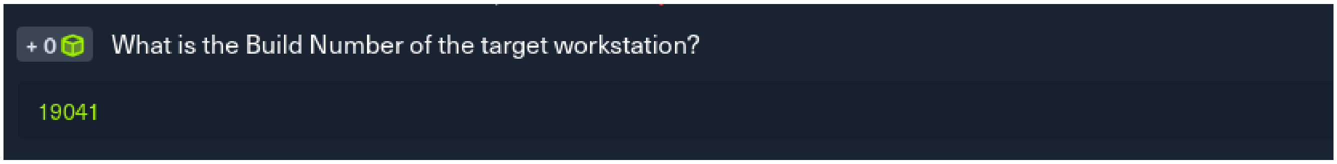
WINDOWS FUNDAMENTALS

INTRODUCTION

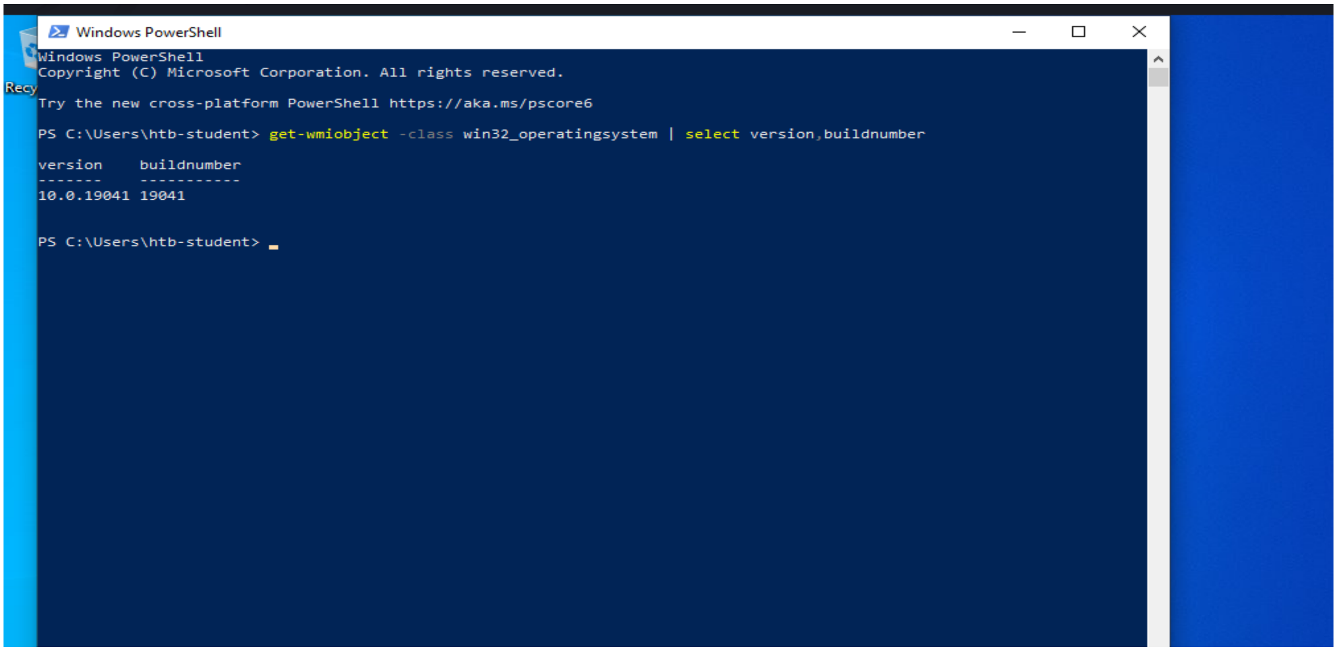
As a penetration tester, it is important to have knowledge of a wide variety of technologies, especially the linux and windows operating systems.

Q & A

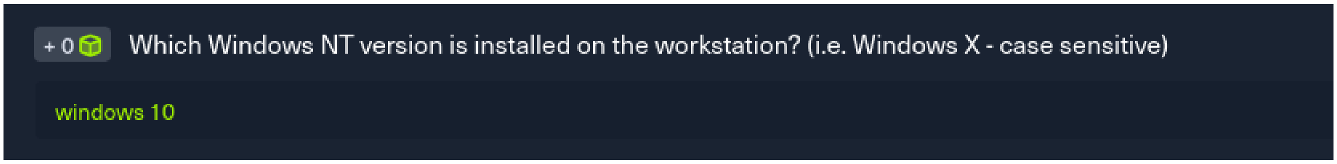


What is the Build Number of the target workstation?

19041

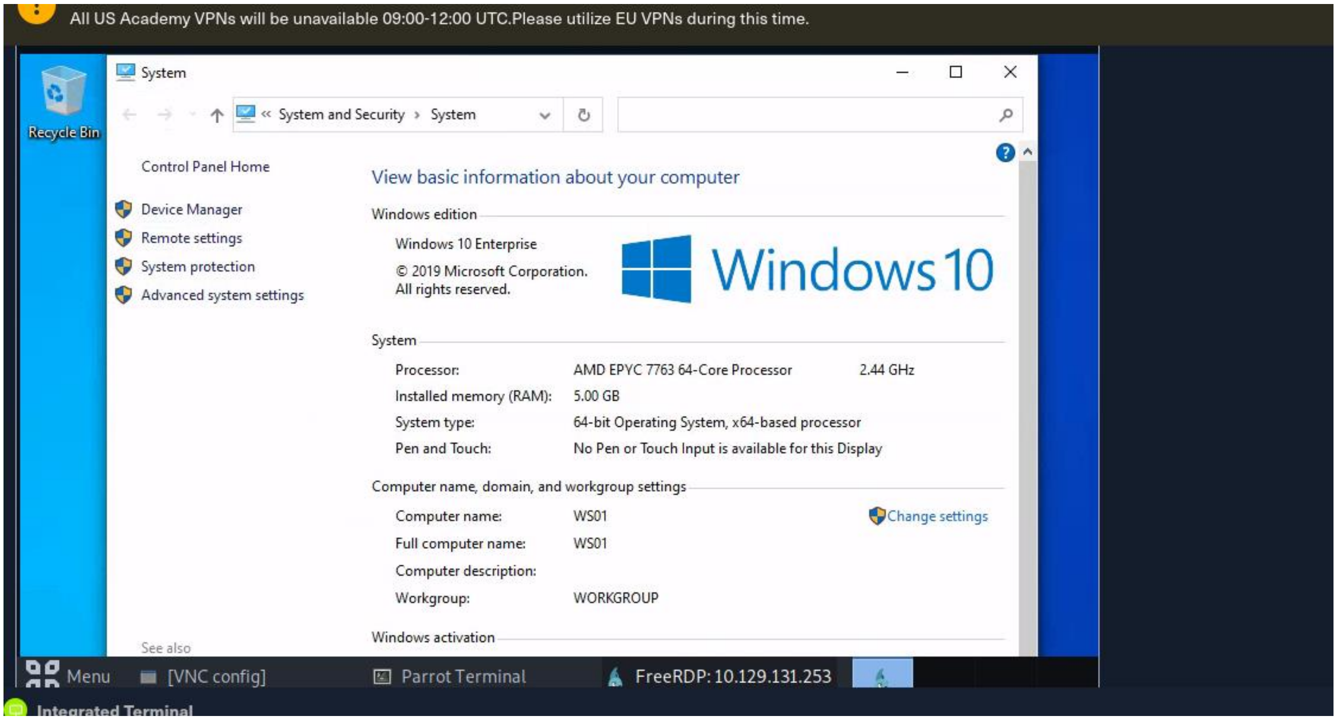


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Users\htb-student> get-wmiobject -class win32_operatingsystem | select version,buildnumber

version    buildnumber
-------    -----------
10.0.19041 19041


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



Which Windows NT version is installed on the workstation? (i.e. Windows X - case sensitive)

windows 10



All US Academy VPNs will be unavailable 09:00-12:00 UTC.Please utilize EU VPNs during this time.

System

View basic information about your computer

Windows edition

Windows 10 Enterprise

© 2019 Microsoft Corporation. All rights reserved.

System

Processor: AMD EPYC 7763 64-Core Processor 2.44 GHz

Installed memory (RAM): 5.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

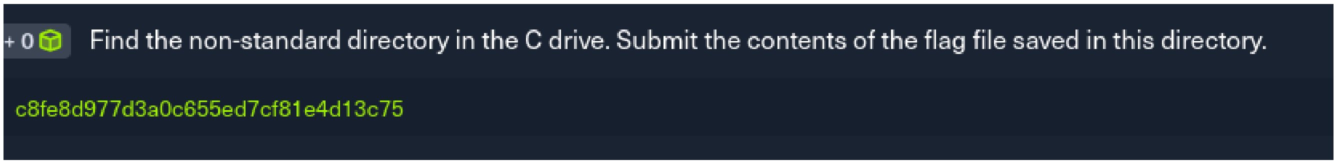
Computer name: WS01

Full computer name: WS01

Computer description:

Workgroup: WORKGROUP

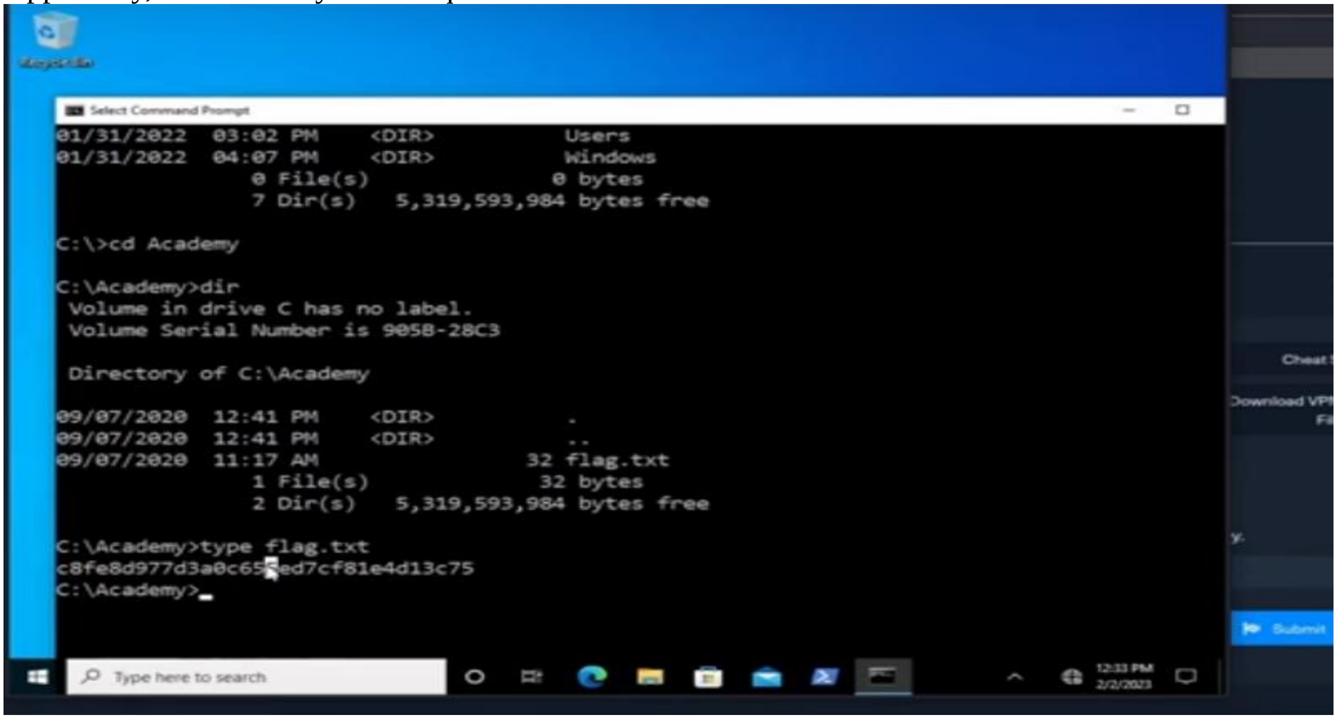
Windows activation



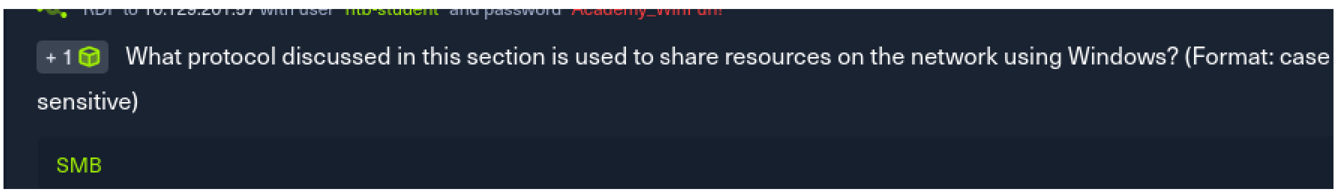
+ 0 Find the non-standard directory in the C drive. Submit the contents of the flag file saved in this directory.

c8fe8d977d3a0c655ed7cf81e4d13c75

Apparently, this directory was unique from other directories.



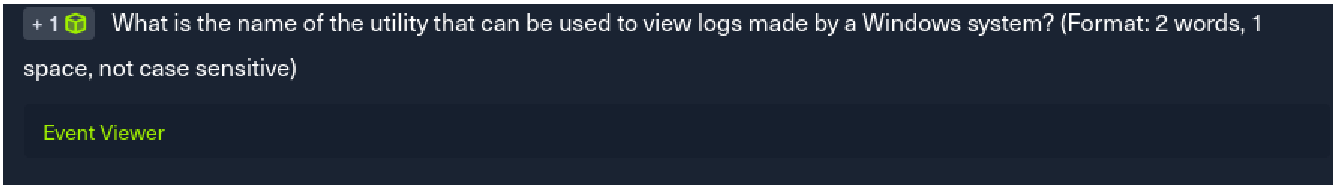
```
01/31/2022  03:02 PM    <DIR>          Users
01/31/2022  04:07 PM    <DIR>          Windows
               0 File(s)              0 bytes
               7 Dir(s)   5,319,593,984 bytes free

C:\>cd Academy

C:\Academy>dir
 Volume in drive C has no label.
 Volume Serial Number is 9058-28C3

 Directory of C:\Academy

09/07/2020  12:41 PM    <DIR>          .
09/07/2020  12:41 PM    <DIR>          ..
09/07/2020  11:17 AM                32 flag.txt
               1 File(s)             32 bytes
               2 Dir(s)   5,319,593,984 bytes free

C:\Academy>type flag.txt
c8fe8d977d3a0c655ed7cf81e4d13c75
C:\Academy>_
```



RDP to 10.129.201.57 with user "htb-student" and password "Academy_WinFun!"

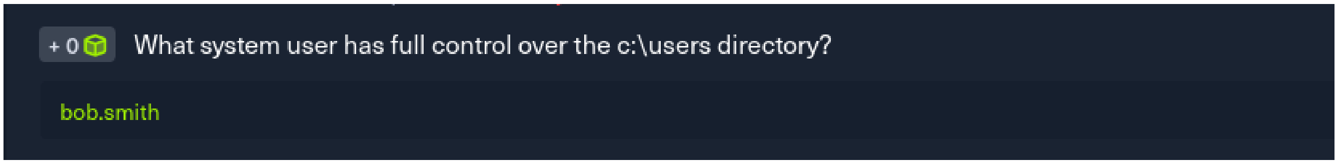
+ 1 What protocol discussed in this section is used to share resources on the network using Windows? (Format: case sensitive)

SMB



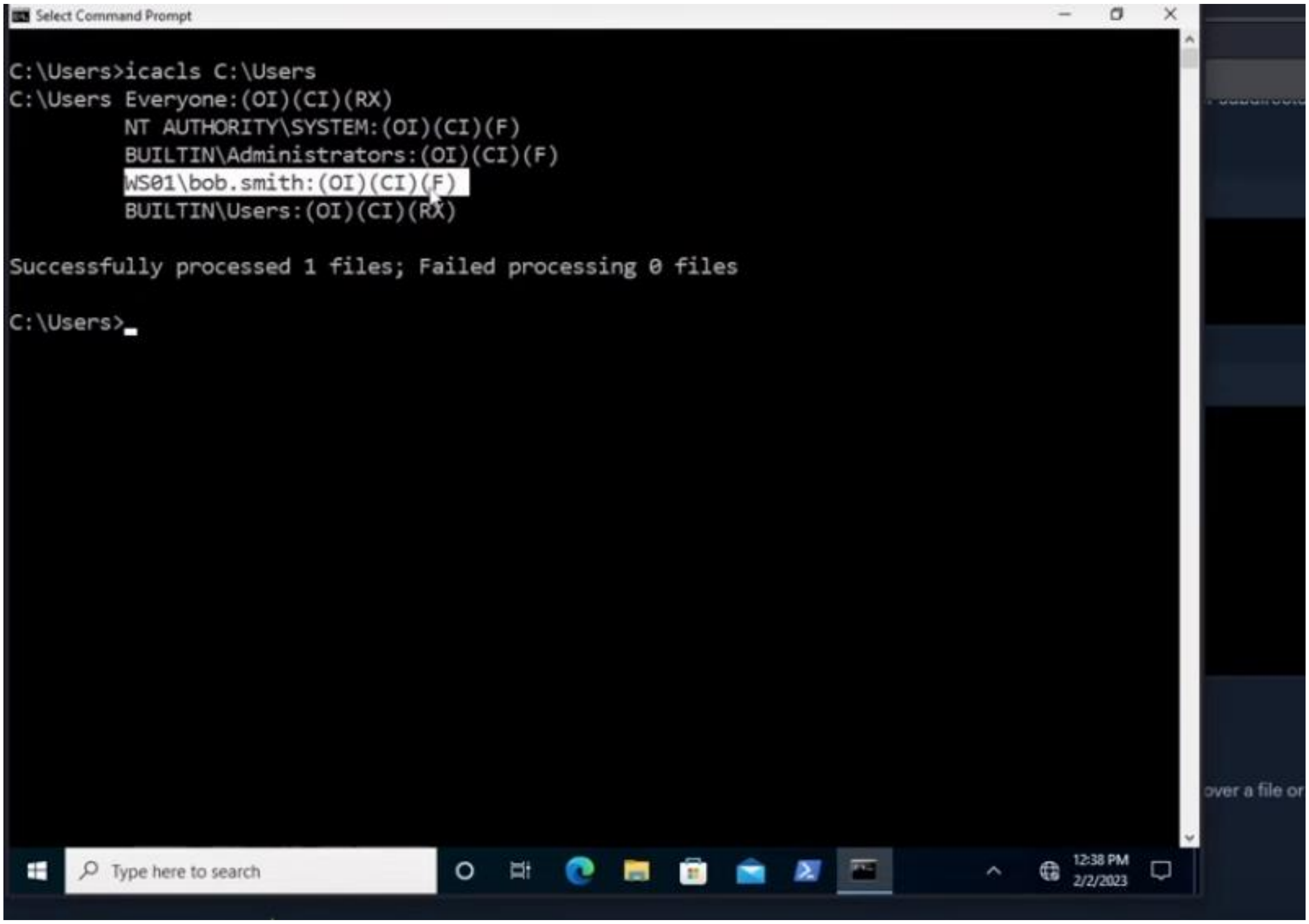
+ 1 What is the name of the utility that can be used to view logs made by a Windows system? (Format: 2 words, 1 space, not case sensitive)

Event Viewer

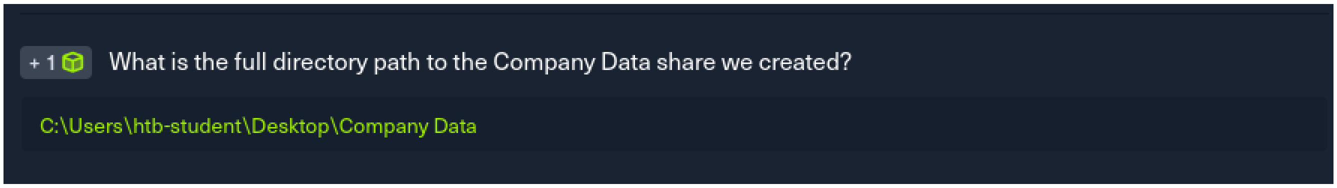


+ 0 What system user has full control over the c:\users directory?

bob.smith

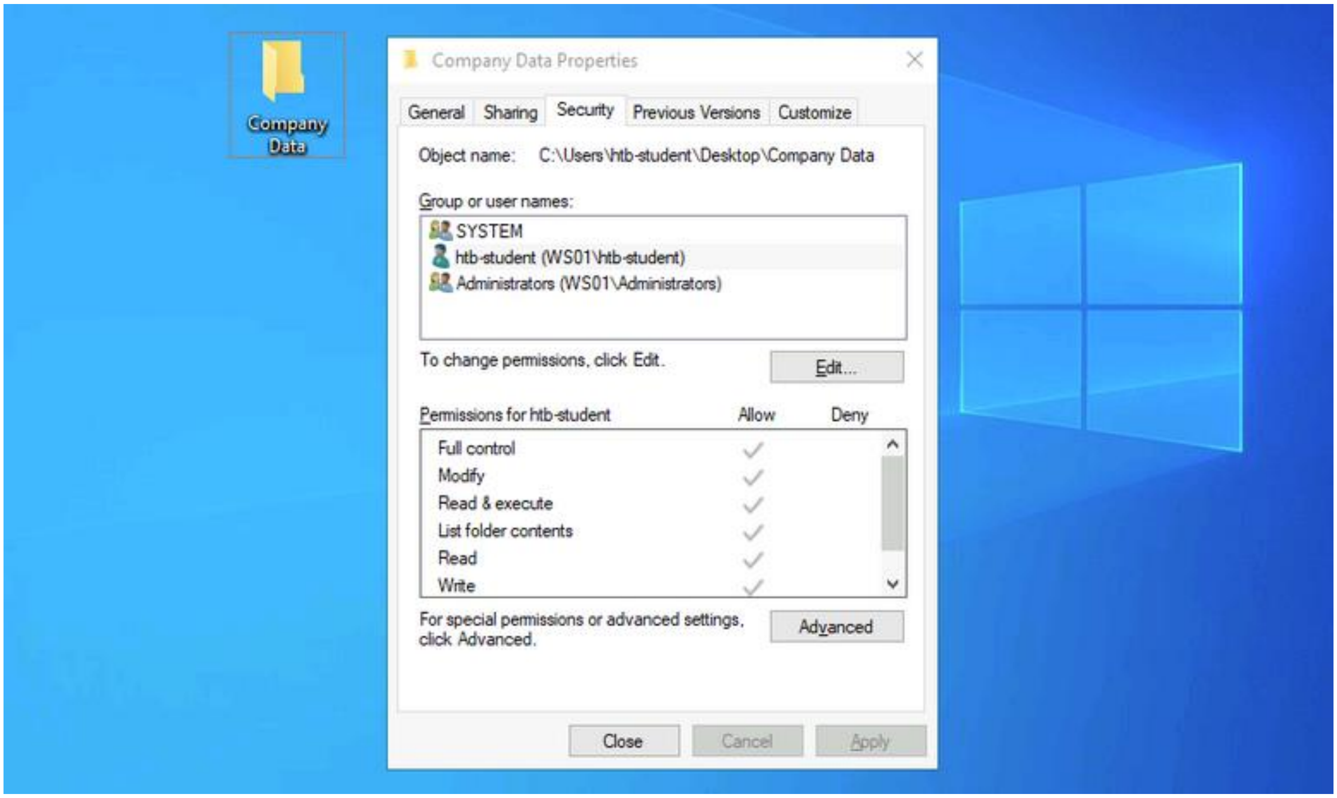


```
C:\Users>icacls C:\Users
C:\Users Everyone:(OI)(CI)(RX)
         NT AUTHORITY\SYSTEM:(OI)(CI)(F)
         BUILTIN\Administrators:(OI)(CI)(F)
         WS01\bob.smith:(OI)(CI)(F)
         BUILTIN\Users:(OI)(CI)(RX)

Successfully processed 1 files; Failed processing 0 files

C:\Users>_
```



+1 What is the full directory path to the Company Data share we created?

C:\Users\htb-student\Desktop\Company Data



Object name: C:\Users\htb-student\Desktop\Company Data

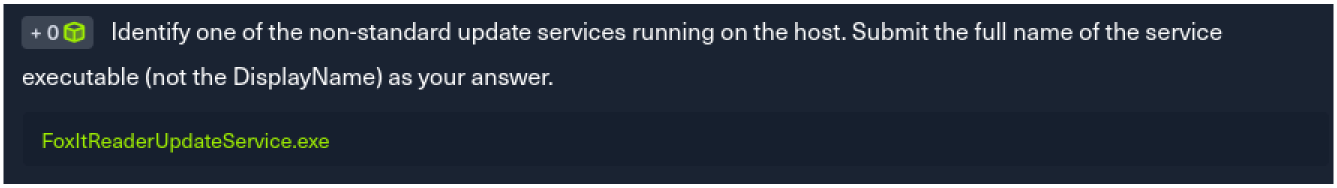
Group or user names:

- SYSTEM
- htb-student (WS01\htb-student)
- Administrators (WS01\Administrators)

To change permissions, click Edit.

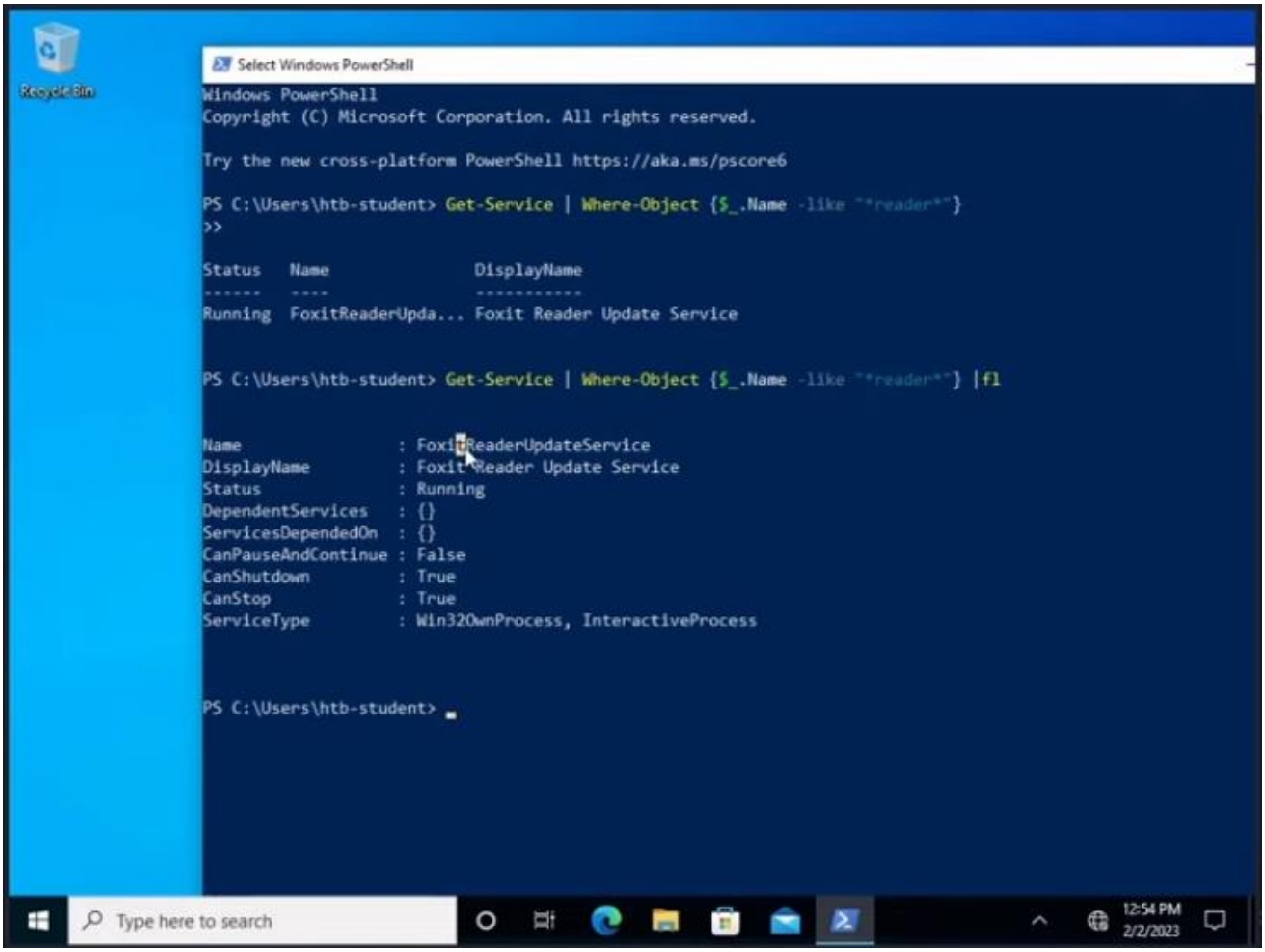
Permissions for htb-student	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

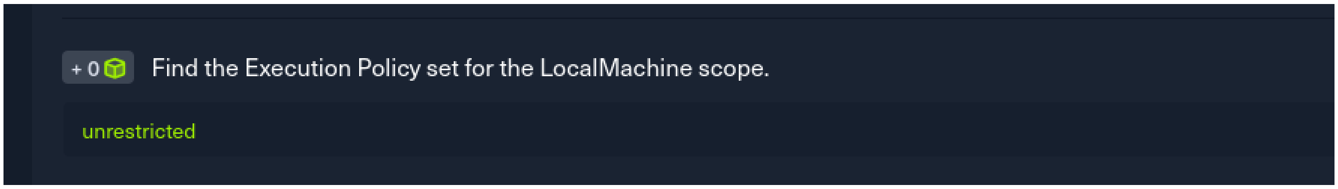


+0 Identify one of the non-standard update services running on the host. Submit the full name of the service executable (not the DisplayName) as your answer.

FoxItReaderUpdateService.exe

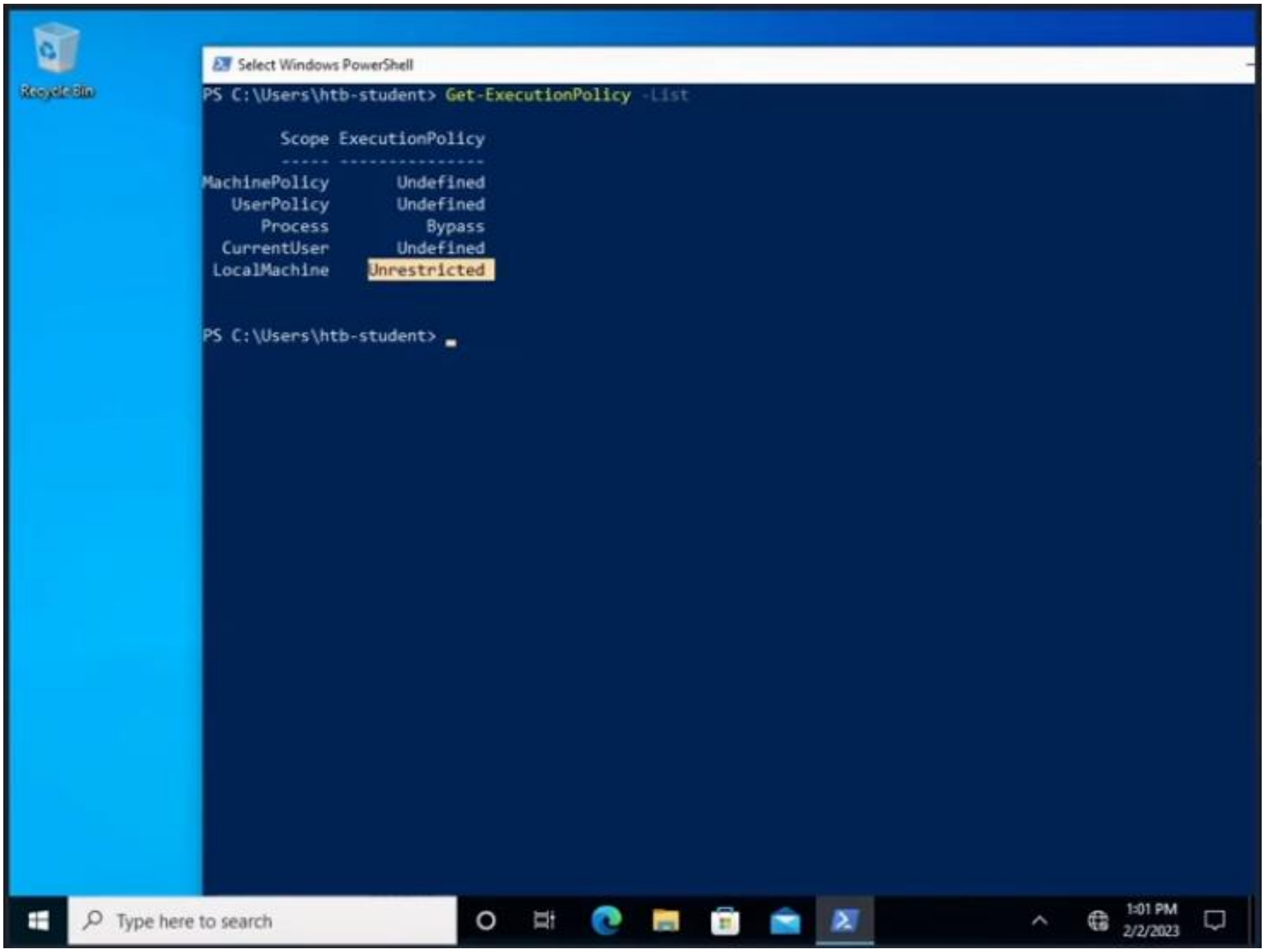


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Users\htb-student> Get-Service | Where-Object {$_.Name -like "*reader*"}
>>

Status   Name               DisplayName
------   ----               -----------
Running  FoxitReaderUpda... Foxit Reader Update Service


PS C:\Users\htb-student> Get-Service | Where-Object {$_.Name -like "*reader*"} |fl


Name                : FoxitReaderUpdateService
DisplayName         : Foxit Reader Update Service
Status              : Running
DependentServices   : {}
ServicesDependedOn  : {}
CanPauseAndContinue : False
CanShutdown         : True
CanStop             : True
ServiceType         : Win32OwnProcess, InteractiveProcess



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

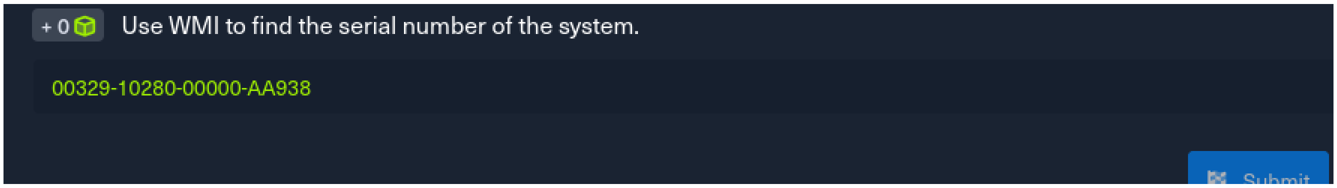


+ 0 Find the Execution Policy set for the LocalMachine scope.

unrestricted

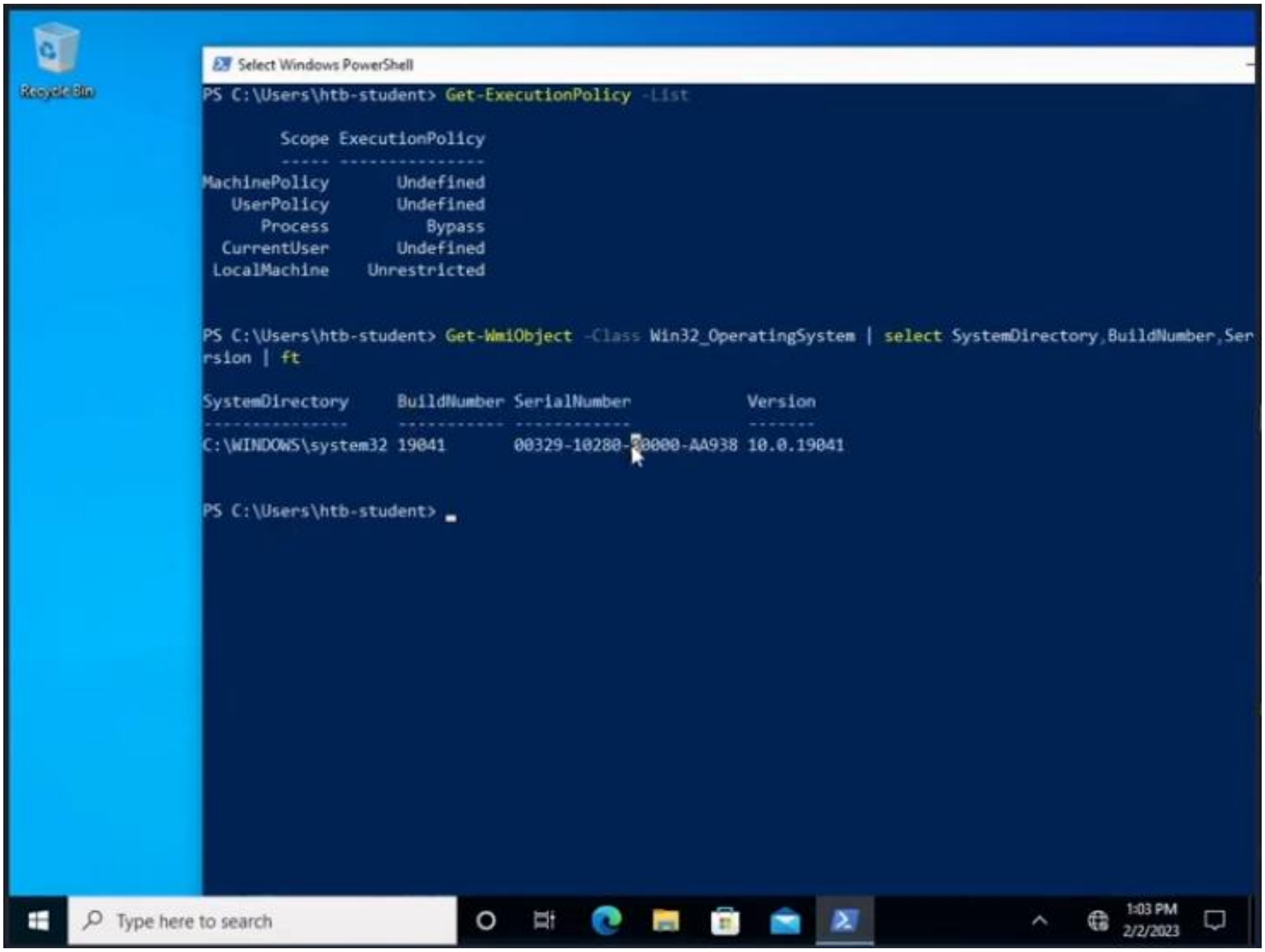


```
PS C:\Users\htb-student> Get-ExecutionPolicy -List

        Scope ExecutionPolicy
        ----- ---------------
MachinePolicy       Undefined
   UserPolicy       Undefined
      Process          Bypass
  CurrentUser       Undefined
 LocalMachine    Unrestricted


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

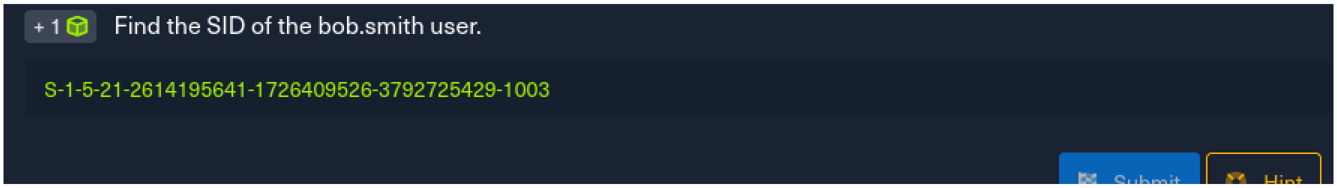


Use WMI to find the serial number of the system.

00329-10280-00000-AA938

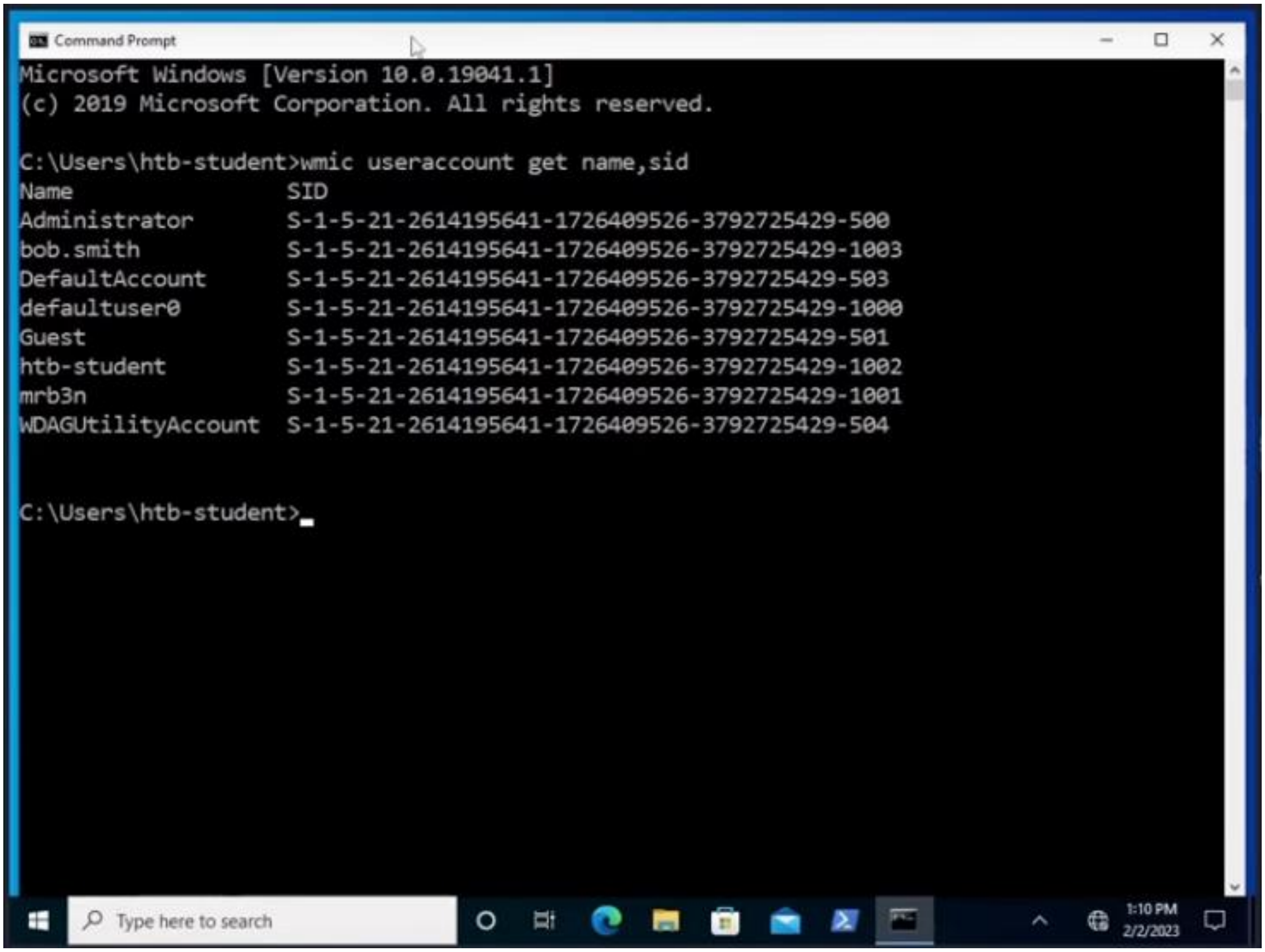


```
PS C:\Users\htb-student> Get-ExecutionPolicy -List

        Scope ExecutionPolicy
        ----- ---------------
MachinePolicy       Undefined
   UserPolicy       Undefined
      Process          Bypass
  CurrentUser       Undefined
 LocalMachine    Unrestricted


PS C:\Users\htb-student> Get-WmiObject -Class Win32_OperatingSystem | select SystemDirectory,BuildNumber,Ser
rsion | ft

SystemDirectory     BuildNumber SerialNumber            Version
---------------     ----------- ------------            -------
C:\WINDOWS\system32 19041       00329-10280-00000-AA938 10.0.19041


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

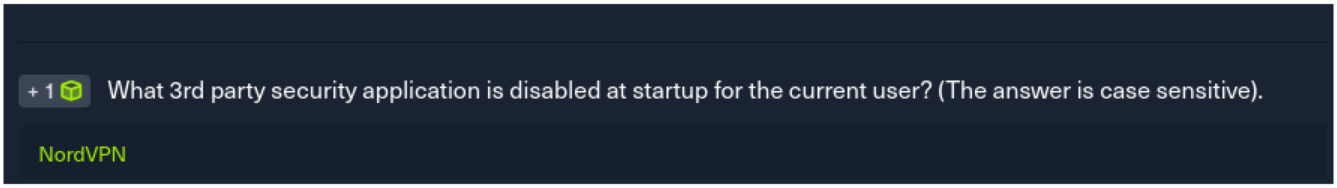


Find the SID of the bob.smith user.

S-1-5-21-2614195641-1726409526-3792725429-1003

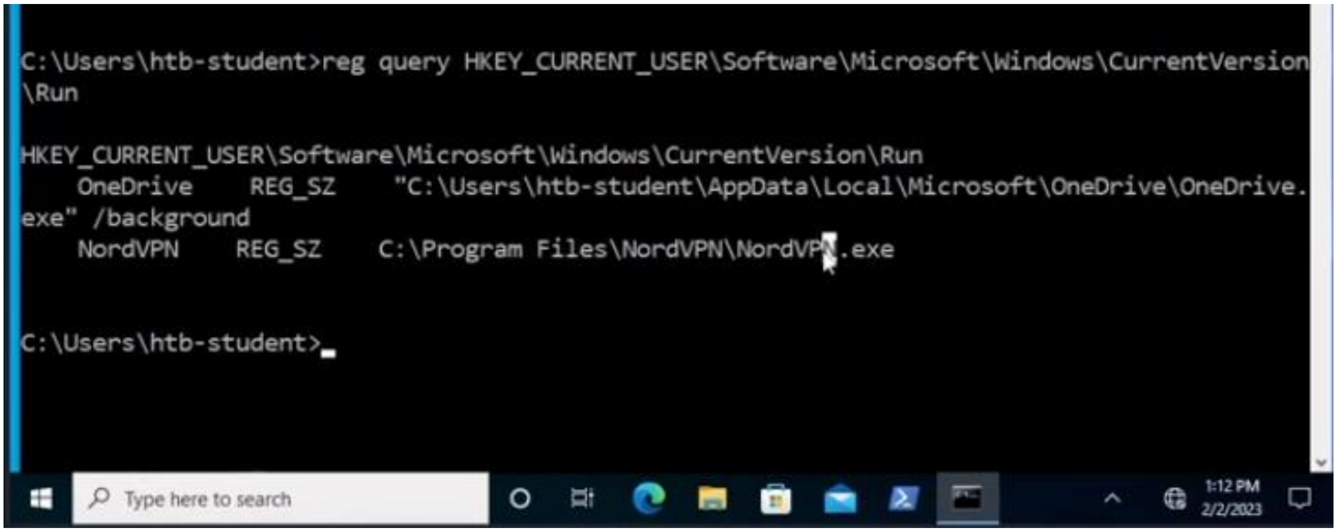


```
Microsoft Windows [Version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\htb-student>wmic useraccount get name,sid
Name                SID
Administrator       S-1-5-21-2614195641-1726409526-3792725429-500
bob.smith           S-1-5-21-2614195641-1726409526-3792725429-1003
DefaultAccount      S-1-5-21-2614195641-1726409526-3792725429-503
defaultuser0        S-1-5-21-2614195641-1726409526-3792725429-1000
Guest               S-1-5-21-2614195641-1726409526-3792725429-501
htb-student         S-1-5-21-2614195641-1726409526-3792725429-1002
mrb3n               S-1-5-21-2614195641-1726409526-3792725429-1001
WDAGUtilityAccount  S-1-5-21-2614195641-1726409526-3792725429-504


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

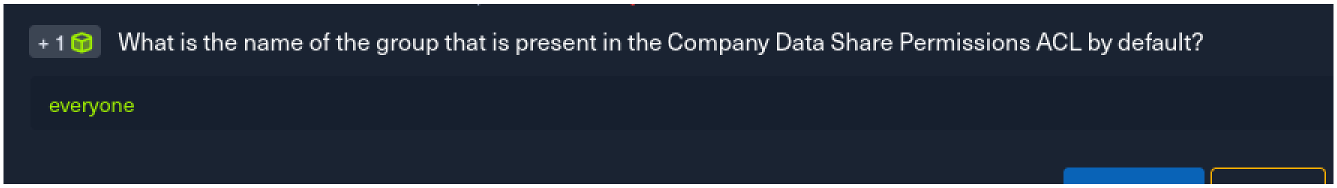


+ 1 What 3rd party security application is disabled at startup for the current user? (The answer is case sensitive).

NordVPN

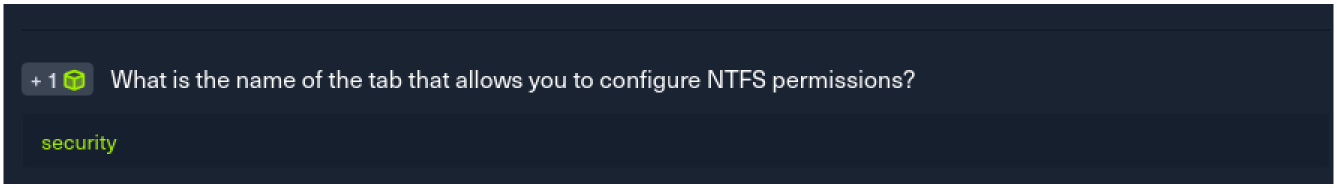


```
C:\Users\htb-student>reg query HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
    OneDrive    REG_SZ    "C:\Users\htb-student\AppData\Local\Microsoft\OneDrive\OneDrive.
exe" /background
    NordVPN    REG_SZ    C:\Program Files\NordVPN\NordVPN.exe


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



What is the name of the group that is present in the Company Data Share Permissions ACL by default?

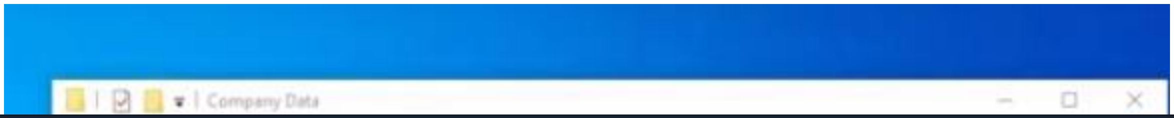
everyone

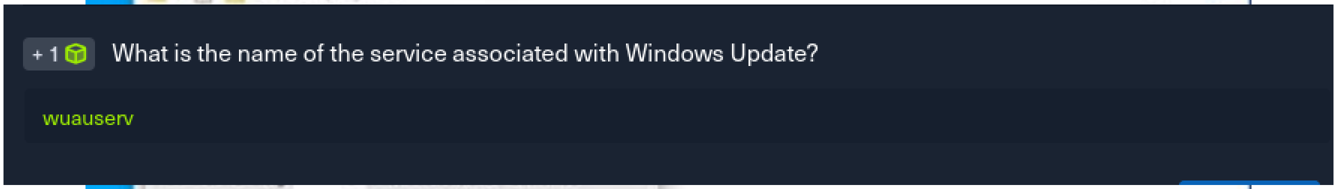


What is the name of the tab that allows you to configure NTFS permissions?

security

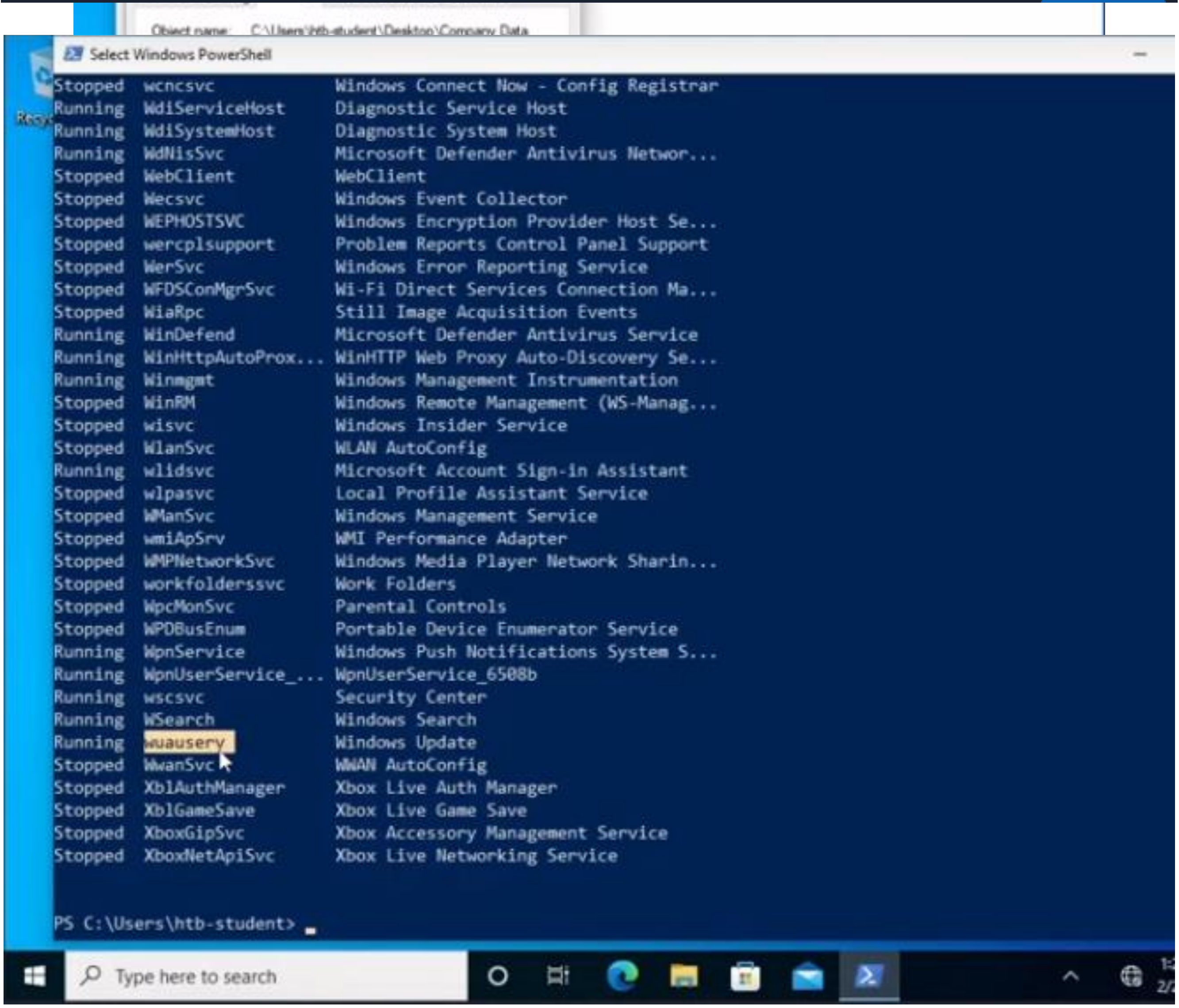
Under the properties of the company data folder, under the security tab we are allowed to configure the NTFS as shown in the image below.



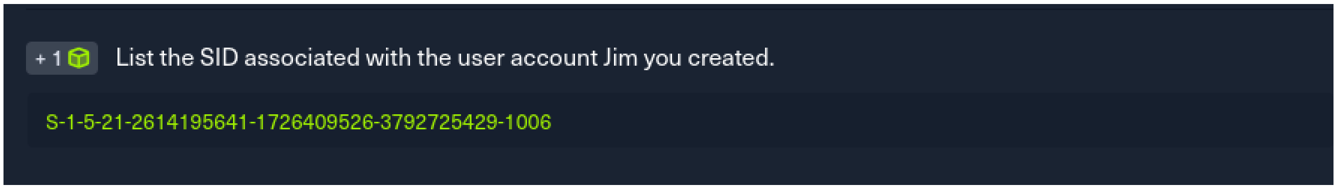


+1 What is the name of the service associated with Windows Update?

wuauserv

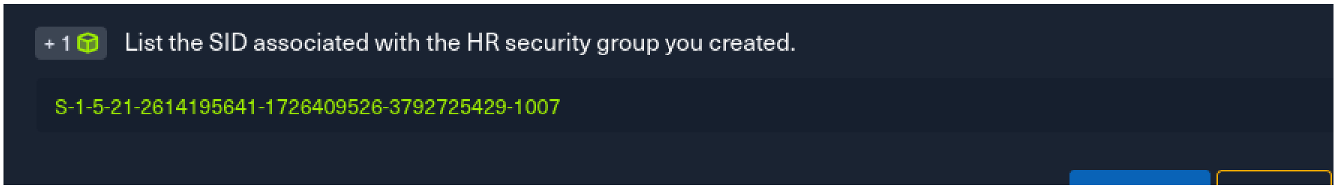

Object name: C:\Users\htb-student\Desktop\Company Data
Select Windows PowerShell
Type here to search

```
Stopped  wcncsvc             Windows Connect Now - Config Registrar
Running  WdiServiceHost      Diagnostic Service Host
Running  WdiSystemHost       Diagnostic System Host
Running  WdNisSvc            Microsoft Defender Antivirus Networ...
Stopped  WebClient           WebClient
Stopped  Wecsvc              Windows Event Collector
Stopped  WEPHOSTSVC          Windows Encryption Provider Host Se...
Stopped  wercplsupport       Problem Reports Control Panel Support
Stopped  WerSvc              Windows Error Reporting Service
Stopped  WFDSConMgrSvc       Wi-Fi Direct Services Connection Ma...
Stopped  WiaRpc              Still Image Acquisition Events
Running  WinDefend           Microsoft Defender Antivirus Service
Running  WinHttpAutoProx...  WinHTTP Web Proxy Auto-Discovery Se...
Running  Winmgmt             Windows Management Instrumentation
Stopped  WinRM               Windows Remote Management (WS-Manag...
Stopped  wisvc               Windows Insider Service
Stopped  WlanSvc             WLAN AutoConfig
Running  wlidsvc             Microsoft Account Sign-in Assistant
Stopped  wlpasvc             Local Profile Assistant Service
Stopped  WManSvc             Windows Management Service
Stopped  wmiApSrv            WMI Performance Adapter
Stopped  WMPNetworkSvc       Windows Media Player Network Sharin...
Stopped  workfolderssvc      Work Folders
Stopped  WpcMonSvc           Parental Controls
Stopped  WPDBusEnum          Portable Device Enumerator Service
Running  WpnService          Windows Push Notifications System S...
Running  WpnUserService_...  WpnUserService_6508b
Running  wscsvc              Security Center
Running  WSearch             Windows Search
Running  wuauserv            Windows Update
Stopped  WwanSvc             WWAN AutoConfig
Stopped  XblAuthManager      Xbox Live Auth Manager
Stopped  XblGameSave         Xbox Live Game Save
Stopped  XboxGipSvc          Xbox Accessory Management Service
Stopped  XboxNetApiSvc       Xbox Live Networking Service


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



+1 List the SID associated with the user account Jim you created.

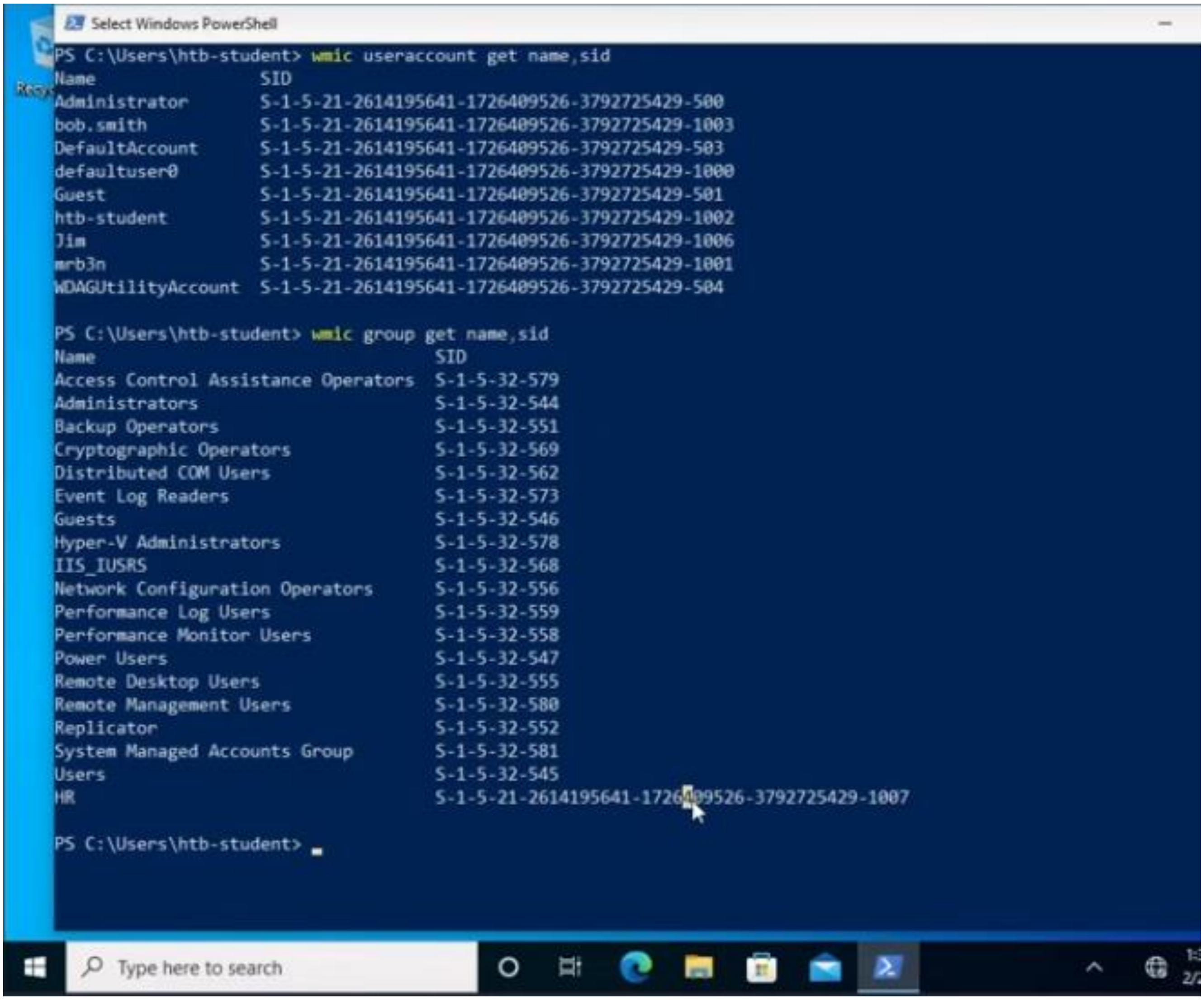
S-1-5-21-2614195641-1726409526-3792725429-1006



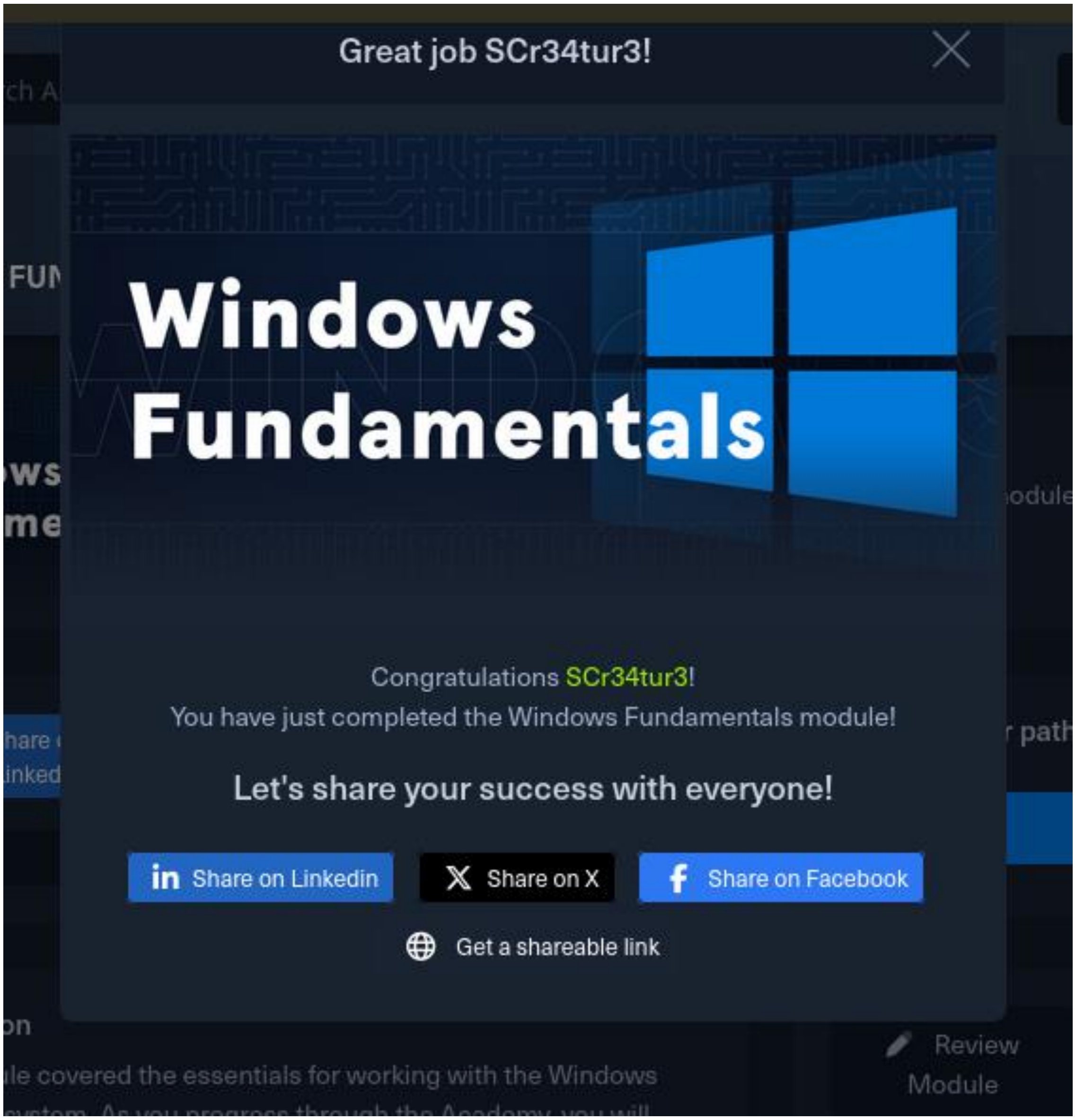
List the SID associated with the HR security group you created.

S-1-5-21-2614195641-1726409526-3792725429-1007

The image below show the actual place I got the SID of both Jim and HR security group



```
PS C:\Users\htb-student> wmic useraccount get name,sid
Name                SID
Administrator       S-1-5-21-2614195641-1726409526-3792725429-500
bob.smith           S-1-5-21-2614195641-1726409526-3792725429-1003
DefaultAccount      S-1-5-21-2614195641-1726409526-3792725429-503
defaultuser0        S-1-5-21-2614195641-1726409526-3792725429-1000
Guest               S-1-5-21-2614195641-1726409526-3792725429-501
htb-student         S-1-5-21-2614195641-1726409526-3792725429-1002
Jim                 S-1-5-21-2614195641-1726409526-3792725429-1006
mrb3n               S-1-5-21-2614195641-1726409526-3792725429-1001
WDAGUtilityAccount  S-1-5-21-2614195641-1726409526-3792725429-504

PS C:\Users\htb-student> wmic group get name,sid
Name                                 SID
Access Control Assistance Operators  S-1-5-32-579
Administrators                       S-1-5-32-544
Backup Operators                     S-1-5-32-551
Cryptographic Operators              S-1-5-32-569
Distributed COM Users                S-1-5-32-562
Event Log Readers                    S-1-5-32-573
Guests                               S-1-5-32-546
Hyper-V Administrators               S-1-5-32-578
IIS_IUSRS                            S-1-5-32-568
Network Configuration Operators      S-1-5-32-556
Performance Log Users                S-1-5-32-559
Performance Monitor Users            S-1-5-32-558
Power Users                          S-1-5-32-547
Remote Desktop Users                 S-1-5-32-555
Remote Management Users              S-1-5-32-580
Replicator                           S-1-5-32-552
System Managed Accounts Group        S-1-5-32-581
Users                                S-1-5-32-545
HR                                   S-1-5-21-2614195641-1726409526-3792725429-1007

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



Great job SCr34tur3!

Congratulations SCr34tur3!

You have just completed the Windows Fundamentals module!

Let's share your success with everyone!

https://academy.hackthebox.com/achievement/1287818/49

CONCLUSION

This was a great module that enabled me to understand the windows OS structure.

In conclusion, having a solid grasp of the windows OS concept will help us understand the various attack pathways into windows systems.