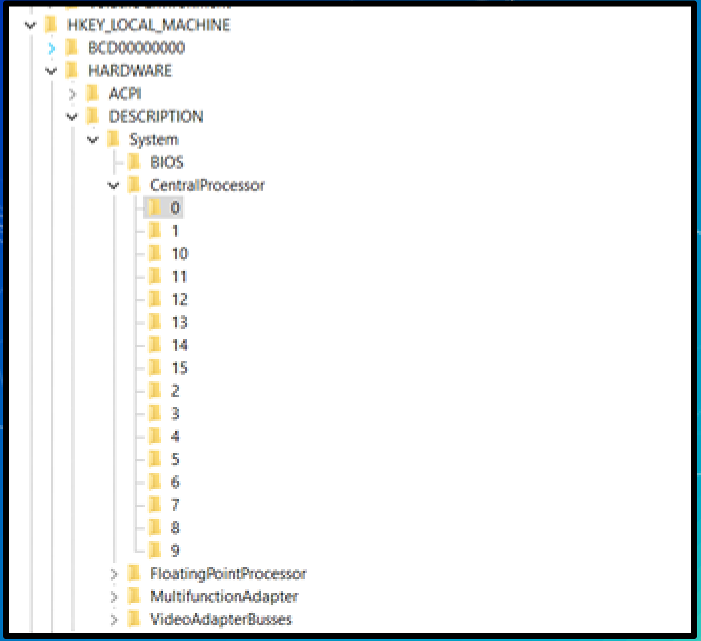
Registry

- Hierarchical database
  - Stores low-level settings



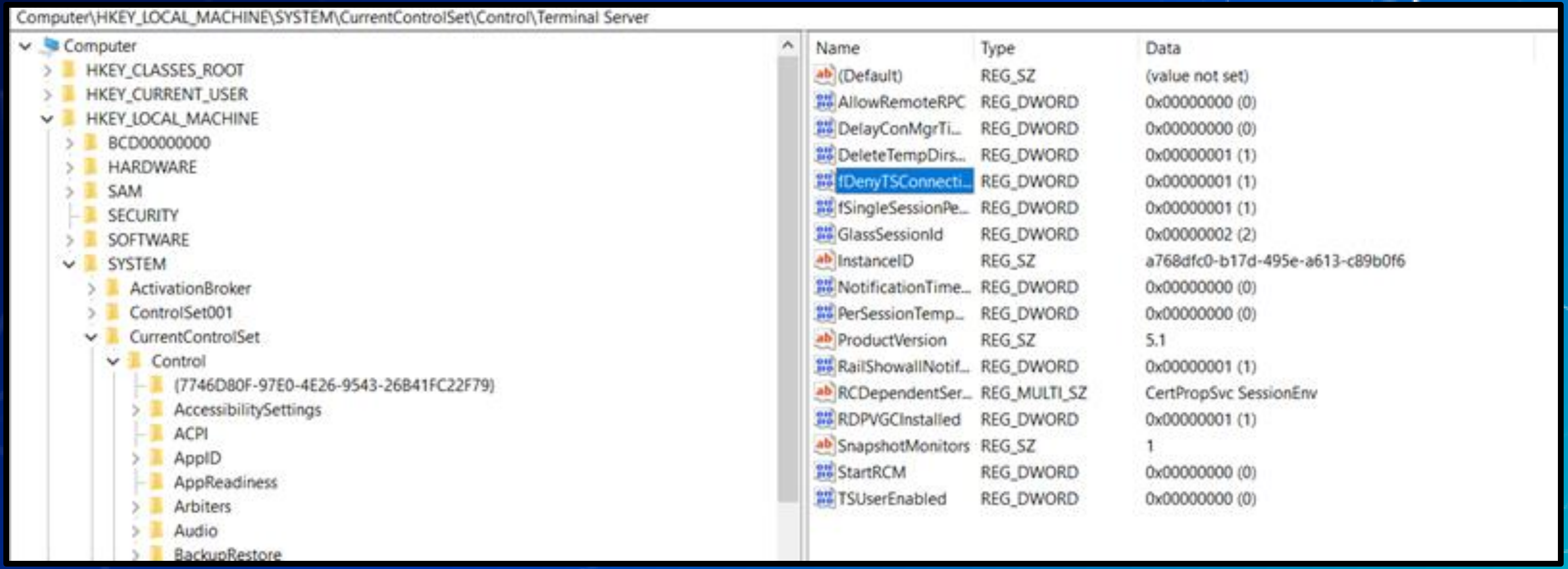
Computer\HKEY_LOCAL_MACHINE

```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
  HKEY_USERS
  HKEY_CURRENT_CONFIG
```



```
HKEY_LOCAL_MACHINE
  BCD00000000
  HARDWARE
    ACPI
    DESCRIPTION
      System
        BIOS
        CentralProcessor
          0
          1
          10
          11
          12
          13
          14
          15
          2
          3
          4
          5
          6
          7
          8
          9
        FloatingPointProcessor
        MultifunctionAdapter
        VideoAdapterBusses
```

Registry cont.

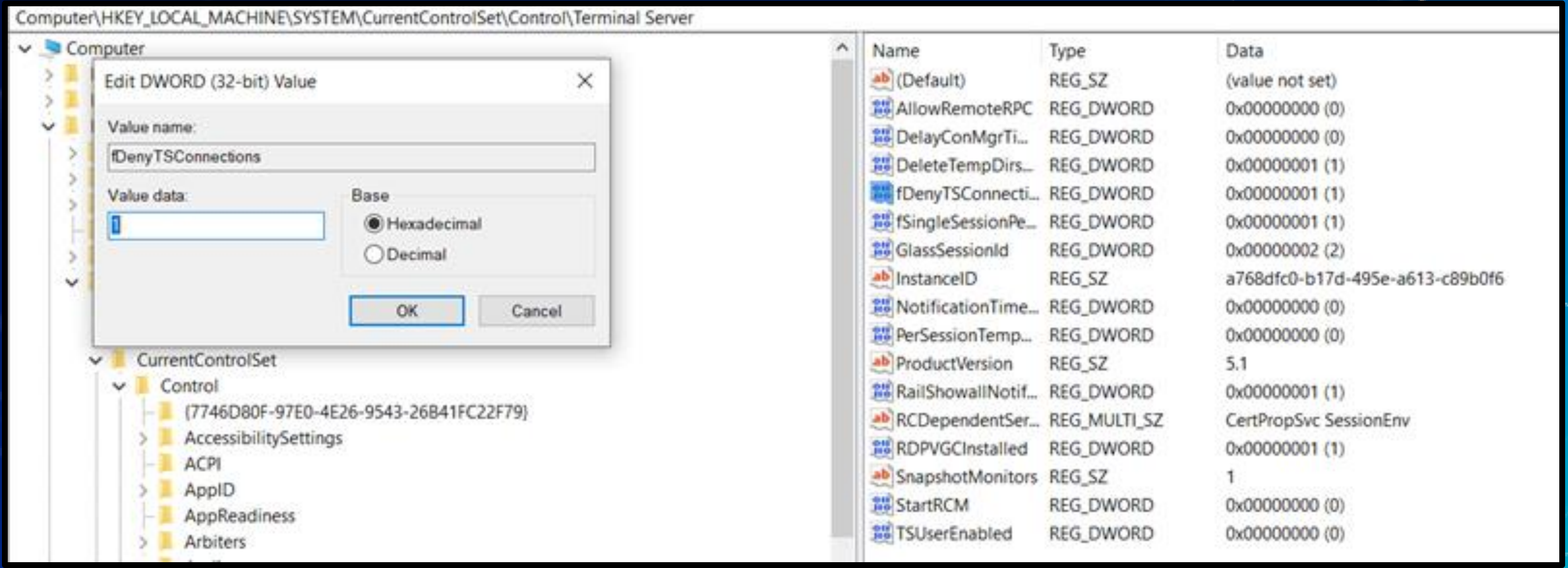


Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server

```
Computer
  HKEY_CLASSES_ROOT
  HKEY_CURRENT_USER
  HKEY_LOCAL_MACHINE
    BCD00000000
    HARDWARE
    SAM
    SECURITY
    SOFTWARE
    SYSTEM
      ActivationBroker
      ControlSet001
      CurrentControlSet
        Control
          {7746D80F-97E0-4E26-9543-26B41FC22F79}
          AccessibilitySettings
          ACPI
          AppID
          AppReadiness
          Arbiters
          Audio
          BackupRestore
```

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
RailShowallNotif...	REG_DWORD	0x00000001 (1)
RCDependentSer...	REG_MULTI_SZ	CertPropSvc SessionEnv
RDPVGCInstalled	REG_DWORD	0x00000001 (1)
SnapshotMonitors	REG_SZ	1
StartRCM	REG_DWORD	0x00000000 (0)
TSUserEnabled	REG_DWORD	0x00000000 (0)

Registry cont.



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

Edit DWORD (32-bit) Value

Value name:
fDenyTSConnections

Value data:
1

Base
● Hexadecimal
○ Decimal

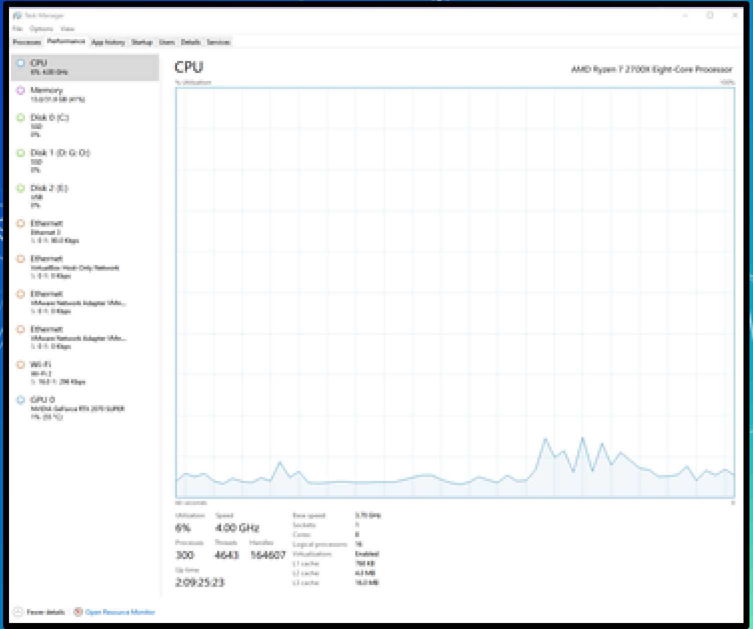
Name	Type	Data
(Default)	REG_SZ	(value not set)
AllowRemoteRPC	REG_DWORD	0x00000000 (0)
DelayConMgrTi...	REG_DWORD	0x00000000 (0)
DeleteTempDirs...	REG_DWORD	0x00000001 (1)
fDenyTSConnecti...	REG_DWORD	0x00000001 (1)
fSingleSessionPe...	REG_DWORD	0x00000001 (1)
GlassSessionId	REG_DWORD	0x00000002 (2)
InstanceID	REG_SZ	a768dfc0-b17d-495e-a613-c89b0f6
NotificationTime...	REG_DWORD	0x00000000 (0)
PerSessionTemp...	REG_DWORD	0x00000000 (0)
ProductVersion	REG_SZ	5.1
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)

Netdef

Task Manager

Task Manager

- Provides high-level view of what is running



CPU

Memory

Disk 0 (C:)

Disk 1 (D: G: O:)

Disk 2 (E:)

Ethernet

Ethernet

Ethernet

Ethernet

Wi-Fi

GPU 0

CPU

AMD Ryzen 7 2700X Eight-Core Processor

6%

4.00 GHz

300

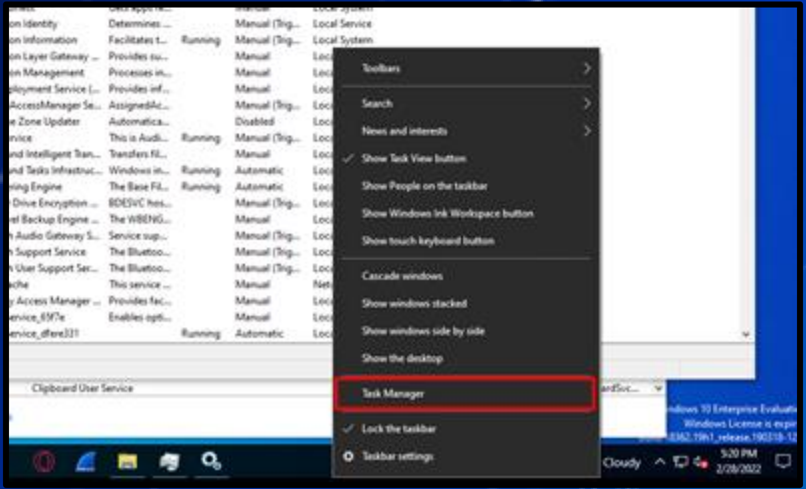
4643

164607

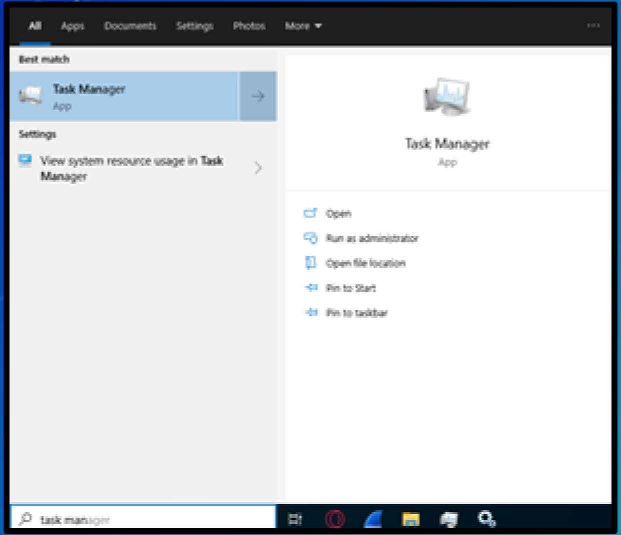
2:09:25:23

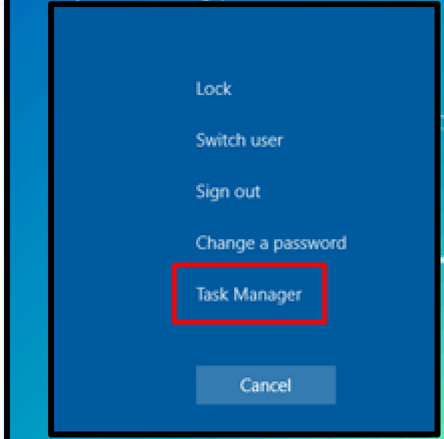
Task Manager cont.

- How to open it?



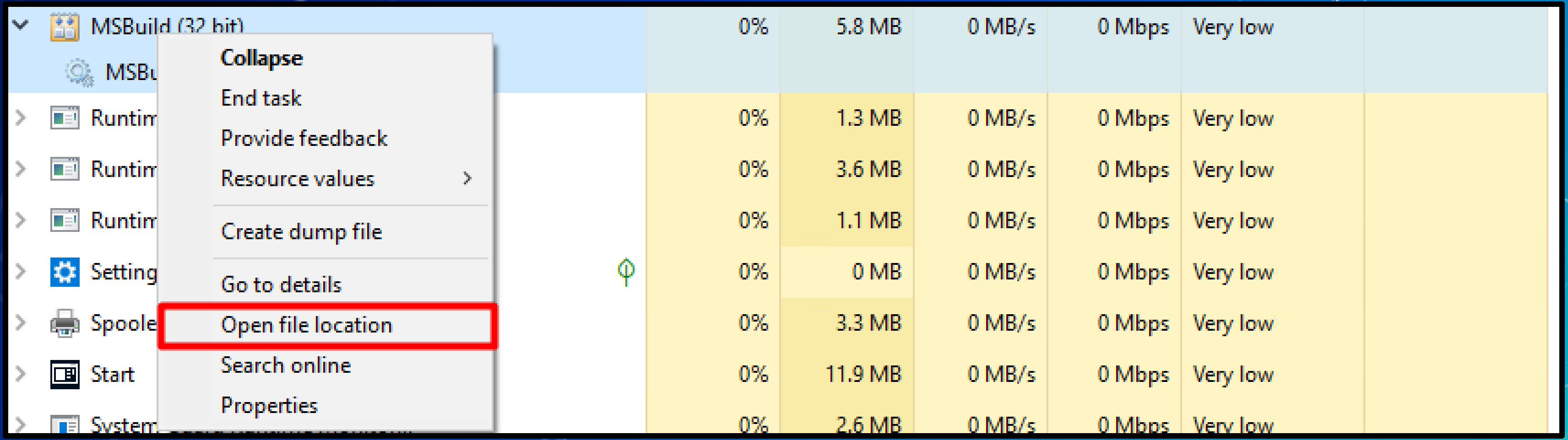
on Identity	Determines ...		Manual (Trig...	Local Service
on Information	Facilitates t...	Running	Manual (Trig...	Local System
on Layer Gateway ...	Provides su...		Manual	Loc
on Management	Processes in...		Manual	Loc
ployment Service (...	Provides inf...		Manual	Loc
AccessManager Se...	AssignedAc...		Manual (Trig...	Loc
e Zone Updater	Automatica...		Disabled	Loc
rvice	This is Audi...	Running	Manual (Trig...	Loc
nd Intelligent Tran...	Transfers fil...		Manual	Loc
nd Tasks Infrastruc...	Windows in...	Running	Automatic	Loc
ing Engine	The Base Fil...	Running	Automatic	Loc
Drive Encryption ...	BDESVC hos...		Manual (Trig...	Loc
el Backup Engine ...	The WBENG...		Manual	Loc
h Audio Gateway S...	Service sup...		Manual (Trig...	Loc
h Support Service	The Bluetoo...		Manual (Trig...	Loc
h User Support Ser...	The Bluetoo...		Manual (Trig...	Loc
che	This service ...		Manual	Net
y Access Manager ...	Provides fac...		Manual	Loc
ervice_65f7e	Enables opti...		Manual	Loc
ervice_dfere331		Running	Automatic	Loc





Task Manager cont.

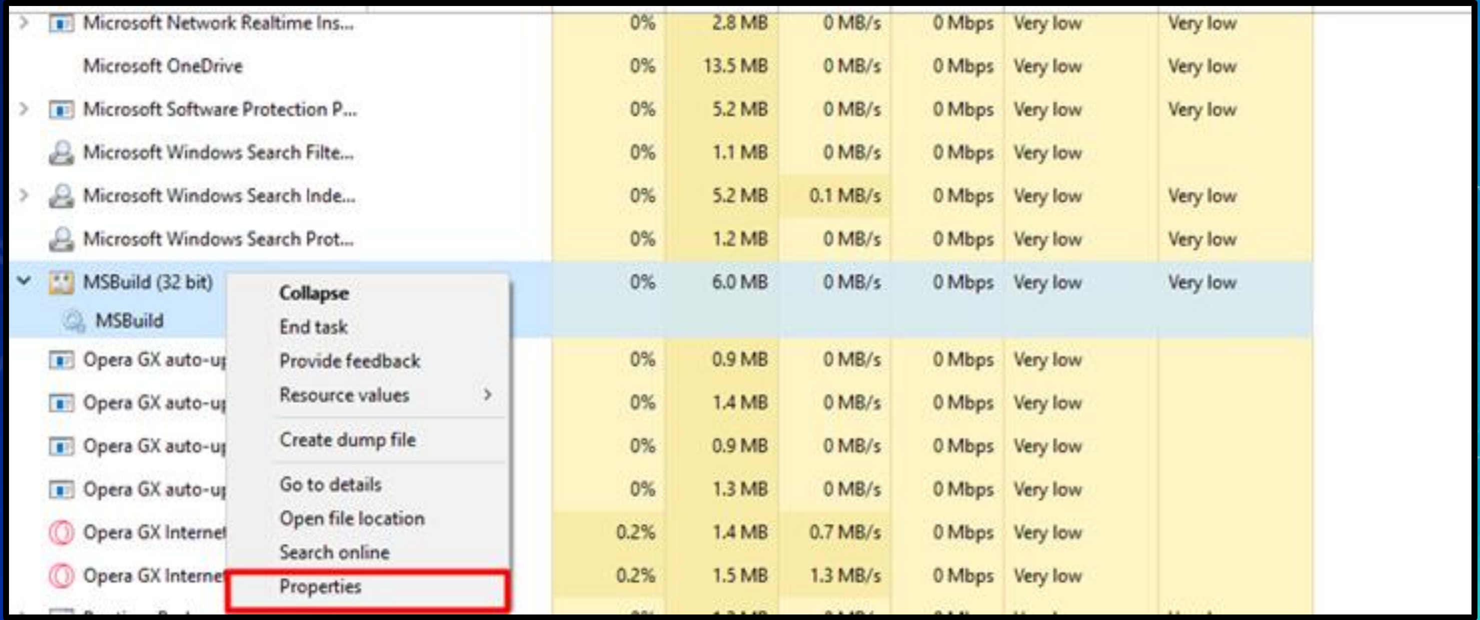
- Can be used to find the location a running executable.



MSBuild (32 bit)	0%	5.8 MB	0 MB/s	0 Mbps	Very low
MSBu					
Runtim	0%	1.3 MB	0 MB/s	0 Mbps	Very low
Runtim	0%	3.6 MB	0 MB/s	0 Mbps	Very low
Runtim	0%	1.1 MB	0 MB/s	0 Mbps	Very low
Setting	0%	0 MB	0 MB/s	0 Mbps	Very low
Spoole	0%	3.3 MB	0 MB/s	0 Mbps	Very low
Start	0%	11.9 MB	0 MB/s	0 Mbps	Very low
System	0%	2.6 MB	0 MB/s	0 Mbps	Very low

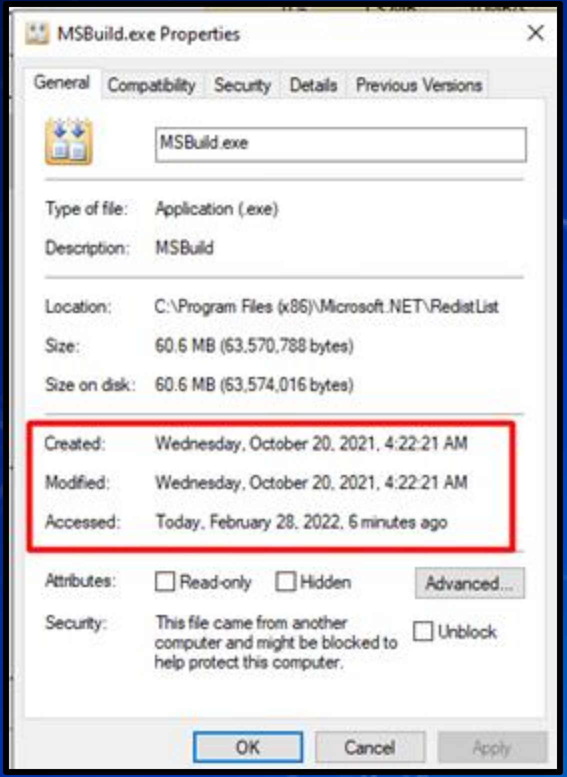
Task Manager cont.

- Show the properties of an executable



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

Task Manager cont.



MSBuild.exe Properties

MSBuild.exe

Type of file: Application (.exe)

Description: MSBuild

Location: C:\Program Files (x86)\Microsoft.NET\RedistList

Size: 60.6 MB (63,570,788 bytes)

Size on disk: 60.6 MB (63,574,016 bytes)

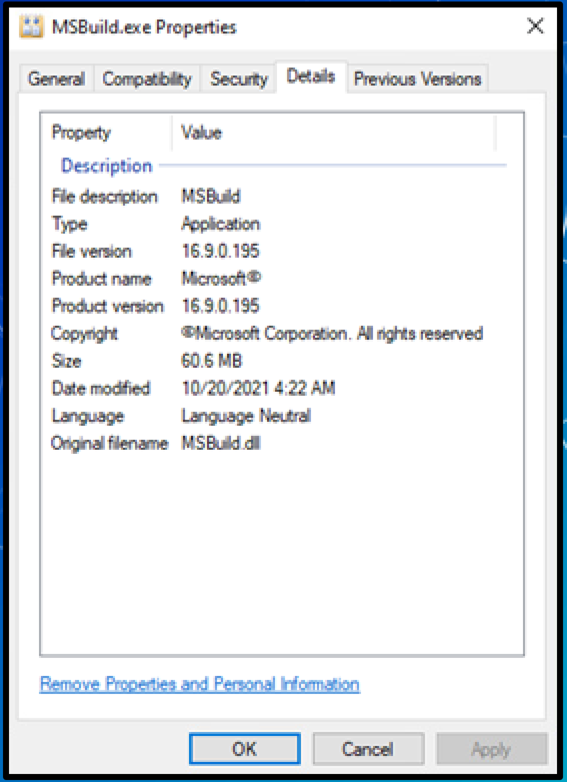
Created: Wednesday, October 20, 2021, 4:22:21 AM

Modified: Wednesday, October 20, 2021, 4:22:21 AM

Accessed: Today, February 28, 2022, 6 minutes ago

Attributes: □ Read-only □ Hidden Advanced...

Security: This file came from another computer and might be blocked to help protect this computer. □ Unblock



MSBuild.exe Properties

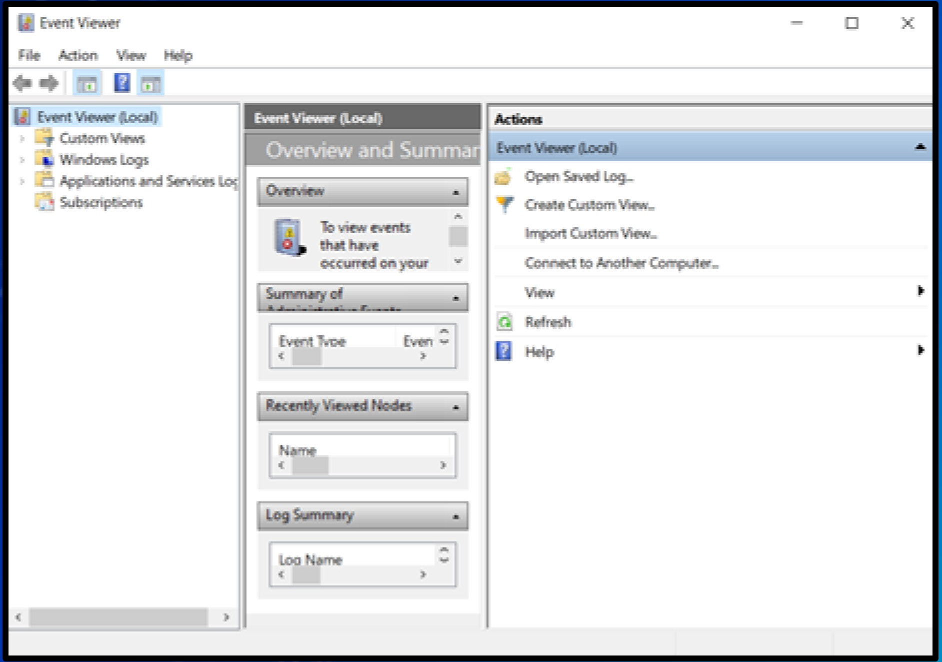
Property	Value
Description	
File description	MSBuild
Type	Application
File version	16.9.0.195
Product name	Microsoft®
Product version	16.9.0.195
Copyright	©Microsoft Corporation. All rights reserved
Size	60.6 MB
Date modified	10/20/2021 4:22 AM
Language	Language Neutral
Original filename	MSBuild.dll

Remove Properties and Personal Information

Event Viewer

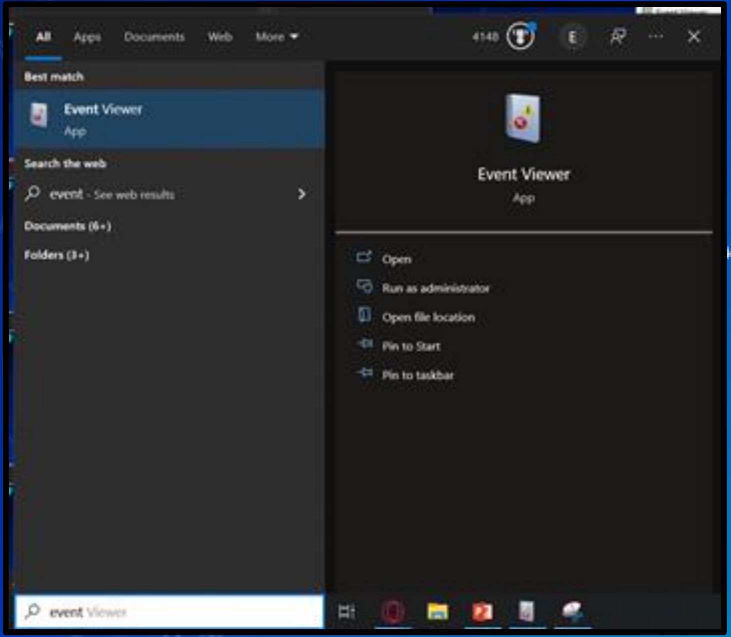
Event Viewer

- Log viewer for Windows



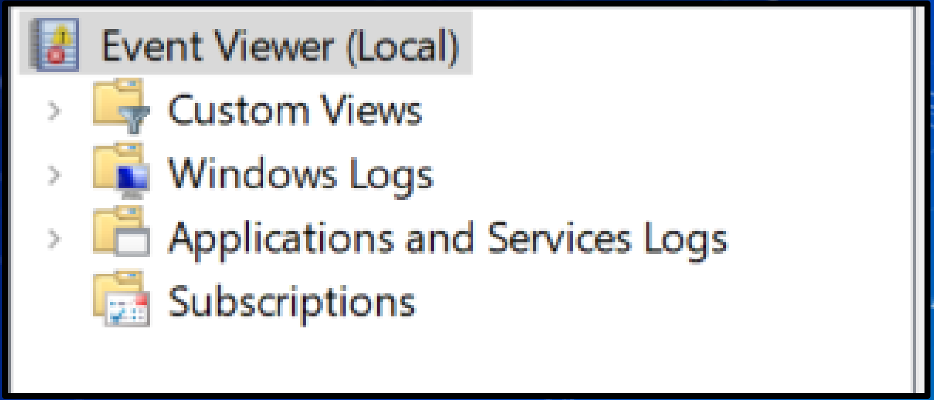
Event Viewer

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

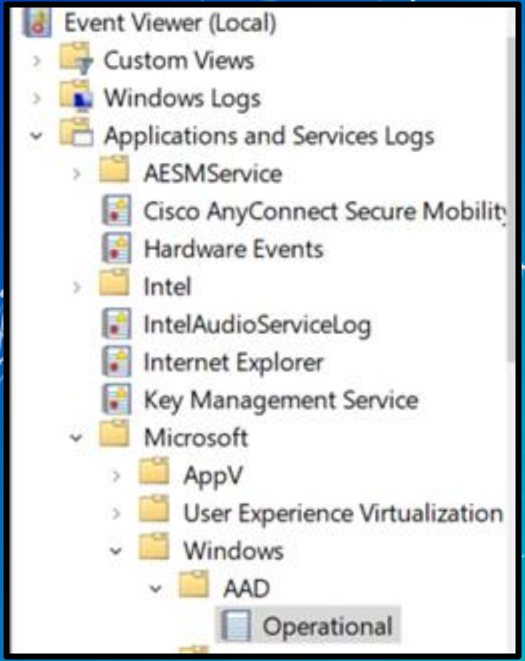


Event Viewer cont.

- Logs are stored in a hierarchical structure



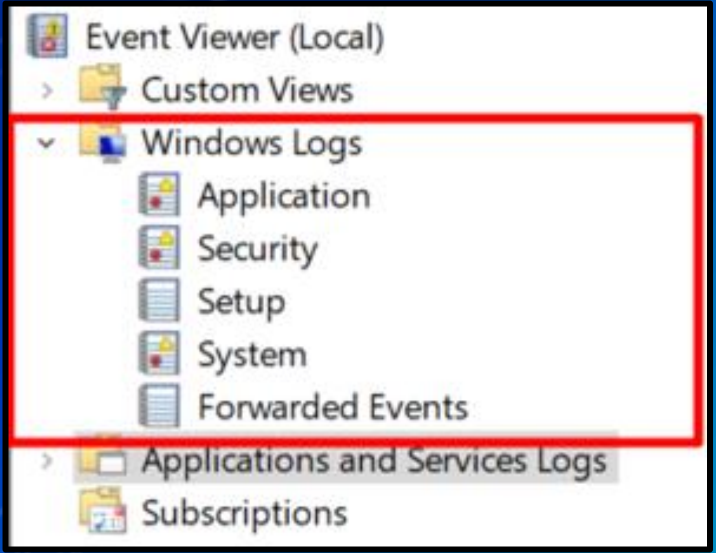
```
Event Viewer (Local)
  > Custom Views
  > Windows Logs
  > Applications and Services Logs
    Subscriptions
```



```
Event Viewer (Local)
  > Custom Views
  > Windows Logs
  v Applications and Services Logs
      > AESMService
        Cisco AnyConnect Secure Mobilit
        Hardware Events
      > Intel
        IntelAudioServiceLog
        Internet Explorer
        Key Management Service
      v Microsoft
          > AppV
          > User Experience Virtualization
          v Windows
              v AAD
                  Operational
```

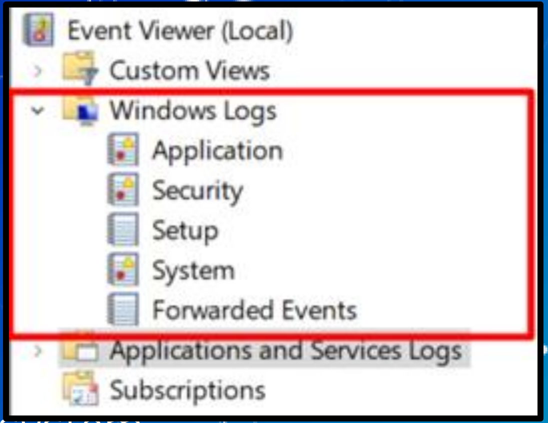
Event Viewer cont.

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



Event Viewer (Local)
- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Logs
- Subscriptions

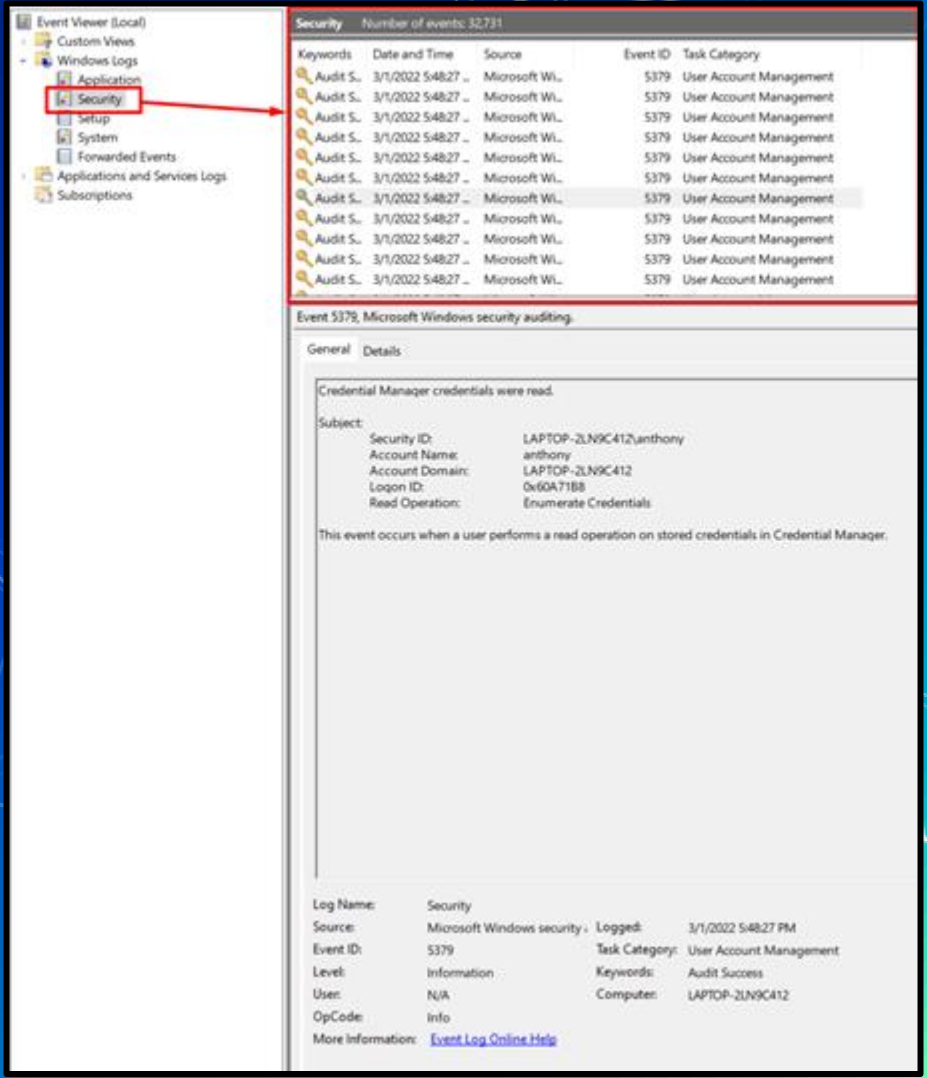
Event Viewer cont.


Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Subscriptions

- 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



Security   Number of events: 32,731

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

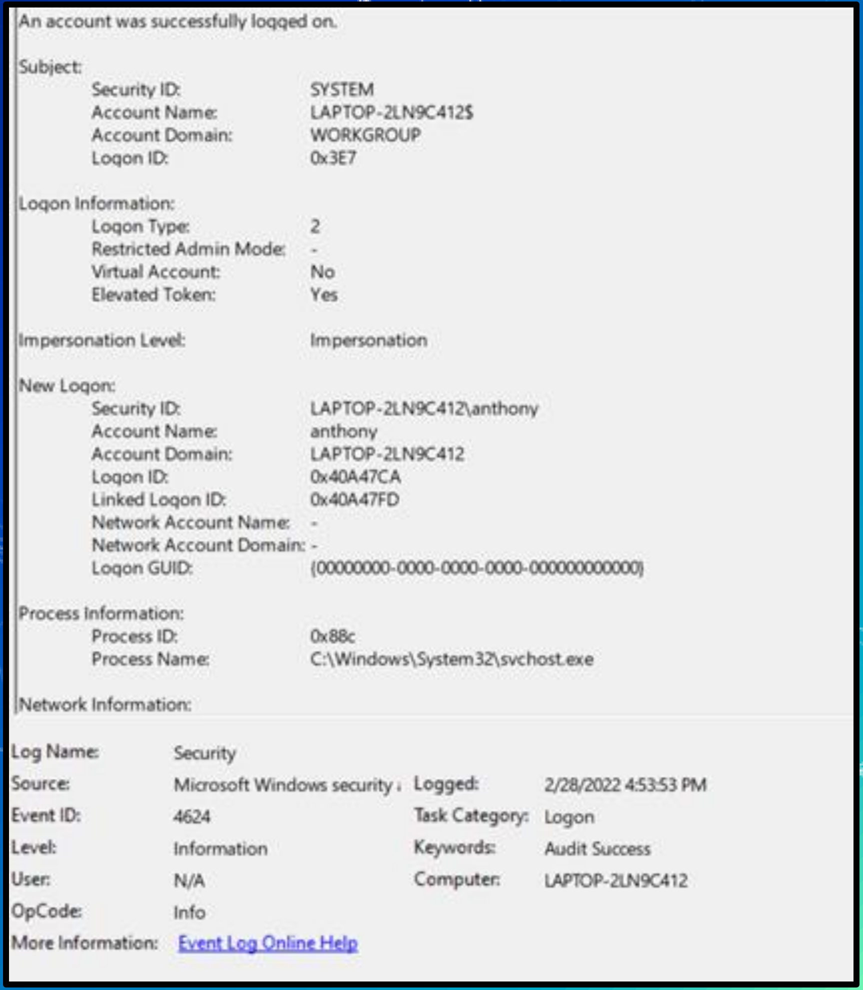
Event 5379, Microsoft Windows security auditing.

```
Credential Manager credentials were read.

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

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

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

Event Viewer cont.

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



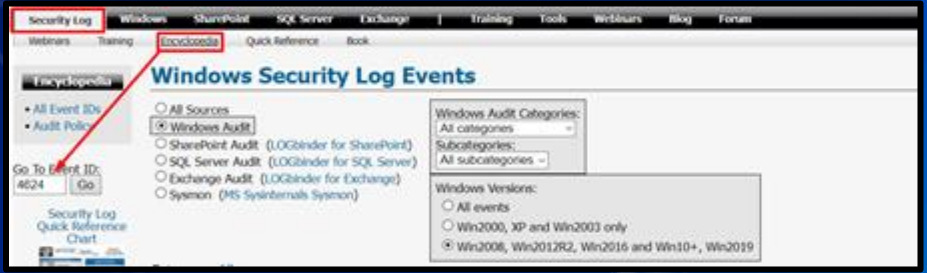
```
An account was successfully logged on.

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

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

Impersonation Level:                Impersonation

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

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

Network Information:
```

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

Event Viewer cont.

- Event IDs
  - Identifier numbers Microsoft assigns to types of events.
- Resource for Security Event IDs
  - https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx

Event Viewer cont.



Windows Security Log Events

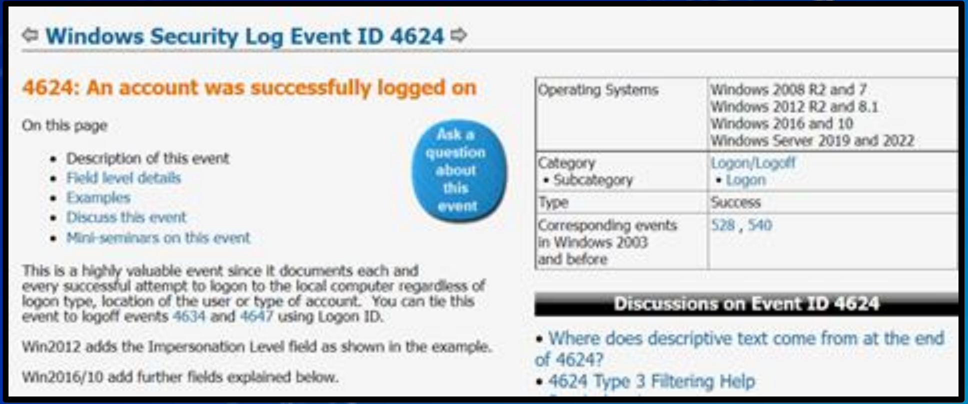
○ All Sources
● Windows Audit
○ SharePoint Audit (LOGbinder for SharePoint)
○ SQL Server Audit (LOGbinder for SQL Server)
○ Exchange Audit (LOGbinder for Exchange)
○ Sysmon (MS Sysinternals Sysmon)

Go To Event ID: 4624

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.

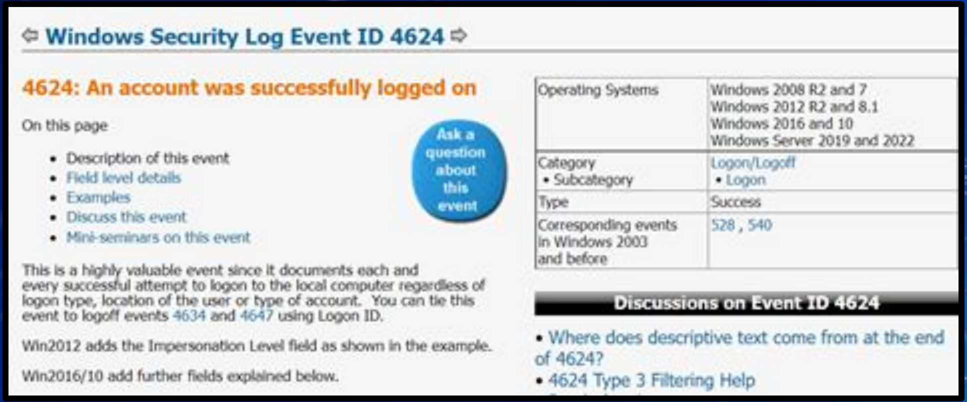
Win2016/10 add further fields explained below.

Operating Systems	Windows 2008 R2 and 7 Windows 2012 R2 and 8.1 Windows 2016 and 10 Windows Server 2019 and 2022
Category • 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.



⇦ 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.

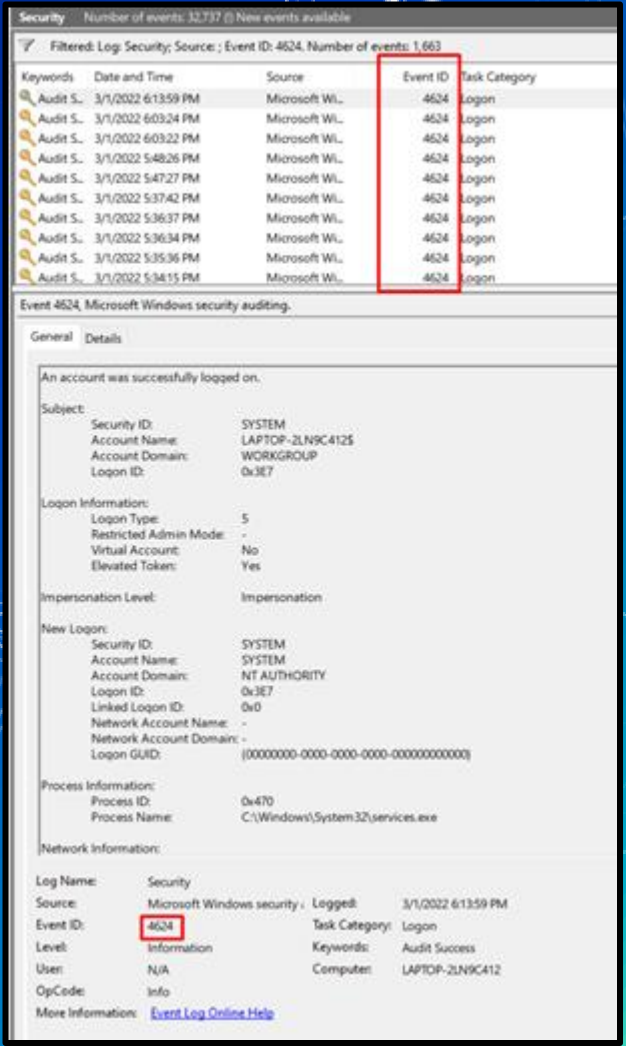
Win2012 adds the Impersonation Level field as shown in the example.

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 • 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



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

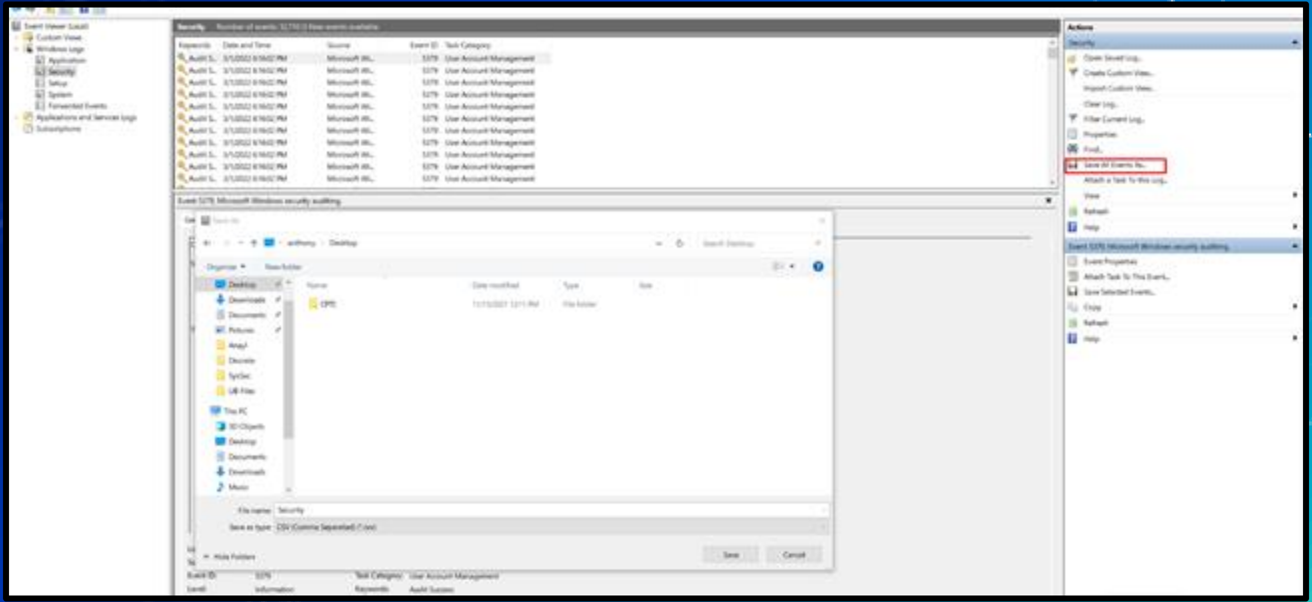
Event 4624, Microsoft Windows security auditing.

```
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:                Impersonation

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

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

Network Information:
```

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

Event Viewer cont.

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



Security Number of events: 32,750 [illegible]

Keywords	Date and Time	Source	Event ID	Task Category
Audit S...	3/1/2022 8:16:02 PM	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 8:16:02 PM	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 8:16:02 PM	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 8:16:02 PM	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 8:16:02 PM	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 8:16:02 PM	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 8:16:02 PM	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 8:16:02 PM	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 8:16:02 PM	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 8:16:02 PM	Microsoft Wi...	5379	User Account Management
Audit S...	3/1/2022 8:16:02 PM	Microsoft Wi...	5379	User Account Management

Event 5379, Microsoft Windows security auditing.

File name: Security

Save as type: CSV (Comma Separated) (*.csv)

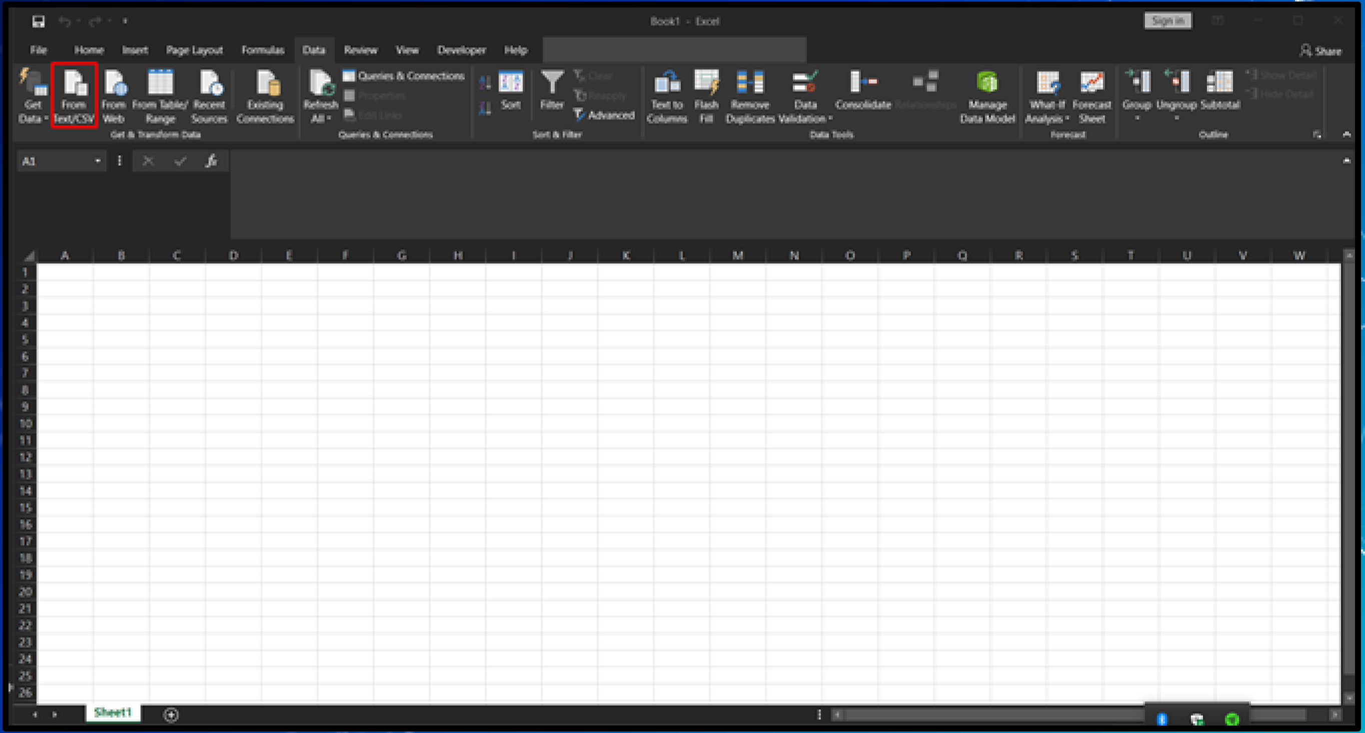
Event ID: 5379 Task Category: User Account Management

Level: Information Keywords: Audit Success

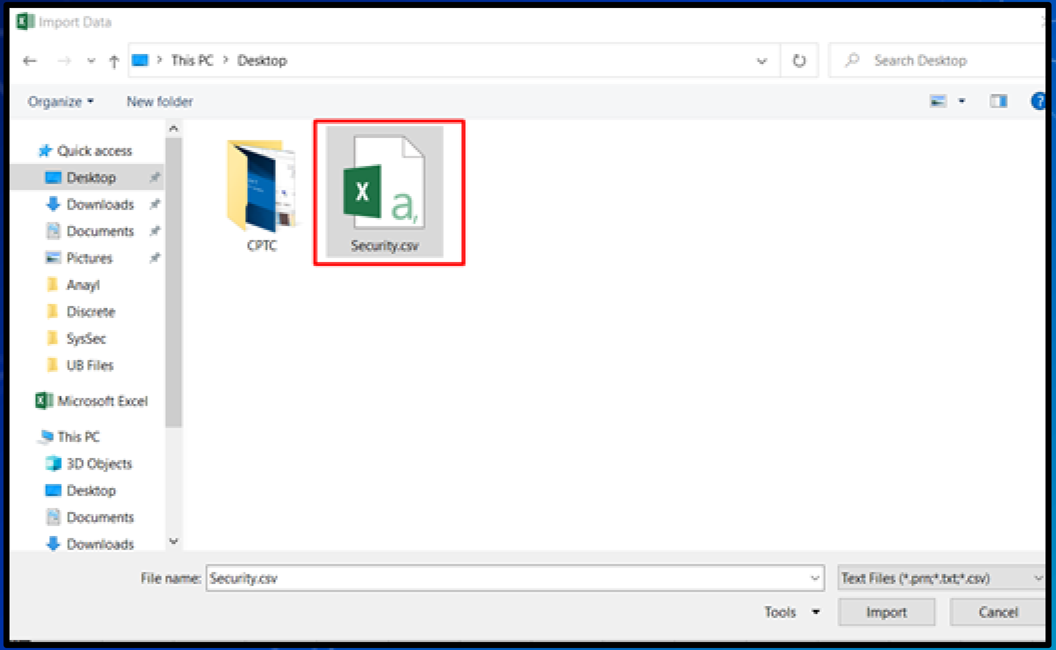
Event Viewer cont.

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

Importing Logs in Excel



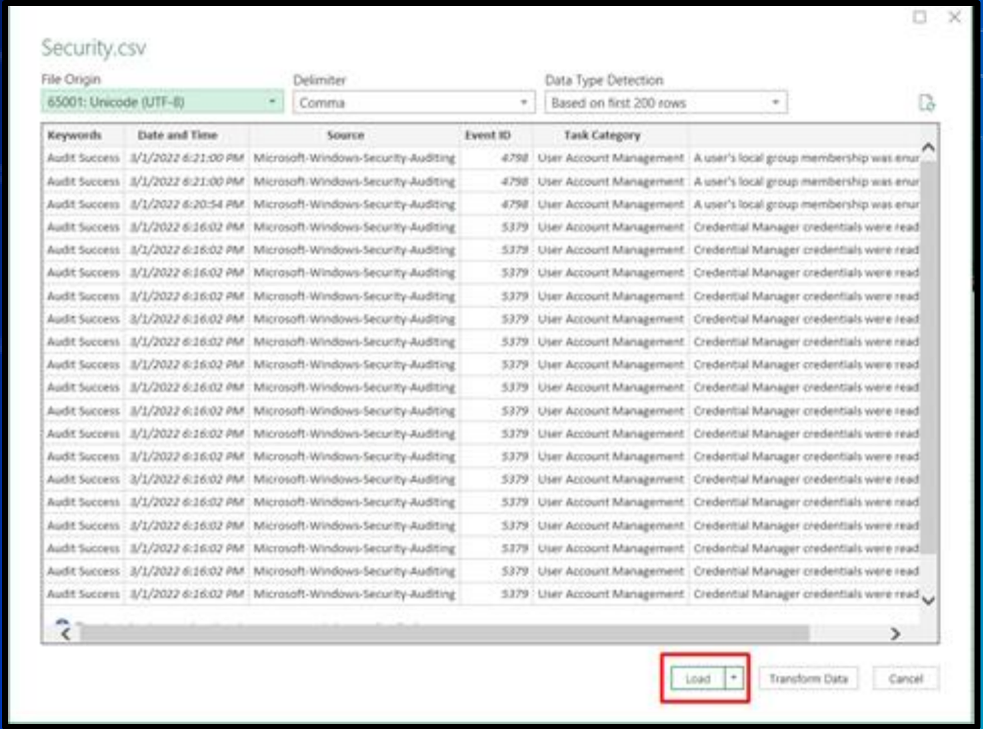
Importing Logs in Excel



File name: Security.csv

Text Files (*.prn;*.txt;*.csv)

Importing Logs in Excel



Security.csv

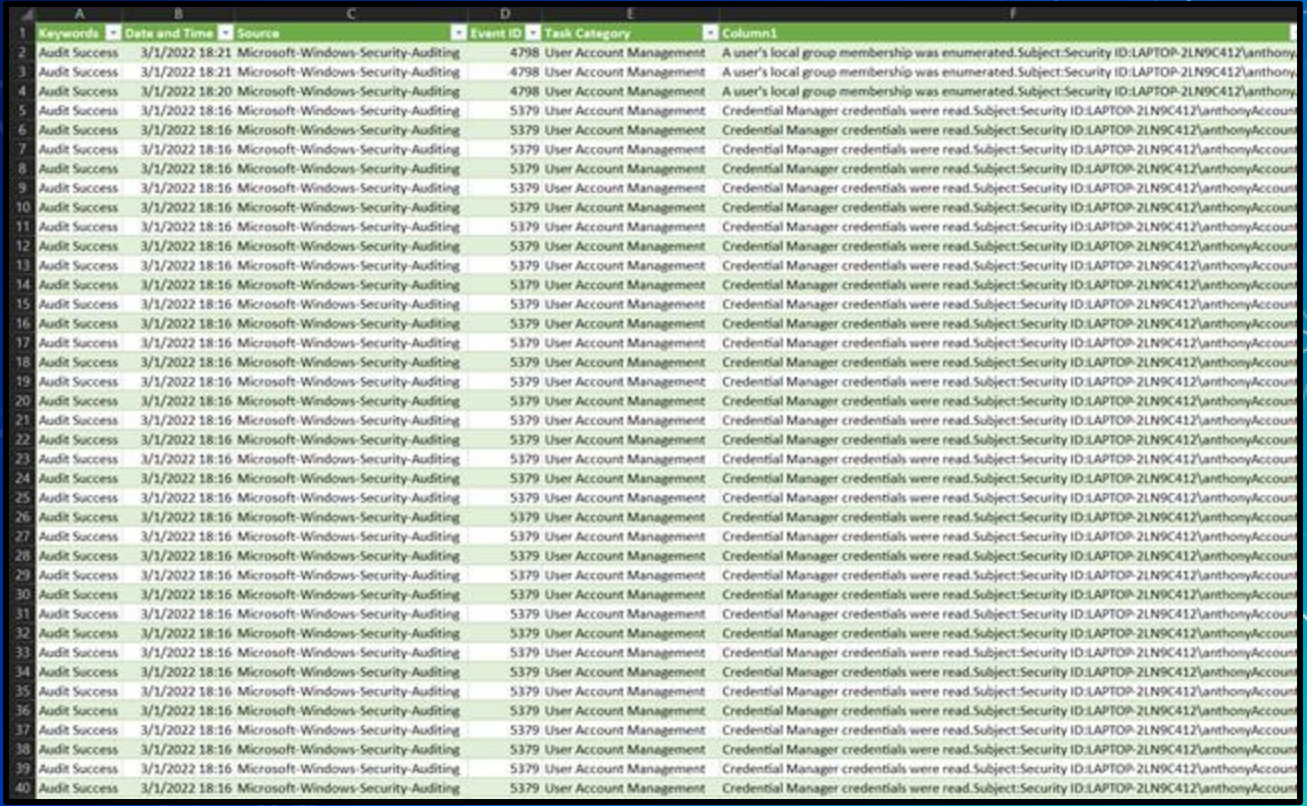
File Origin: 65001: Unicode (UTF-8)

Delimiter: Comma

Data Type Detection: Based on first 200 rows

Keywords	Date and Time	Source	Event ID	Task Category	
Audit Success	3/1/2022 6:21:00 PM	Microsoft-Windows-Security-Auditing	4798	User Account Management	A user's local group membership was 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

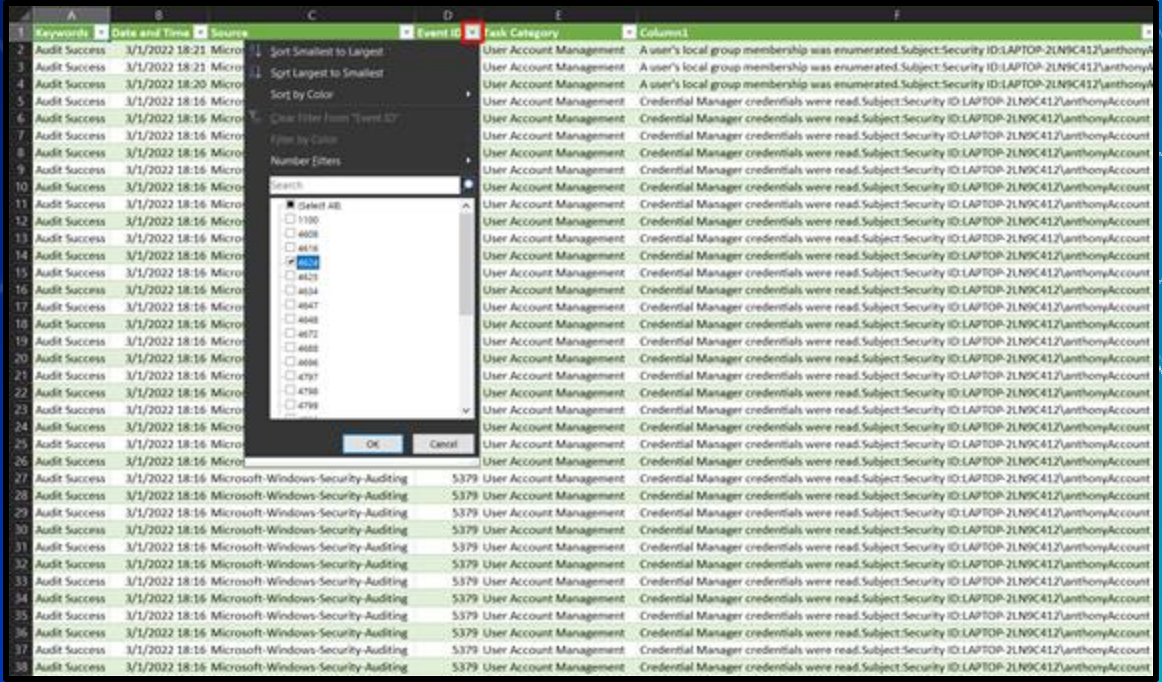
Logs in Excel



	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

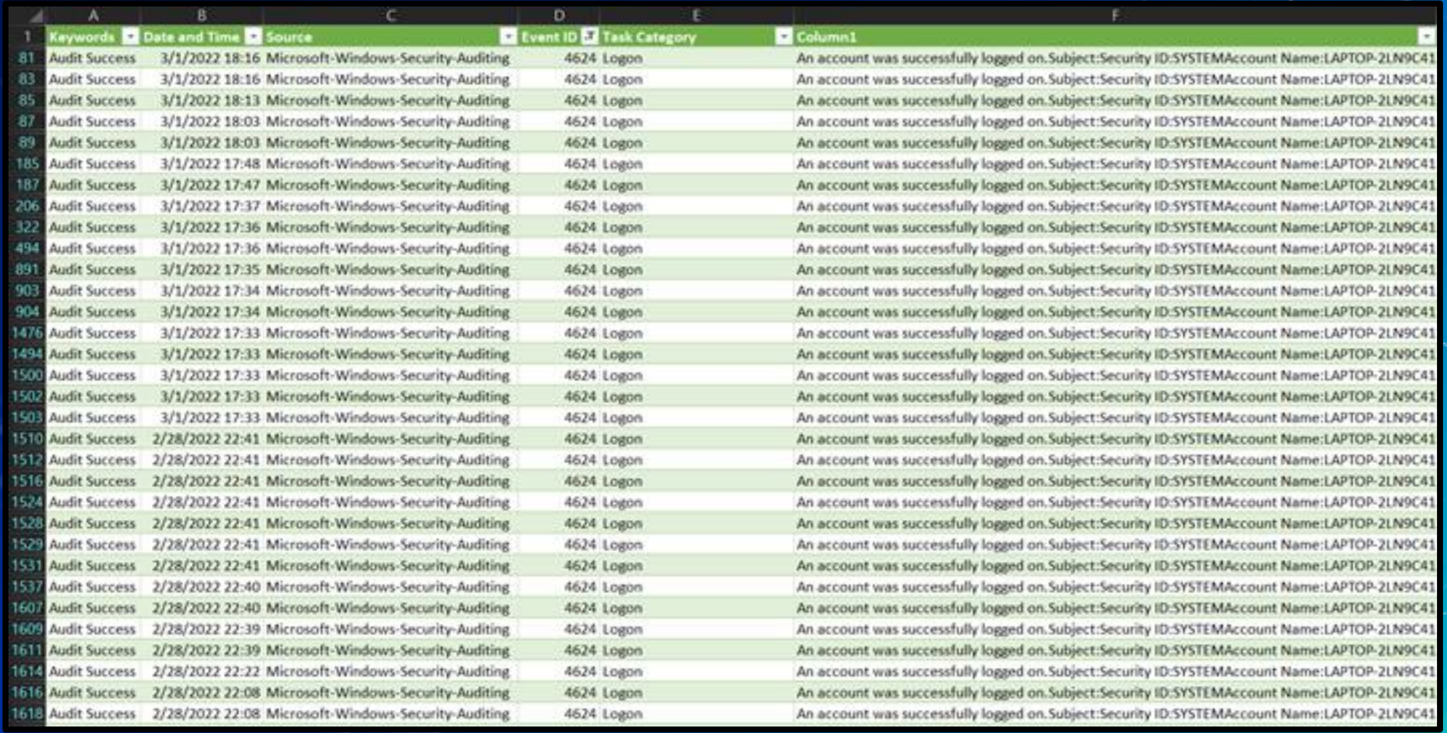
Logs in Excel

- Within Excel we can search logs using filters.



	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	Micro		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	Micro		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	Micro		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	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
6	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
7	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
8	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
9	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
10	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
11	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
12	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
13	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
14	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
15	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
16	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
17	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
18	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
19	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
20	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
21	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
22	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
23	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
24	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
25	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
26	Audit Success	3/1/2022 18:16	Micro		User Account Management	Credential Manager credentials were read.Subject:Security ID:LAPTOP-2LN9C412\anthonyAccount
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\anthonyAccount
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\anthonyAccount
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\anthonyAccount
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\anthonyAccount
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\anthonyAccount
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\anthonyAccount
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\anthonyAccount
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\anthonyAccount
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\anthonyAccount
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\anthonyAccount
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\anthonyAccount
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\anthonyAccount

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.

Questions?

Network Forensics

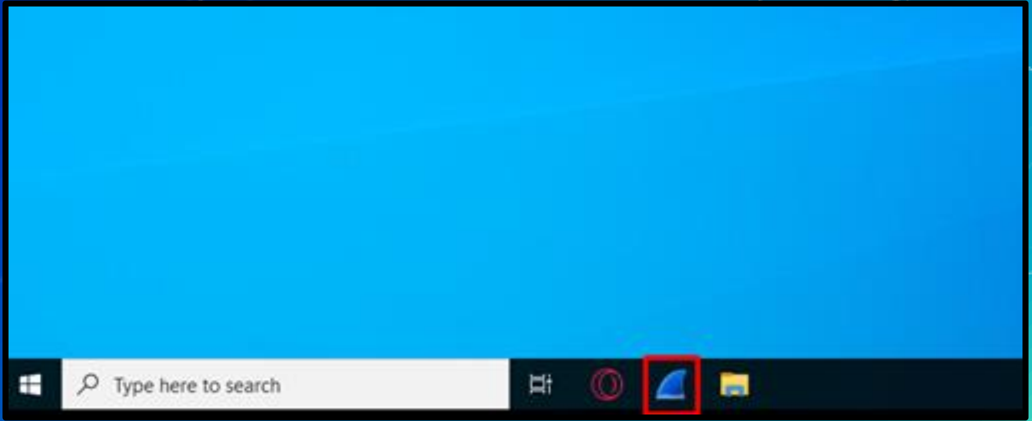
NetDef

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



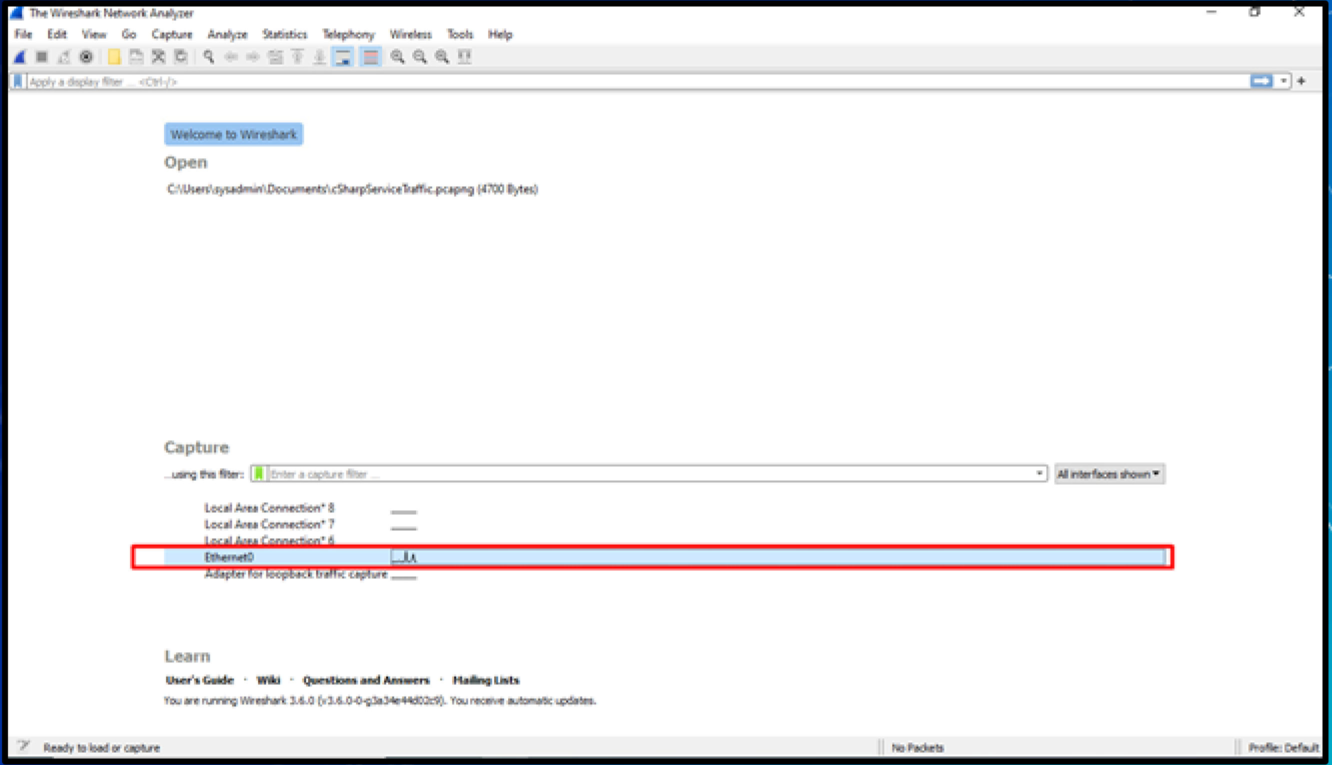
In Class Activity

WireShark

Hands on 0 - Wireshark

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

Network Forensics Hands-on



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark

Open

C:\Users\sysadmin\Documents\cSharpServiceTraffic.pcapng (4700 Bytes)

Capture

...using this filter: Enter a capture filter ... All interfaces shown

Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6
Ethernet0
Adapter for loopback traffic capture

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.6.0 (v3.6.0-0-g3a34e44d02c9). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

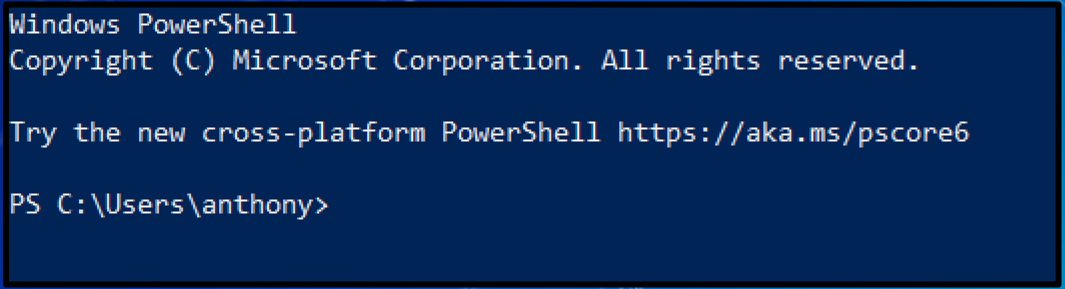
Break Slide

Netdef

PowerShell For IR

PowerShell

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



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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\anthony>
```

Cmdlets

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

Get-Filehash

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

In Class Activity

PowerShell

Hands on 1 – Piping Output

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

Hands on 1 – Piping Output

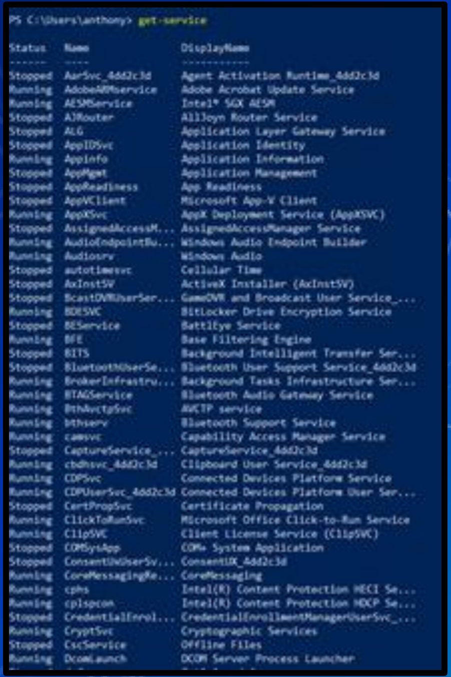
- Any problems with the result?

Hands on 1 – Piping Output

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

Searching PowerShell Output

- `Get-Service` “Gets the services on the computer.”

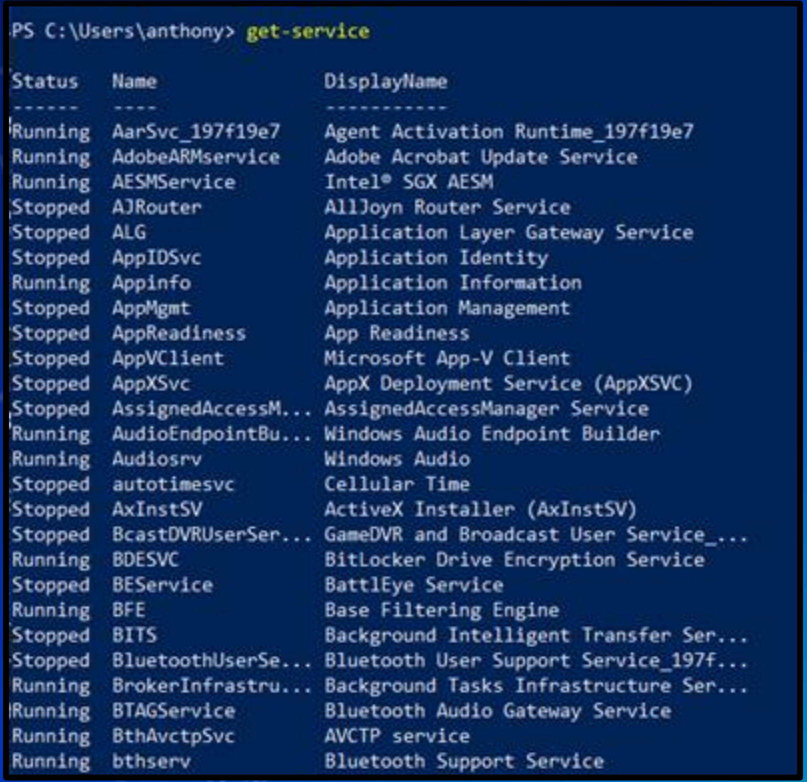


```
PS C:\Users\anthony> get-service

Status   Name               DisplayName
------   ----               -----------
Stopped  AarSvc_4dd2c3d     Agent Activation Runtime_4dd2c3d
Running  AdobeARMservice    Adobe Acrobat Update Service
Running  AESMService        Intel® SGX AESM
Stopped  AJRouter           AllJoyn Router Service
Stopped  ALG                Application Layer Gateway Service
Stopped  AppIDSvc           Application Identity
Running  Appinfo            Application Information
Stopped  AppMgmt            Application Management
Stopped  AppReadiness       App Readiness
Stopped  AppVClient         Microsoft App-V Client
Running  AppXSvc            AppX Deployment Service (AppXSVC)
Stopped  AssignedAccessM... AssignedAccessManager Service
Running  AudioEndpointBu... Windows Audio Endpoint Builder
Running  Audiosrv           Windows Audio
Stopped  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
```

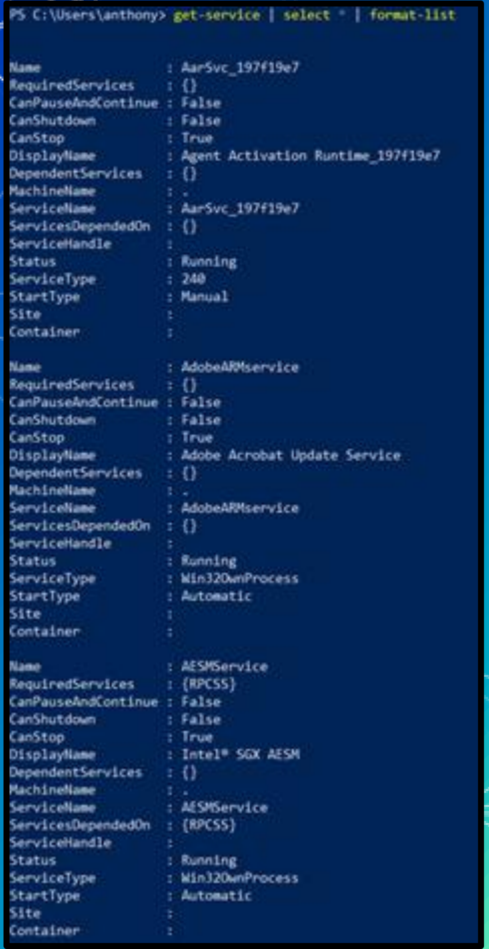
Hands on 2 – Searching Output

- 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`?

Break Slide

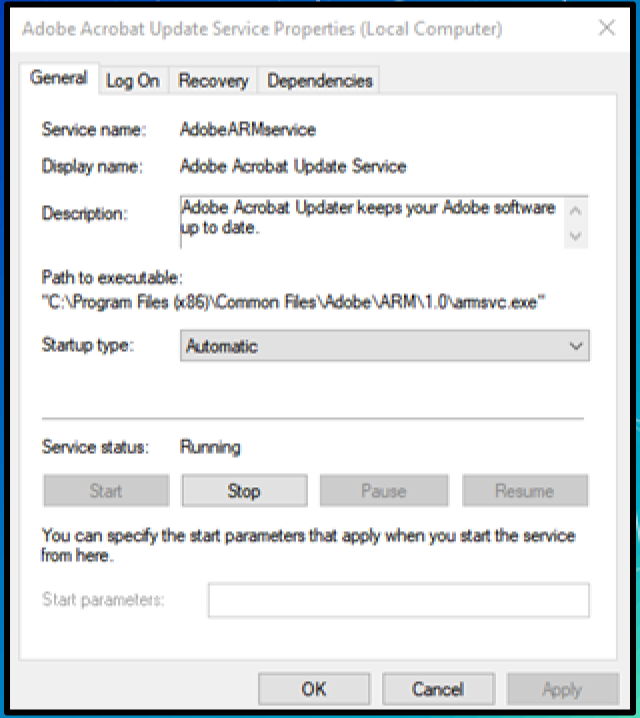
WMI & Services

Windows Management Instrumentation (WMI)

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

Services

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



Adobe Acrobat Update Service Properties (Local Computer)

Service name: AdobeARMservice

Display name: Adobe Acrobat Update Service

Description: Adobe Acrobat Updater keeps your Adobe software up to date.

Path to executable:
"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"

Startup type: Automatic

Service status: Running

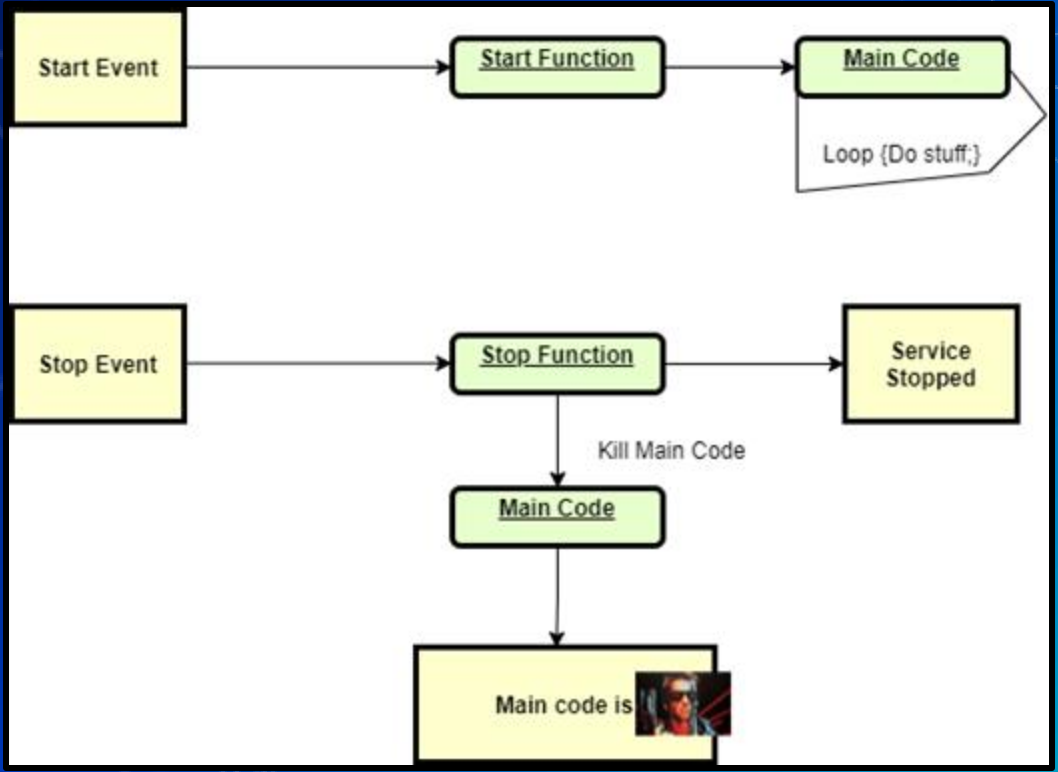
You can specify the start parameters that apply when you start the service from here.

Start parameters:

Services

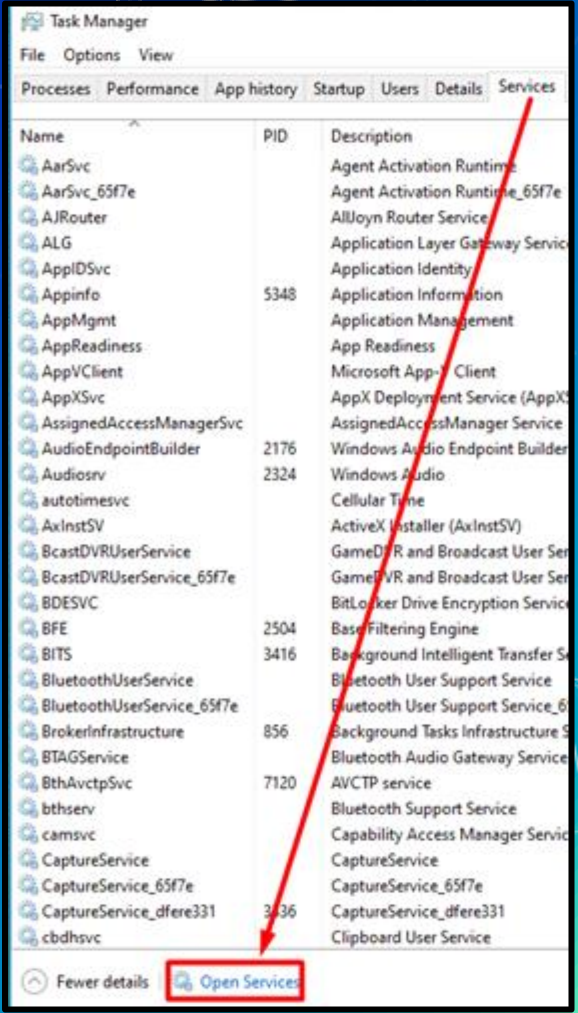
- Can run as `nt authority \system`
  - `nt authority \system` != `root`
  - Is more powerful than an "administrator"
- Active even when no user is signed in
- May be hosted by the service host (svchost.exe)
- May executables that are designated to be services
- Follow a defined service model

Service Model



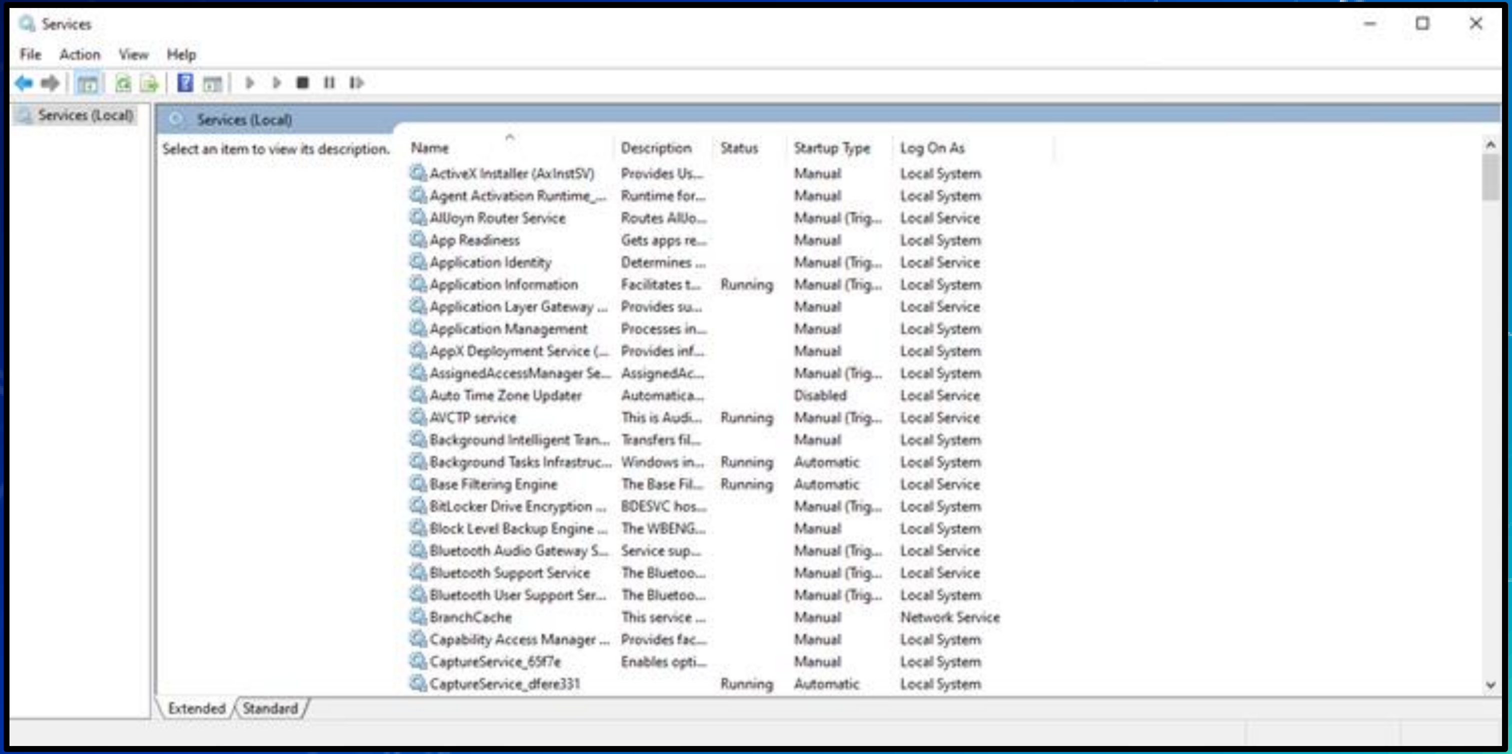
How to list services?

- Open Task Manager and navigate to services tab


Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
Open Services

Name	PID	Description
AarSvc		Agent Activation Runtime
AarSvc_65f7e		Agent Activation Runtime_65f7e
AJRouter		AllJoyn Router Service
ALG		Application Layer Gateway Servic
AppIDSvc		Application Identity
Appinfo	5348	Application Information
AppMgmt		Application Management
AppReadiness		App Readiness
AppVClient		Microsoft App-V Client
AppXSvc		AppX Deployment Service (AppX
AssignedAccessManagerSvc		AssignedAccessManager Service
AudioEndpointBuilder	2176	Windows Audio Endpoint Builder
Audiosrv	2324	Windows Audio
autotimesvc		Cellular Time
AxInstSV		ActiveX Installer (AxInstSV)
BcastDVRUserService		GameDVR and Broadcast User Ser
BcastDVRUserService_65f7e		GameDVR and Broadcast User Ser
BDESVC		BitLocker Drive Encryption Servic
BFE	2504	Base Filtering Engine
BITS	3416	Background Intelligent Transfer S
BluetoothUserService		Bluetooth User Support Service
BluetoothUserService_65f7e		Bluetooth User Support Service_6
BrokerInfrastructure	856	Background Tasks Infrastructure S
BTAGService		Bluetooth Audio Gateway Service
BthAvctpSvc	7120	AVCTP service
bthserv		Bluetooth Support Service
camsvc		Capability Access Manager Servic
CaptureService		CaptureService
CaptureService_65f7e		CaptureService_65f7e
CaptureService_dfere331	3436	CaptureService_dfere331
cbdhsvc		Clipboard User Service

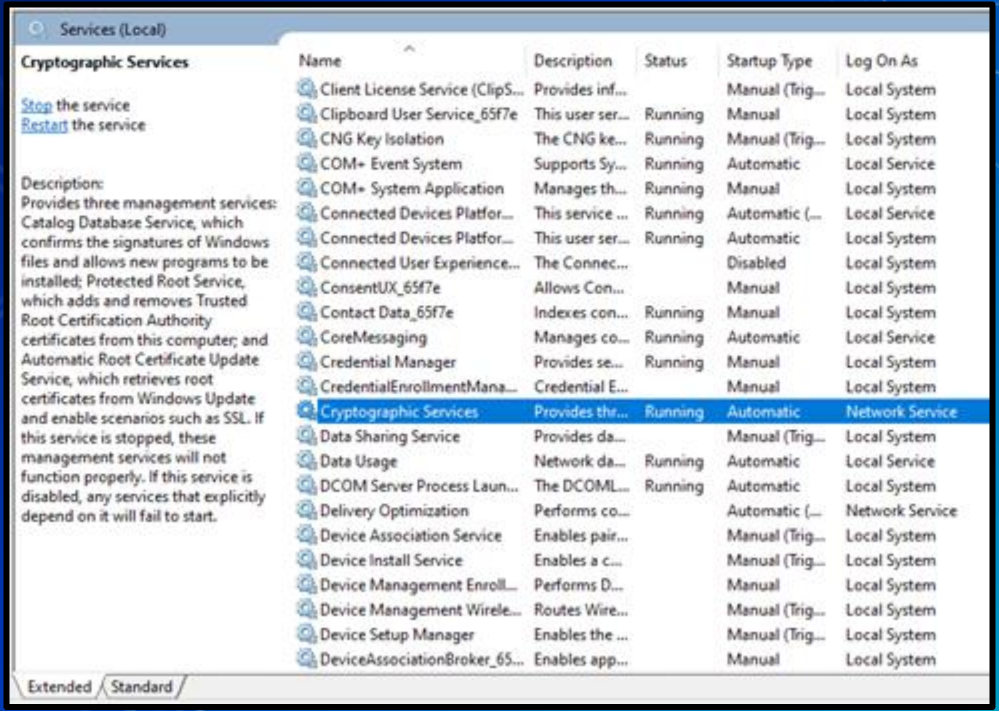
Services List



Select an item to view its description.

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

Services List



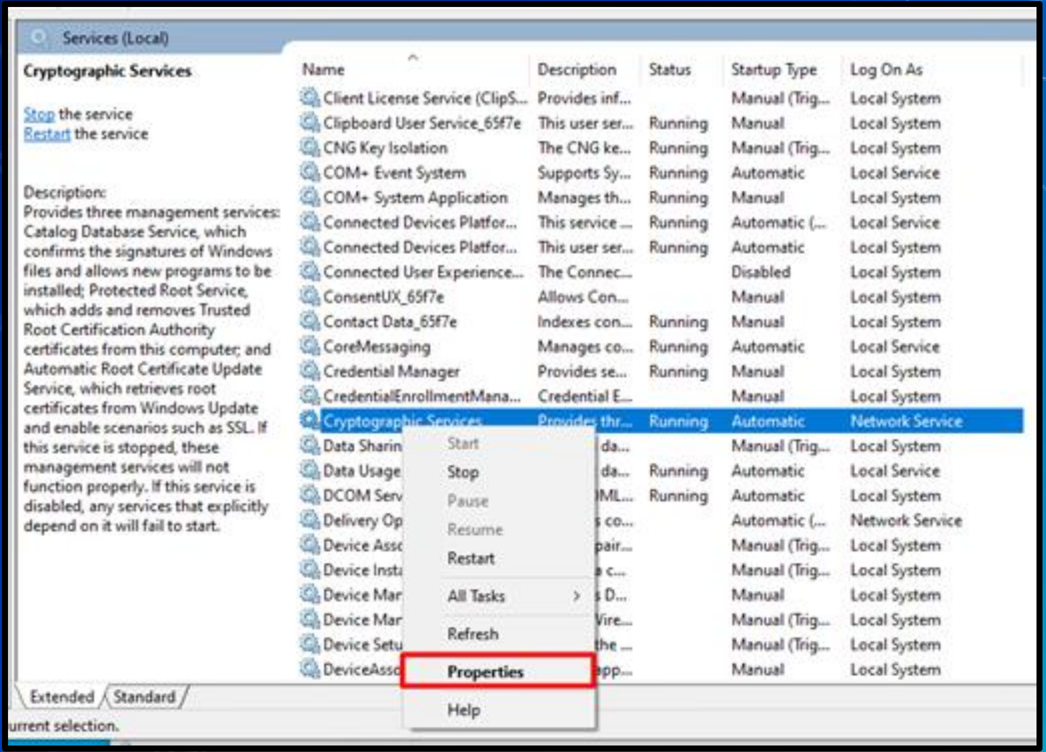
Cryptographic Services

Stop the service
Restart the service

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

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

Services List



Services (Local)

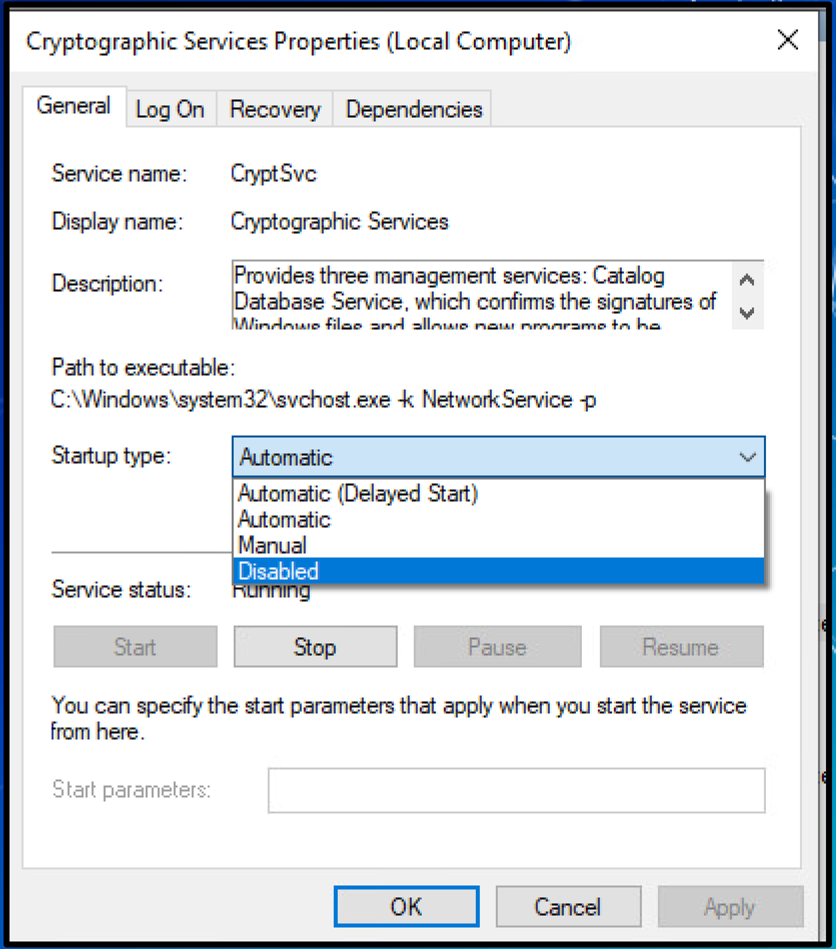
Cryptographic Services

Stop the service
Restart the service

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

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

Services List



Cryptographic Services Properties (Local Computer)

Service name: CryptSvc

Display name: Cryptographic Services

Description: Provides three management services: Catalog Database Service, which confirms the signatures of Windows files and allows new programs to be

Path to executable:
C:\Windows\system32\svchost.exe -k NetworkService -p

Startup type: Automatic

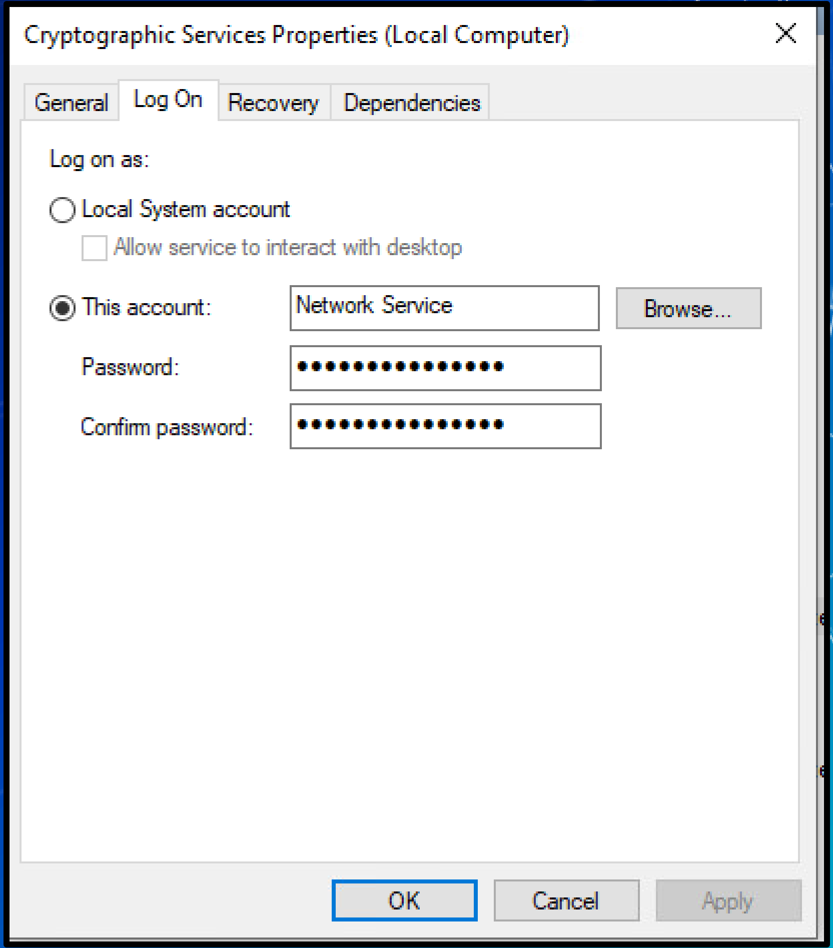
- Automatic (Delayed Start)
- Automatic
- Manual
- Disabled

Service status: Running

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

Start parameters:

Services List



Cryptographic Services Properties (Local Computer)

Log on as:

○ Local System account

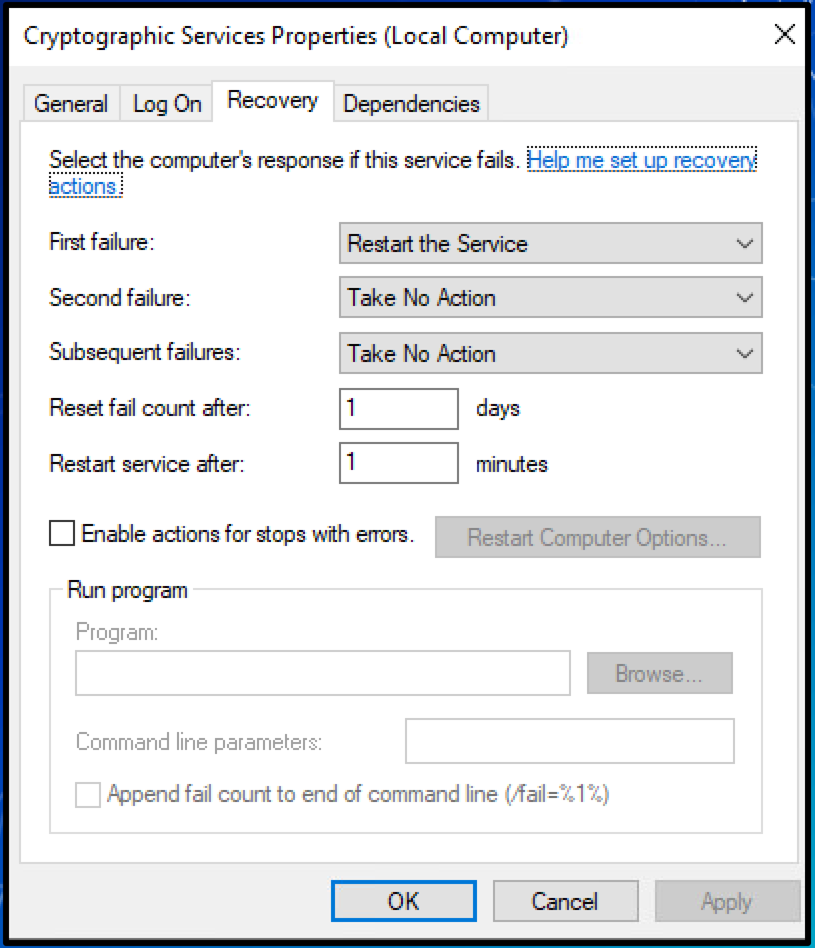
□ Allow service to interact with desktop

● This account: Network Service

Password: •••••••••••••••

Confirm password: •••••••••••••••

Services List



Cryptographic Services Properties (Local Computer)

Select the computer's response if this service fails. Help me set up recovery actions

First failure:	Restart the Service
Second failure:	Take No Action
Subsequent failures:	Take No Action
Reset fail count after:	1 days
Restart service after:	1 minutes

□ Enable actions for stops with errors.

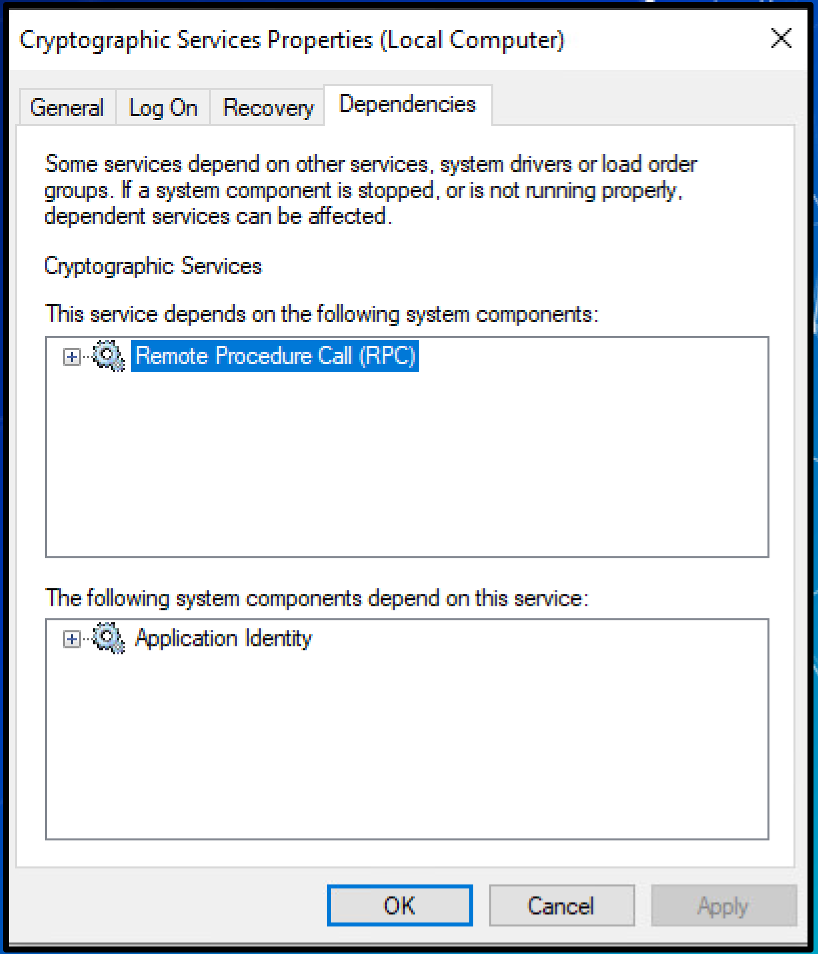
Run program

Program:

Command line parameters:

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

Services List



Cryptographic Services Properties (Local Computer)

Some services depend on other services, system drivers or load order groups. If a system component is stopped, or is not running properly, dependent services can be affected.

Cryptographic Services

This service depends on the following system components:

- Remote Procedure Call (RPC)

The following system components depend on this service:

- Application Identity

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?

IF YOU SEE SOMETHING,
SAY SOMETHING.
BE SUSPICIOUS OF ANYTHING NOT ON Google
Tell a cop, an MTA employee or call 1-888-NYC-SAFE.
SubTalk

NetDef

Hands on 3- Delete a Malicious Service

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

RESTART YOUR WINDOWS VM

Persistence

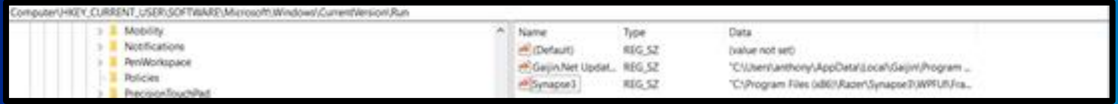
Persistence

- 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)

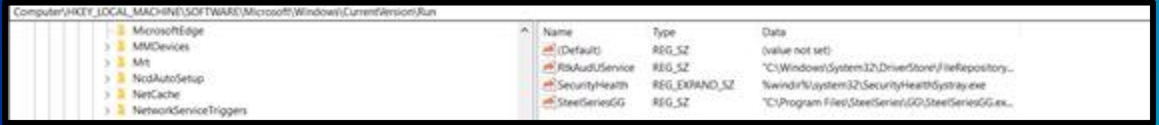
Registry Keys



Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

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

- 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`

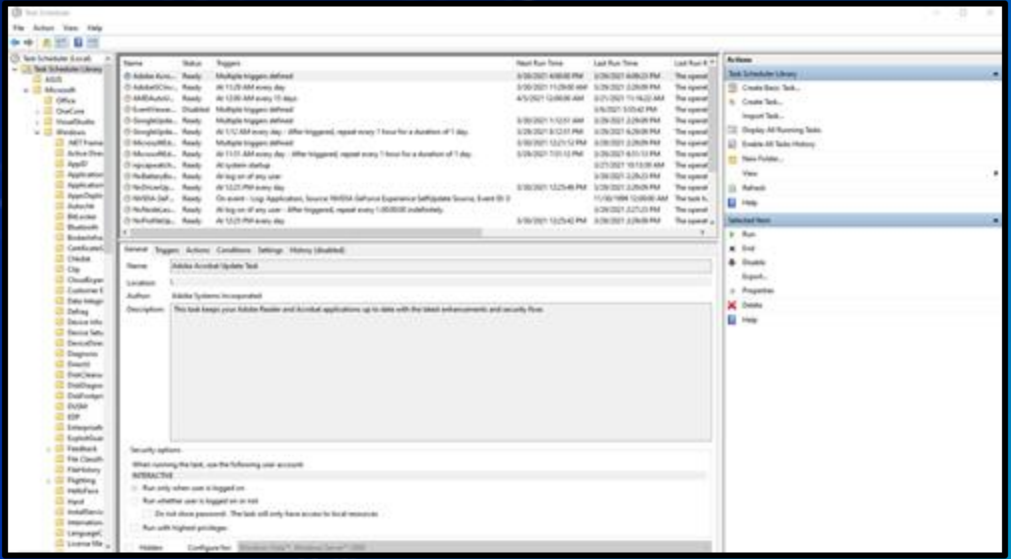


Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

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

Scheduled Tasks

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



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run R
Adobe Acro...	Ready	Multiple triggers defined	3/30/2021 4:00:00 PM	3/29/2021 4:09:23 PM	The operati
AdobeGCInv...	Ready	At 11:29 AM every day	3/30/2021 11:29:00 AM	3/29/2021 3:29:09 PM	The operati
AMDAutoU...	Ready	At 12:00 AM every 15 days	4/5/2021 12:00:00 AM	3/21/2021 11:16:22 AM	The operati
EventViewer...	Disabled	Multiple triggers defined		3/6/2021 3:03:42 PM	The operati
GoogleUpda...	Ready	Multiple triggers defined	3/30/2021 1:12:51 AM	3/29/2021 3:29:09 PM	The operati
GoogleUpda...	Ready	At 1:12 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	3/29/2021 8:12:51 PM	3/29/2021 6:29:08 PM	The operati
MicrosoftEd...	Ready	Multiple triggers defined	3/30/2021 12:21:12 PM	3/28/2021 3:29:09 PM	The operati
MicrosoftEd...	Ready	At 11:51 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	3/29/2021 7:51:12 PM	3/29/2021 6:51:13 PM	The operati
npcapwatch...	Ready	At system startup		3/21/2021 10:13:00 AM	The operati
NvBatteryBo...	Ready	At log on of any user		3/28/2021 3:28:23 PM	The operati
NvDriverUp...	Ready	At 12:25 PM every day	3/30/2021 12:25:48 PM	3/29/2021 3:29:09 PM	The operati
NVIDIA GeF...	Ready	On event - Log: Application, Source: NVIDIA GeForce Experience SelfUpdate Source, Event ID: 0		11/30/1999 12:00:00 AM	The task h...
NvNodeLau...	Ready	At log on of any user - After triggered, repeat every 1.00:00:00 indefinitely.		3/29/2021 3:27:23 PM	The operati
NvProfileUp...	Ready	At 12:25 PM every day	3/30/2021 12:25:42 PM	3/29/2021 3:29:09 PM	The operati

General | Triggers | Actions | Conditions | Settings | History (disabled)

Name: Adobe Acrobat Update Task

Location: \

Author: Adobe Systems Incorporated

Description: This task keeps your Adobe Reader and Acrobat applications up to date with the latest enhancements and security fixes.

Security options

When running the task, use the following user account:

INTERACTIVE

○ Run only when user is logged on

○ Run whether user is logged on or not

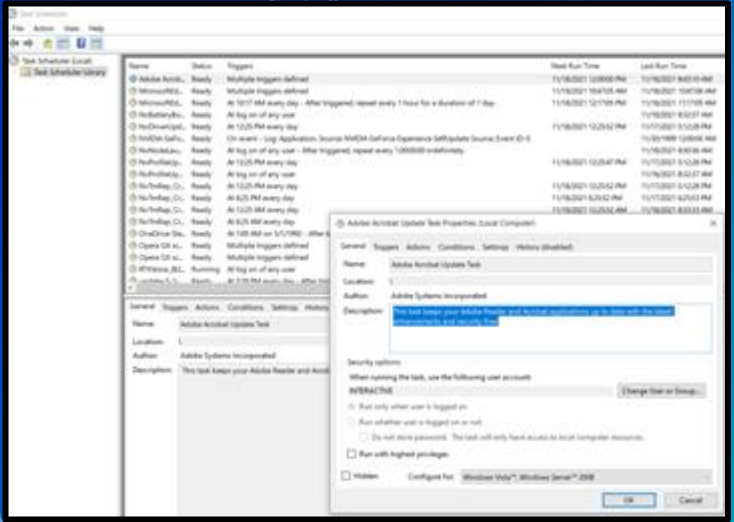
□ Do not store password. The task will only have access to local resources

□ Run with highest privileges

□ Hidden   Configure for: Windows Vista™, Windows Server™ 2008

Scheduled Tasks cont.

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



Name	Status	Triggers	Next Run Time	Last Run Time
Adobe Acrob...	Ready	Multiple triggers defined	[illegible]	[illegible]
MicrosoftEd...	Ready	Multiple triggers defined	[illegible]	[illegible]
MicrosoftEd...	Ready	At 10:17 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	[illegible]	[illegible]
NvBatteryBo...	Ready	At log on of any user		[illegible]
NvDriverUpd...	Ready	At 12:25 PM every day	[illegible]	[illegible]
NVIDIA GeFo...	Ready	On event - Log: Application, Source: NVIDIA GeForce Experience SelfUpdate Source, Event ID: 0		[illegible]
NvNodeLau...	Ready	At log on of any user - After triggered, repeat every 1.00:00:00 indefinitely.		[illegible]
NvProfileUp...	Ready	At 12:25 PM every day	[illegible]	[illegible]
NvProfileUp...	Ready	At log on of any user		[illegible]
NvTmRep_Cr...	Ready	At 12:25 PM every day	[illegible]	[illegible]
NvTmRep_Cr...	Ready	At 6:25 PM every day	[illegible]	[illegible]
NvTmRep_Cr...	Ready	At 12:25 AM every day	[illegible]	[illegible]
NvTmRep_Cr...	Ready	At 6:25 AM every day		
OneDrive Sta...	Ready	At 1:00 AM on 5/1/1992 - After tri...		
Opera GX sc...	Ready	Multiple triggers defined		
Opera GX sc...	Ready	Multiple triggers defined		
RTKVoice_BL...	Running	At log on of any user		
[illegible]	Ready	At 2:15 PM every day - After tri...		

Name: Adobe Acrobat Update Task

Location: \

Author: Adobe Systems Incorporated

Description: This task keeps your Adobe Reader and Acrobat...

Adobe Acrobat Update Task Properties (Local Computer)

General Triggers Actions Conditions Settings History (disabled)

Name: Adobe Acrobat Update Task

Location: \

Author: Adobe Systems Incorporated

Description: This task keeps your Adobe Reader and Acrobat applications up to date with the latest enhancements and security fixes

Security options

When running the task, use the following user account:

INTERACTIVE

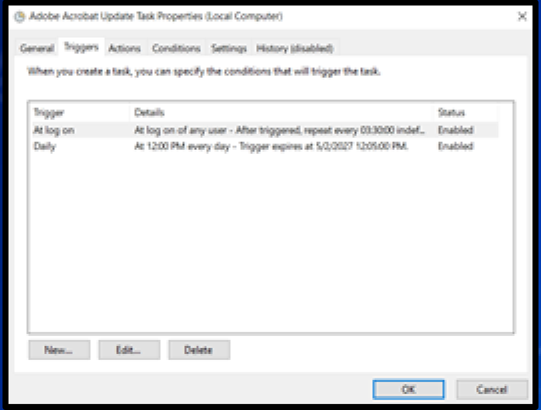
● Run only when user is logged on

○ Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

□ Run with highest privileges

□ Hidden Configure for: Windows Vista™, Windows Server™ 2008



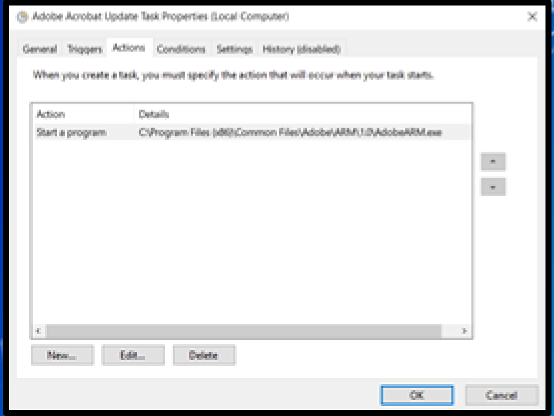
Adobe Acrobat Update Task Properties (Local Computer)

General Triggers Actions Conditions Settings History (disabled)

When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status
At log on	At log on of any user - After triggered, repeat every 03:30:00 indef...	Enabled
Daily	At 12:00 PM every day - Trigger expires at 5/2/2027 12:05:00 PM.	Enabled

New...
Edit...
Delete
OK
Cancel



Adobe Acrobat Update Task Properties (Local Computer)

General Triggers Actions Conditions Settings History (disabled)

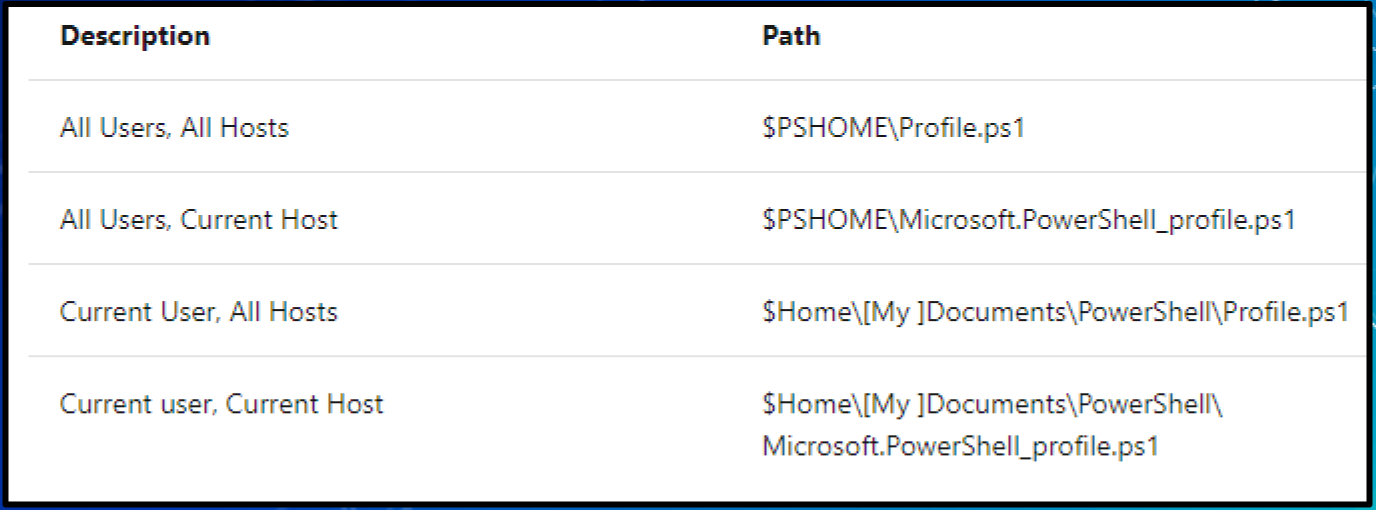
When you create a task, you must specify the action that will occur when your task starts.

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

New...
Edit...
Delete
OK
Cancel

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

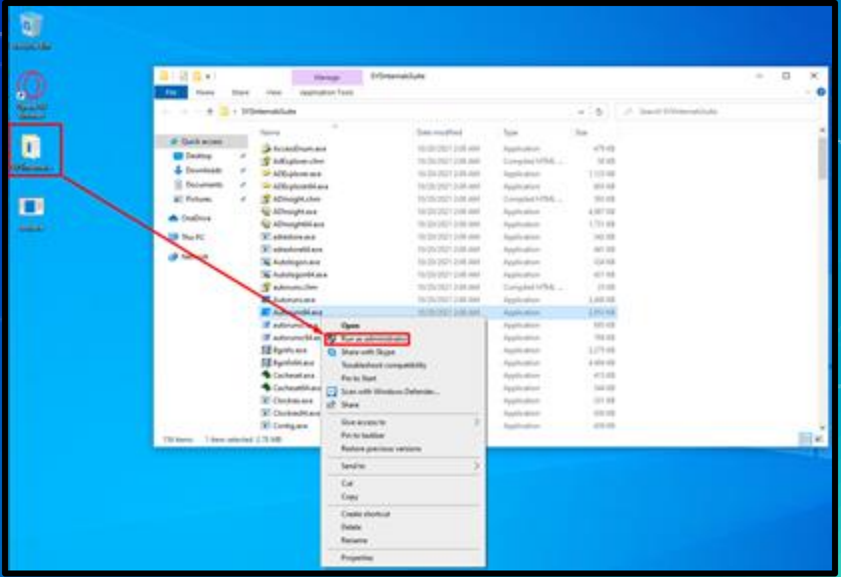
- Group policies can soften the security posture of a device
  - Disable anti-virus
  - Turn off or flood logs
  - Disable firewalls
  - And more!
- Group Policies can be used to establish registry based persistence
- Malicious group policies are very dangerous

Hands on 4 – Combatting Persistence

- Check services again
  - What do you notice?

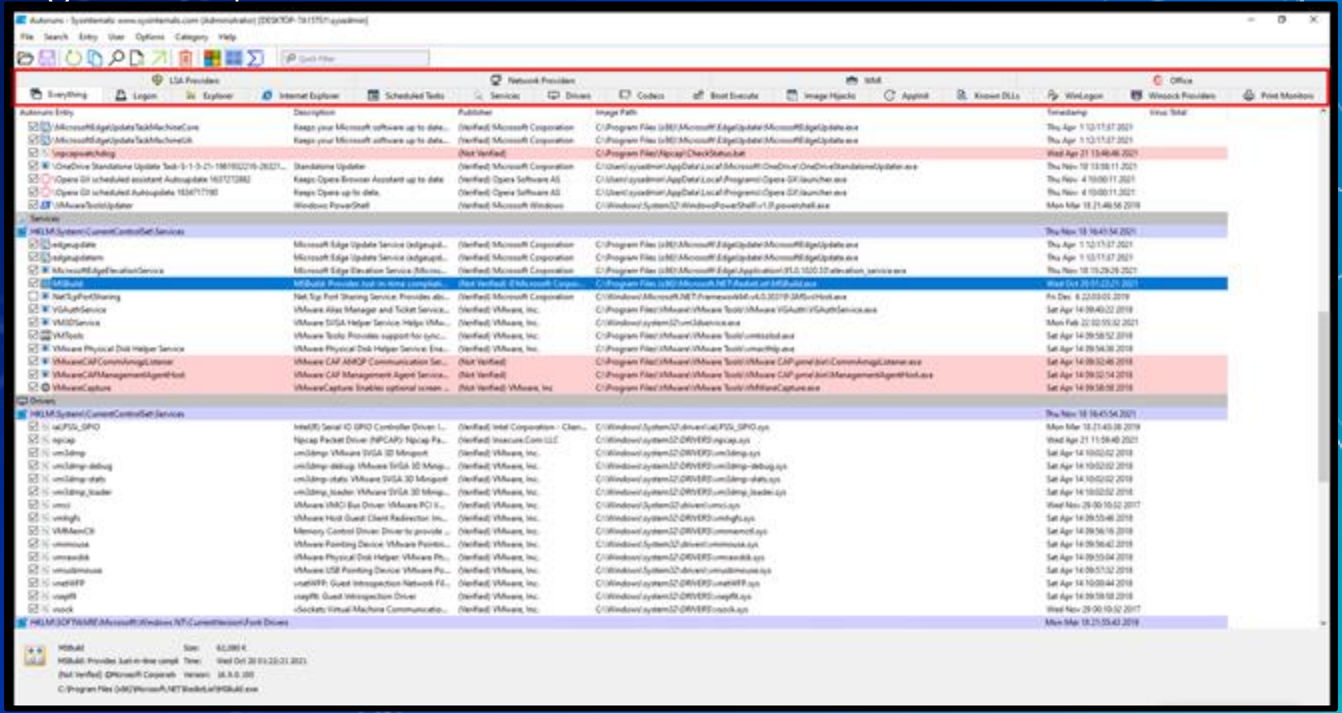
Hands on 4 – Combatting Persistence

- 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

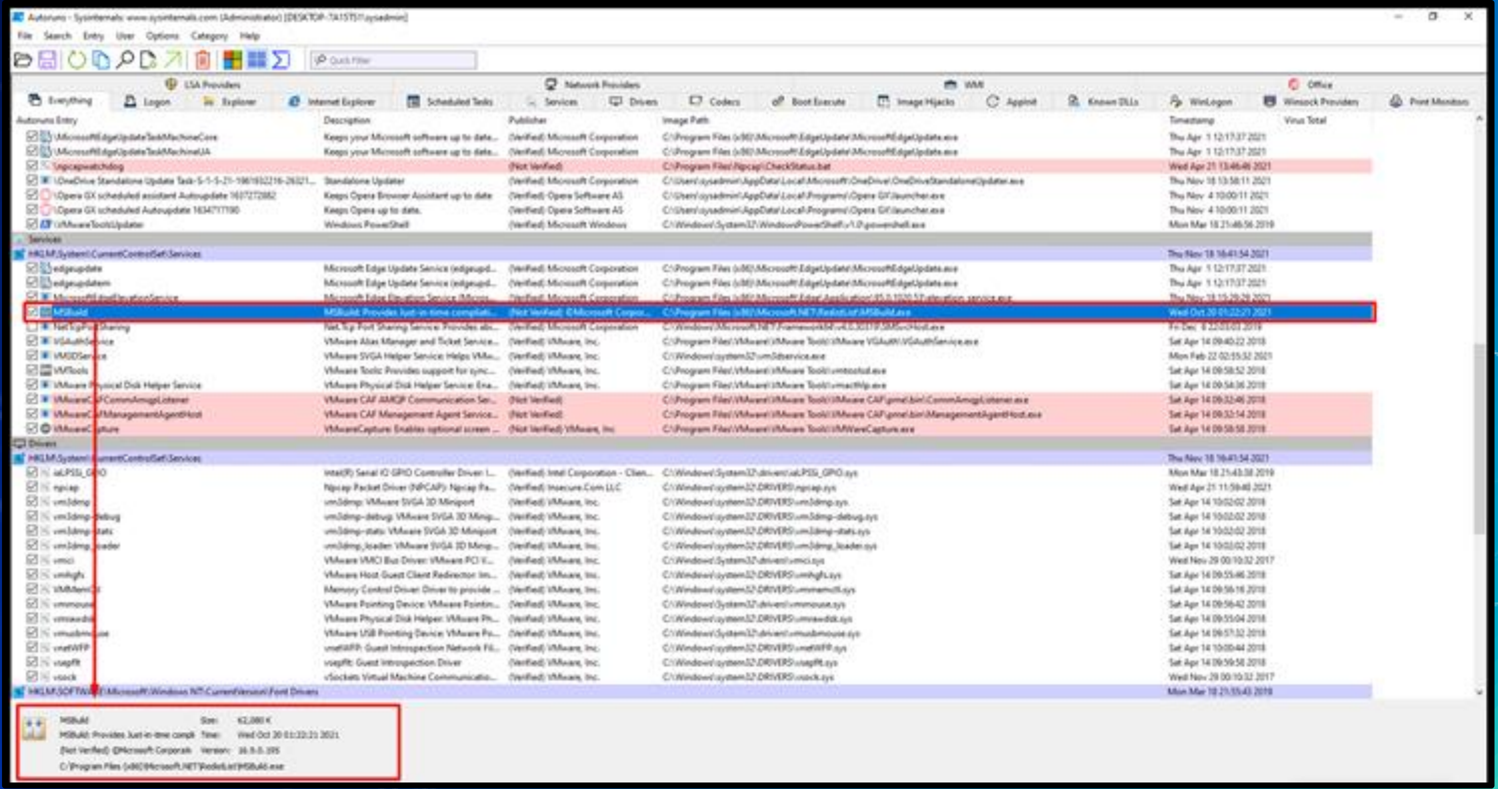


Hands on 4 – Combatting Persistence

- Categories of persistence



Hands on 4 – Combatting Persistence



Autoruns 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...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021	
☑ \npcapwatchdog		(Not Verified)	C:\Program Files\Npcap\CheckStatus.bat	Wed Apr 21 13:46:46 2021	
☑ \OneDrive Standalone Update Task-S-1-5-21-1961932216-26321...	Standalone Updater	(Verified) Microsoft Corporation	C:\Users\sysadmin\AppData\Local\Microsoft\OneDrive\OneDriveStandaloneUpdater.exe	Thu Nov 18 13:58:11 2021	
☑ \Opera GX scheduled assistant Autoupdate 1637272882	Keeps Opera Browser Assistant up to date	(Verified) Opera Software AS	C:\Users\sysadmin\AppData\Local\Programs\Opera GX\launcher.exe	Thu Nov 4 10:00:11 2021	
☑ \Opera GX scheduled Autoupdate 1634717190	Keeps Opera up to date.	(Verified) Opera Software AS	C:\Users\sysadmin\AppData\Local\Programs\Opera GX\launcher.exe	Thu Nov 4 10:00:11 2021	
☑ \VMwareToolsUpdater	Windows PowerShell	(Verified) Microsoft Windows	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Mon Mar 18 21:46:56 2019	
Services					
HKLM\System\CurrentControlSet\Services				Thu Nov 18 16:41:54 2021	
☑ edgeupdate	Microsoft Edge Update Service (edgeupd...	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021	
☑ edgeupdatem	Microsoft Edge Update Service (edgeupd...	(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\95.0.1020.53\elevation_service.exe	Thu Nov 18 13:29:28 2021	
☑ MSBuild	MSBuild: Provides Just-in-time compilati...	(Not Verified) ©Microsoft Corpor...	C:\Program Files (x86)\Microsoft.NET\RedistList\MSBuild.exe	Wed Oct 20 01:22:21 2021	
□ NetTcpPortSharing	Net.Tcp Port Sharing Service: Provides abi...	(Verified) Microsoft Corporation	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.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 VGAuth\VGAuthService.exe	Sat Apr 14 09:40:22 2018	
☑ VM3DService	VMware SVGA Helper Service: Helps VMw...	(Verified) VMware, Inc.	C:\Windows\system32\vm3dservice.exe	Mon Feb 22 02:55:32 2021	
☑ VMTools	VMware Tools: Provides support for sync...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Sat Apr 14 09:58:52 2018	
☑ VMware Physical Disk Helper Service	VMware Physical Disk Helper Service: Ena...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmacthlp.exe	Sat Apr 14 09:54:36 2018	
☑ VMwareCAFCommAmqpListener	VMware CAF AMQP Communication Ser...	(Not Verified)	C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin\CommAmqpListener.exe	Sat Apr 14 09:32:46 2018	
☑ VMwareCAFManagementAgentHost	VMware CAF Management Agent Service...	(Not Verified)	C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin\ManagementAgentHost.exe	Sat Apr 14 09:32:14 2018	
☑ 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\System\CurrentControlSet\Services				Thu Nov 18 16:41:54 2021	
☑ iaLPSS_GPIO	Intel(R) Serial IO GPIO Controller Driver I...	(Verified) Intel Corporation - Clien...	C:\Windows\System32\drivers\iaLPSS_GPIO.sys	Mon Mar 18 21:43:38 2019	
☑ npcap	Npcap Packet Driver (NPCAP): Npcap Pa...	(Verified) Insecure.Com LLC	C:\Windows\system32\DRIVERS\npcap.sys	Wed Apr 21 11:59:40 2021	
☑ vm3dmp	vm3dmp: VMware SVGA 3D Miniport	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vm3dmp.sys	Sat Apr 14 10:02:02 2018	
☑ 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-stats	vm3dmp-stats: VMware SVGA 3D Miniport	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vm3dmp-stats.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	Wed Nov 29 00:10:32 2017	
☑ vmhgfs	VMware Host Guest Client Redirector: Im...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmhgfs.sys	Sat Apr 14 09:55:46 2018	
☑ VMMemCtl	Memory Control Driver: Driver to provide ...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmmemctl.sys	Sat Apr 14 09:56:16 2018	
☑ vmmouse	VMware Pointing Device: VMware Pointin...	(Verified) VMware, Inc.	C:\Windows\System32\drivers\vmmouse.sys	Sat Apr 14 09:56:42 2018	
☑ vmrawdsk	VMware Physical Disk Helper: VMware Ph...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmrawdsk.sys	Sat Apr 14 09:55:04 2018	
☑ vmusbmouse	VMware USB Pointing Device: VMware Po...	(Verified) VMware, Inc.	C:\Windows\System32\drivers\vmusbmouse.sys	Sat Apr 14 09:57:32 2018	
☑ vnetWFP	vnetWFP: Guest Introspection Network Fil...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vnetWFP.sys	Sat Apr 14 10:00:44 2018	
☑ vsepflt	vsepflt: Guest Introspection Driver	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vsepflt.sys	Sat Apr 14 09:59:58 2018	
☑ vsock	vSockets Virtual Machine Communicatio...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vsock.sys	Wed Nov 29 00:10:32 2017	
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Drivers				Mon Mar 18 21:55:43 2019	

MSBuild Size: 62,080 K
MSBuild: Provides Just-in-time compil Time: Wed Oct 20 01:22:21 2021
(Not Verified) ©Microsoft Corporati Version: 16.9.0.195
C:\Program Files (x86)\Microsoft.NET\RedistList\MSBuild.exe

Hands on 4 – Combatting Persistence

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

NetDef

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?