

NAME: DAMIAN MUTISYA

ASSIGNMENT = WINDOWS FUNDAMENTAL

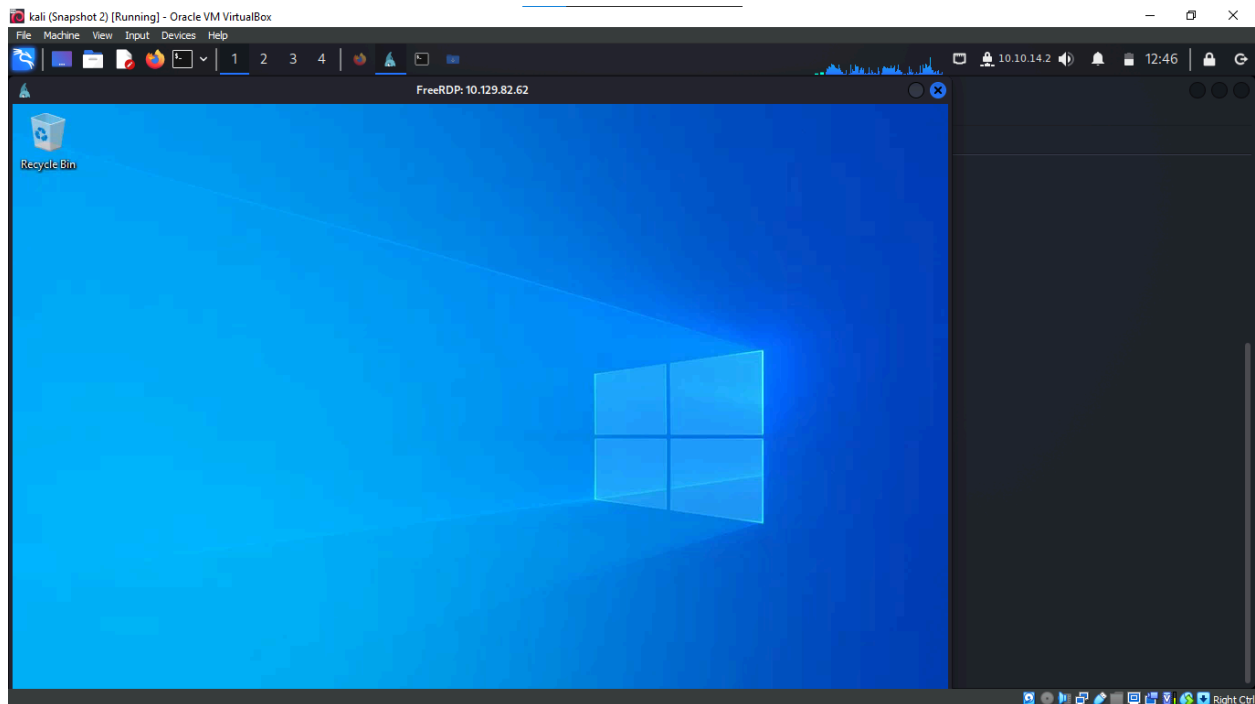
Introduction

This report delves into various aspects of Windows operating system fundamentals, focusing on a specific workstation. It covers a range of topics from system identification and user permissions to network protocols and security features. For the purpose of this analysis, a virtual machine (VM) was connected to a VPN and then remotely accessed the Windows machine from a Linux system using xfreerdp.

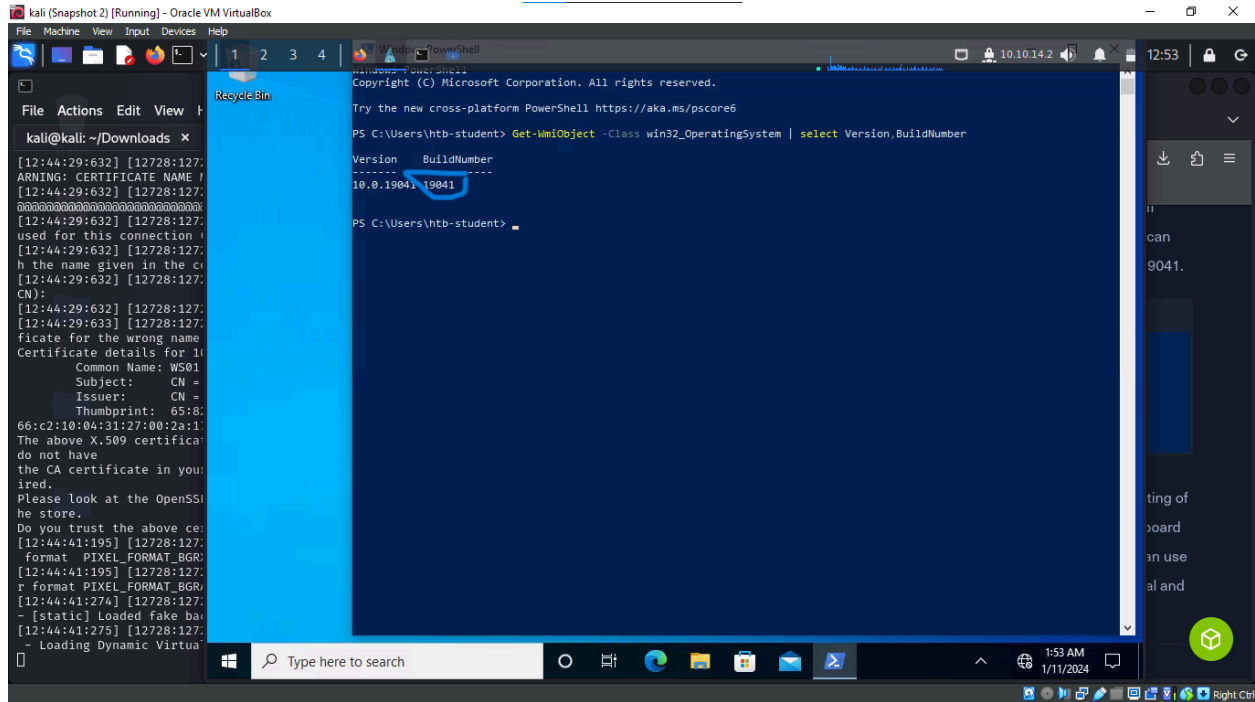
Remote Connection and System Instability

After establishing the VPN connection, the Windows machine was accessed remotely from a Linux system using xfreerdp. However, during the session, the system became unstable. This instability prompted a switch to Remmina, a different remote desktop client, which offered a more stable and efficient working environment.

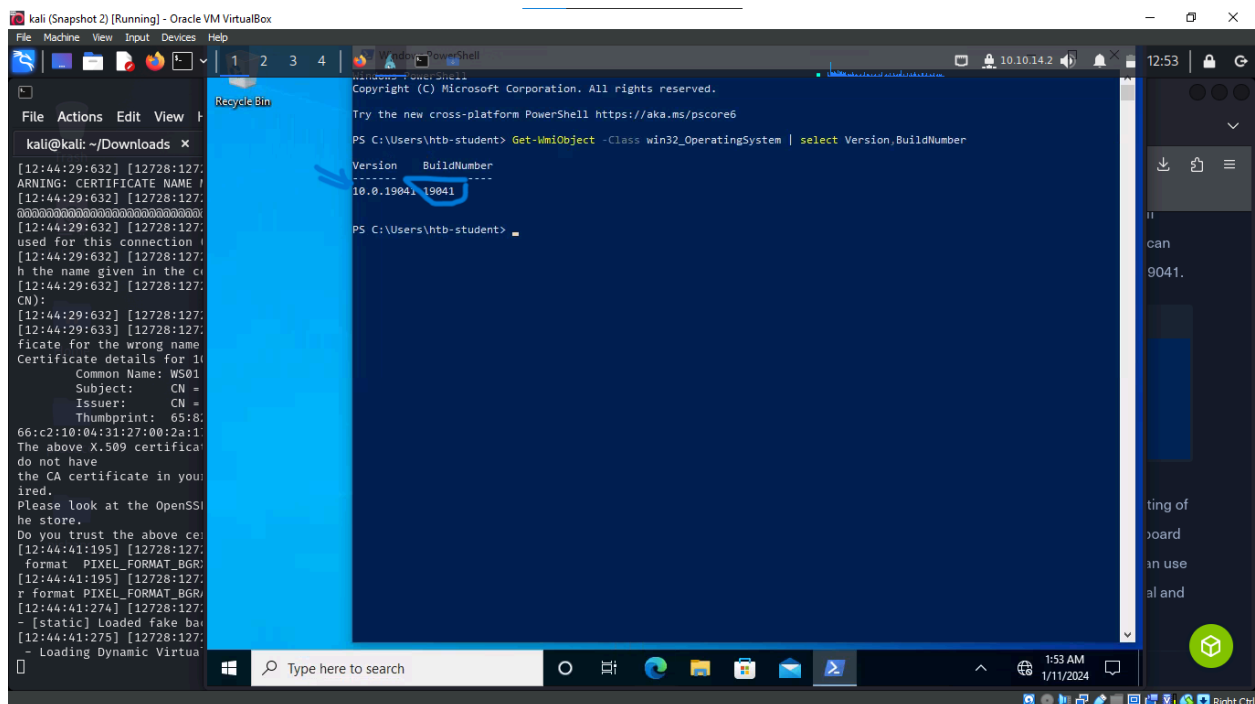
```
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~/Downloads
File Actions Edit View Help
kali@kali: ~/Downloads x root@kali: ~ x
2024-01-11 12:35:17 VERIFY OK: depth=0, C=UK, ST=City, L=London, O=HackTheBox, CN=htb, name=htb, emailAddress=info@hackthebox.eu
2024-01-11 12:35:17 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bit RSA, signature: RSA-SHA1
2024-01-11 12:35:17 [htb] Peer Connection Initiated with [AF_INET]23.106.59.92:1337
2024-01-11 12:35:17 TLS: move_sessions: dest-TM ACTIVE src-TM INITIAL reinit_src=1
2024-01-11 12:35:17 TLS: tls_multi_process: initial untrusted session promoted to trusted
2024-01-11 12:35:19 SENT CONTROL [htb]: 'PUSH_REQUEST' (status=1)
2024-01-11 12:35:19 PUSH: Received control message: 'PUSH_REPLY,route 10.10.10.0 255.255.254.0,route 10.129.0.0 255.255.0.0,route-ipv6 dead:beef:::1,explicit-exit-notify,tun-ipv6,route-gateway 10.10.14.1,topology subnet,ping 10,ping-restart 120,ifconfig-ipv6 dead:beef:2::1000/64 dead:beef:2::1,ifconfig 10.10.14.2 255.255.254.0,peer-id 137,cipher AES-256-CBC'
2024-01-11 12:35:19 OPTIONS IMPORT: --ifconfig/up options modified
2024-01-11 12:35:19 OPTIONS IMPORT: route options modified
2024-01-11 12:35:19 OPTIONS IMPORT: route-related options modified
2024-01-11 12:35:19 net_route_v4_best_gw query: dst 0.0.0.0
2024-01-11 12:35:19 net_route_v4_best_gw result: via 192.168.167.144 dev eth0
2024-01-11 12:35:19 ROUTE_GATEWAY 192.168.167.144/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:df:55:da
2024-01-11 12:35:19 GDG6: Remote host ipv6=n/a
2024-01-11 12:35:19 net_route_v6_best_gw query: dst ::
2024-01-11 12:35:19 sitnl_send: rtnl: generic error (-101): Network is unreachable
2024-01-11 12:35:19 ROUTE6: default_gateway=UNDEF
2024-01-11 12:35:19 TUN/TAP device tun0 opened
2024-01-11 12:35:19 net_iface_mtu_set: mtu 1500 for tun0
2024-01-11 12:35:19 net_iface_up: set tun0 up
2024-01-11 12:35:19 net_addr_v4_add: 10.10.14.2/23 dev tun0
2024-01-11 12:35:19 net_iface_mtu_set: mtu 1500 for tun0
2024-01-11 12:35:19 net_iface_up: set tun0 up
2024-01-11 12:35:19 net_addr_v6_add: dead:beef:2::1000/64 dev tun0
2024-01-11 12:35:19 net_route_v4_add: 10.10.10.0/23 via 10.10.14.1 dev [NULL] table 0 metric -1
2024-01-11 12:35:19 net_route_v4_add: 10.129.0.0/16 via 10.10.14.1 dev [NULL] table 0 metric -1
2024-01-11 12:35:19 add_route_ipv6(dead:beef::/64 -> dead:beef:2::1 metric -1) dev tun0
2024-01-11 12:35:19 net_route_v6_add: dead:beef::/64 via :: dev tun0 table 0 metric -1
2024-01-11 12:35:19 Initialization Sequence Completed
2024-01-11 12:35:19 Data Channel: cipher 'AES-256-CBC', auth 'SHA256', peer-id: 137, compression: 'lzo'
2024-01-11 12:35:19 Timers: ping 10, ping-restart 120
2024-01-11 12:35:19 Protocol options: explicit-exit-notify 1
```



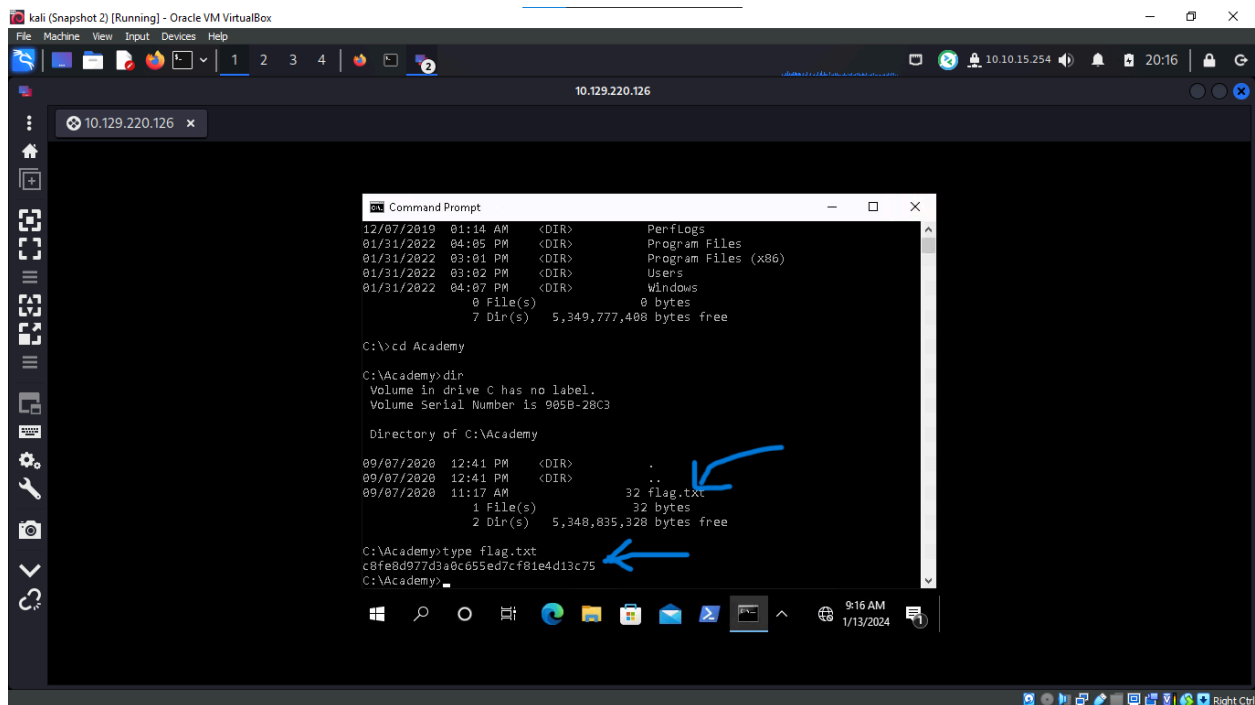
1. **Question:** What is the Build Number of the target workstation? **Answer:** 19041. This refers to the specific version of the Windows 10 operating system installed on the workstation, indicating its update and feature status.



2. **Question:** Which Windows NT version is installed on the workstation? **Answer:** Windows 10. This identifies the major release version of the Microsoft Windows NT operating system on the workstation.



3. **Question:** Find the non-standard directory in the C drive. What are the contents of the flag file saved in this directory? **Answer:** c8fe8d977d3a0c655ed7cf81e4d13c75. This unusual directory name suggests a specific application or user-created content, requiring further investigation for context and content.



The screenshot shows a Kali Linux terminal window with the following commands and output:

```
12/07/2019 01:14 AM <DIR> PerfLogs
01/31/2022 04:05 PM <DIR> Program Files
01/31/2022 03:01 PM <DIR> Program Files (x86)
01/31/2022 03:02 PM <DIR> Users
01/31/2022 04:07 PM <DIR> Windows
0 File(s) 0 bytes
7 Dir(s) 5,349,777,408 bytes free

C:\>cd Academy

C:\Academy>dir
Volume in drive C has no label.
Volume Serial Number is 905B-28C3

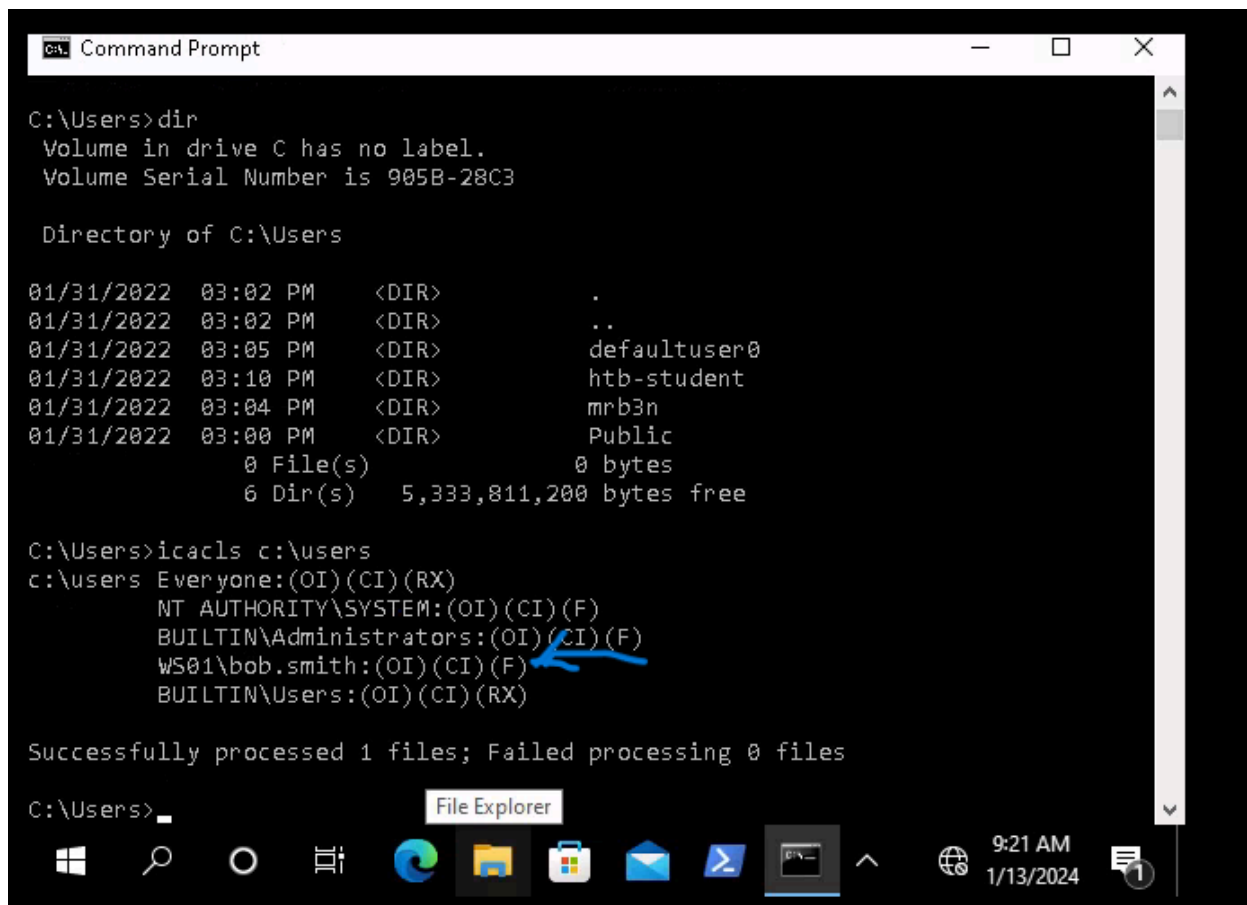
Directory of C:\Academy

09/07/2020 12:41 PM <DIR> .
09/07/2020 12:41 PM <DIR> ..
09/07/2020 11:17 AM <DIR> 32 flag.txt
1 File(s) 32 bytes
2 Dir(s) 5,348,835,328 bytes free

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

Two blue arrows are present: one pointing to the '32 flag.txt' entry in the directory listing, and another pointing to the output of the 'type flag.txt' command.

4. **Question:** What system user has full control over the c:\users directory? **Answer:** bob.smith. This user has full administrative control over the 'C:\Users' directory, indicating significant user rights or administrative privileges.

A screenshot of a Windows Command Prompt window titled "C:\ Command Prompt". The window shows the output of the 'dir' command in the C:\Users directory, followed by the 'icacls' command to view permissions. The permissions list includes 'Everyone:(OI)(CI)(RX)', 'NT AUTHORITY\SYSTEM:(OI)(CI)(F)', 'BUILTIN\Administrators:(OI)(CI)(F)', 'WS01\bob.smith:(OI)(CI)(F)' (highlighted with a blue arrow), and 'BUILTIN\Users:(OI)(CI)(RX)'. The taskbar at the bottom shows the Start button, search icon, task view icon, and several application icons including File Explorer, which is currently active. The system clock shows 9:21 AM on 1/13/2024.

```
C:\Users>dir
Volume in drive C has no label.
Volume Serial Number is 905B-28C3

Directory of C:\Users

01/31/2022  03:02 PM    <DIR>          .
01/31/2022  03:02 PM    <DIR>          ..
01/31/2022  03:05 PM    <DIR>          defaultuser0
01/31/2022  03:10 PM    <DIR>          htb-student
01/31/2022  03:04 PM    <DIR>          mnb3n
01/31/2022  03:00 PM    <DIR>          Public
               0 File(s)                0 bytes
               6 Dir(s)      5,333,811,200 bytes free

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>
```

5. **Question:** What protocol discussed in this section is used to share resources on the network using Windows? **Answer:** SMB (Server Message Block). This protocol is crucial for file sharing, printer access, and other networked resource interactions in Windows environments.

NTFS vs. Share Permissions

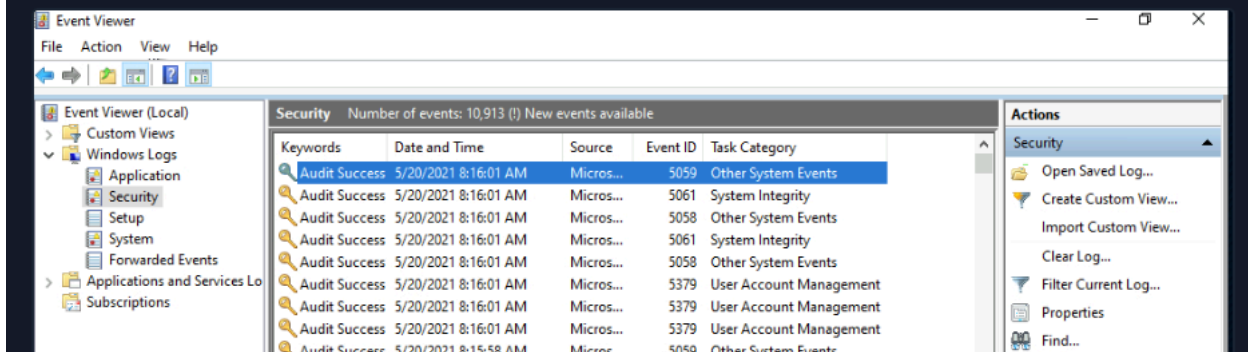
Microsoft owns over 70% of the global market share on desktop operating systems with Windows. This explains why most malware authors choose to write malware for Windows and why many perceive Windows as less secure than other operating systems. From a business perspective it just makes sense for malware authors to expend resources on writing malware for Windows. It is a high-value target. The idea that any OS is immune to malware is a technical fallacy. If software can be written for an operating system then a virus can be written for an operating system. Keep in mind that a virus, by definition, is software written with malicious intent and can be written for any OS. Many variants of malware written for Windows can spread over the network via network shares with lenient permissions applied. It is also worth noting that to this day, the infamous **EternalBlue** vulnerability still haunts unpatched Windows systems running **SMBv1** and often paves the way for ransomware to shut down organizations.

The **Server Message Block protocol (SMB)** is used in Windows to connect shared resources like files and printers. It is used in large, medium, and small enterprise environments. See the image below to visualize this concept:

6. **Question:** What is the name of the utility that can be used to view logs made by a Windows system? **Answer:** Event Viewer. This essential tool allows for the inspection of system logs, aiding in troubleshooting and system monitoring.

Viewing Share access logs in Event Viewer

Event Viewer is another good place to investigate actions completed on Windows. Almost every operating system has a logging mechanism and a utility to view the logs that were captured. Know that a log is like a journal entry for a computer, where the computer writes down all the actions that were performed and numerous details associated with that action. We can view the logs created for every action we performed when accessing the Windows 10 target box, as well as when creating, editing and accessing the shared folder.



7. **Question:** What is the full directory path to the Company Data share we created? **Answer:** C:\Users\htb-student\Desktop\company data. This path specifies the location of a shared data directory, likely used for storing and sharing company-related documents.

```
10.129.208.19 x
Microsoft Windows [version 10.0.19041.1]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\htb-student>net share

Share name      Resource                                Remark
-----
C$              C:\                                    Default share
IPC$            C:\                                   Remote IPC
ADMIN$          C:\WINDOWS                           Remote Admin
company data    C:\Users\htb-student\Desktop\company data
The command completed successfully.

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

8. **Question:** Identify one of the non-standard update services running on the host. What is the full name of the service executable? **Answer:** FoxitReaderUpdateService.exe. This executable is part of a third-party application, Foxit Reader, and is not a native Windows service.

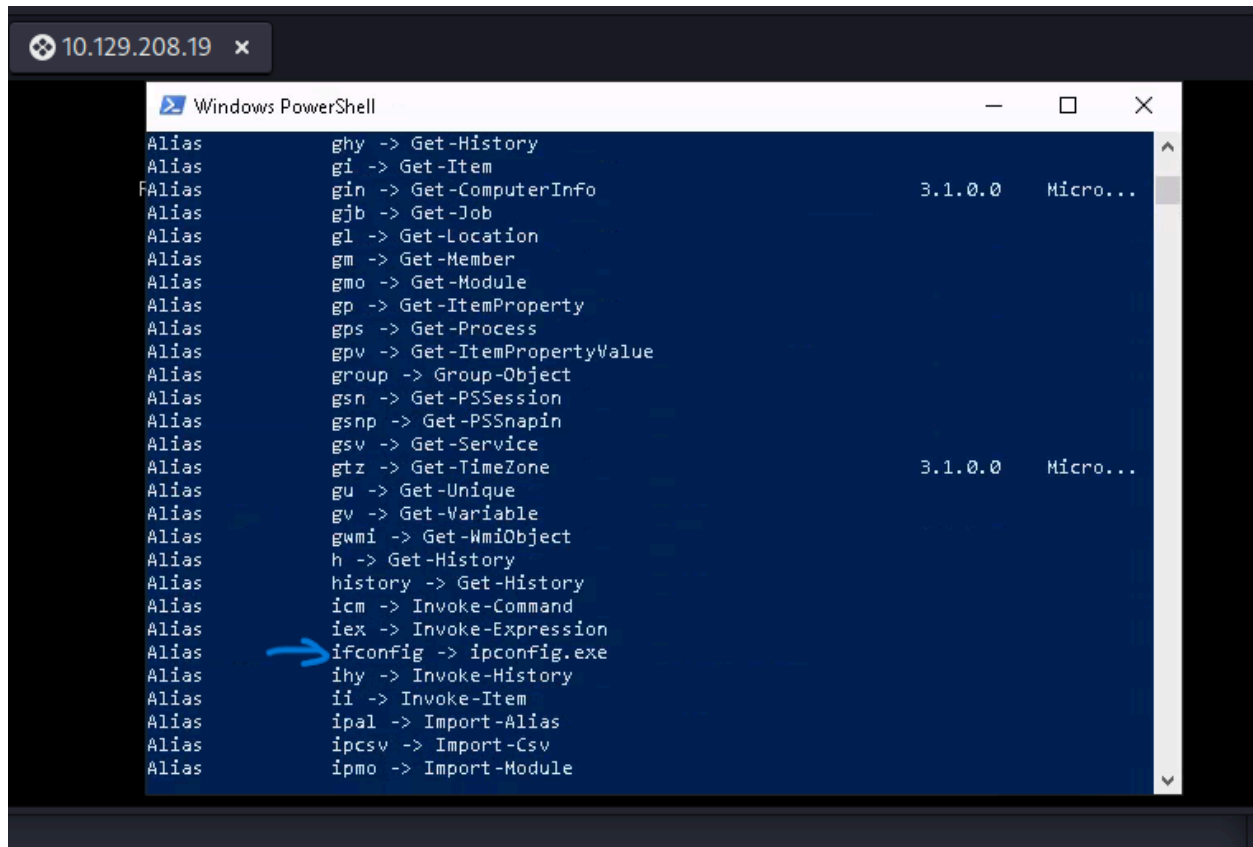
```
9.208.19 x
Windows PowerShell
PS C:\Users\htb-student> Get-Service | where-object {$_.Name -like "*reader*"}f1
Where-Object : A positional parameter cannot be found that accepts argument 'f1'.
At line:1 char:15
+ Get-Service | where-object {$_.Name -like "*reader*"}f1
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (:) [Where-Object], ParameterBindingException
+ FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.WhereObjectCommand

PS C:\Users\htb-student> Get-Service | where-object {$_.Name -like "*reader*"}|f1

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>
```

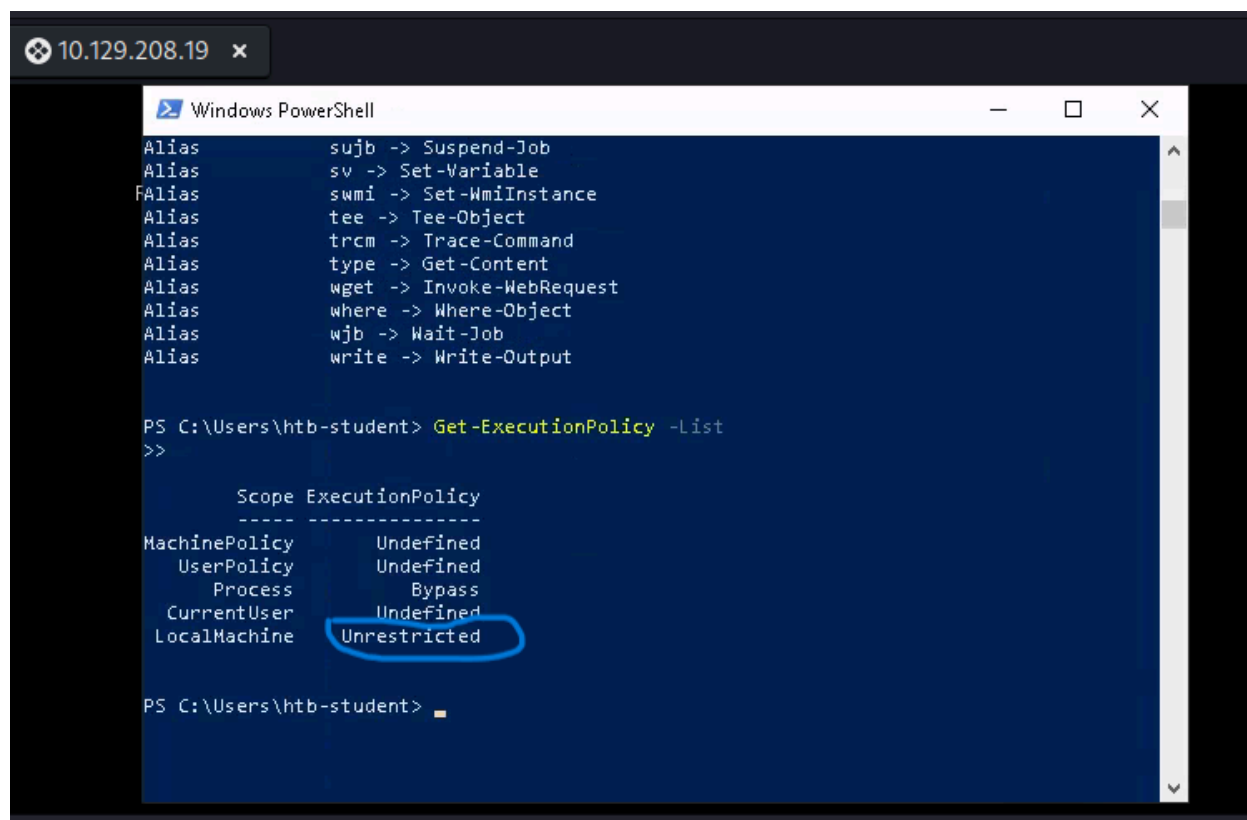
9. **Question:** What is the alias set for the ipconfig.exe command? **Answer:** ifconfig. This alias, typically used in Unix-like systems, has been set for convenience in the Windows environment.



The screenshot shows a Windows PowerShell window with a list of aliases. A blue arrow points to the 'ifconfig' alias, which is mapped to 'ipconfig.exe'. The window title is 'Windows PowerShell' and the address bar shows '10.129.208.19'.

```
Alias      ghy -> Get-History
Alias      gi -> Get-Item
Alias      gin -> Get-ComputerInfo 3.1.0.0 Micro...
Alias      gjb -> Get-Job
Alias      gl -> Get-Location
Alias      gm -> Get-Member
Alias      gmo -> Get-Module
Alias      gp -> Get-ItemProperty
Alias      gps -> Get-Process
Alias      gpv -> Get-ItemPropertyValue
Alias      group -> Group-Object
Alias      gsn -> Get-PSSession
Alias      gsnp -> Get-PSSnapin
Alias      gsv -> Get-Service 3.1.0.0 Micro...
Alias      gtz -> Get-TimeZone
Alias      gu -> Get-Unique
Alias      gv -> Get-Variable
Alias      gwmi -> Get-WmiObject
Alias      h -> Get-History
Alias      history -> Get-History
Alias      icm -> Invoke-Command
Alias      iex -> Invoke-Expression
Alias      ifconfig -> ipconfig.exe
Alias      ihy -> Invoke-History
Alias      ii -> Invoke-Item
Alias      ipal -> Import-Alias
Alias      ipcsv -> Import-Csv
Alias      ipmo -> Import-Module
```

10. **Question:** Find the Execution Policy set for the LocalMachine scope. **Answer:** Unrestricted. This policy setting in PowerShell indicates no restrictions on script execution, which could be a security concern if not managed properly.



A screenshot of a Windows PowerShell terminal window. The title bar shows the address 10.129.208.19. The terminal displays a list of aliases and their corresponding cmdlets, followed by the command `Get-ExecutionPolicy -List` and its output. The output is a table with two columns: Scope and ExecutionPolicy. The 'LocalMachine' scope has an 'Unrestricted' policy, which is circled in blue.

```
Alias      sujb -> Suspend-Job
Alias      sv  -> Set-Variable
Alias      swmi -> Set-WmiInstance
Alias      tee -> Tee-Object
Alias      trcm -> Trace-Command
Alias      type -> Get-Content
Alias      wget -> Invoke-WebRequest
Alias      where -> Where-Object
Alias      wjb -> Wait-Job
Alias      write -> Write-Output

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>
```

11. **Question:** Use WMI to find the serial number of the system. **Answer:** 00329-10280-00000-AA938. This serial number, unique to this system, is retrieved via Windows Management Instrumentation (WMI).

```
10.129.208.19 x
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, SerialNumber, Version | ft
>>

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

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

12. **Question:** Find the SID of the bob.smith user. **Answer:** S-1-5-21-2614195641-1726409526-3792725429-1003. This Security Identifier is unique to the 'bob.smith' user account in the Windows security architecture.

```
10.129.208.19 x
(c) 2019 Microsoft Corporation. All rights reserved.

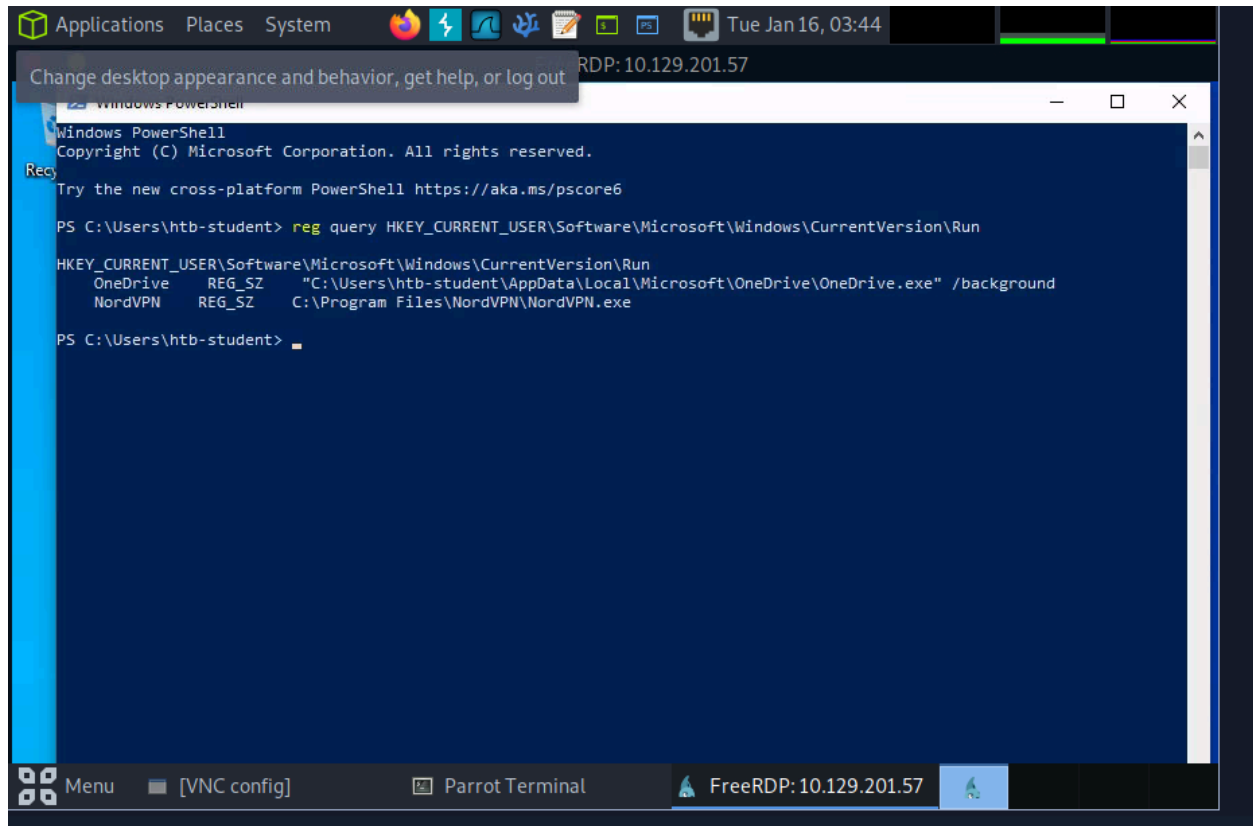
C:\Users\htb-student>wmic useraccount get name sid
Invalid GET Expression.

C:\Users\htb-student>wmic useraccount get-name sid
Invalid GET switch.

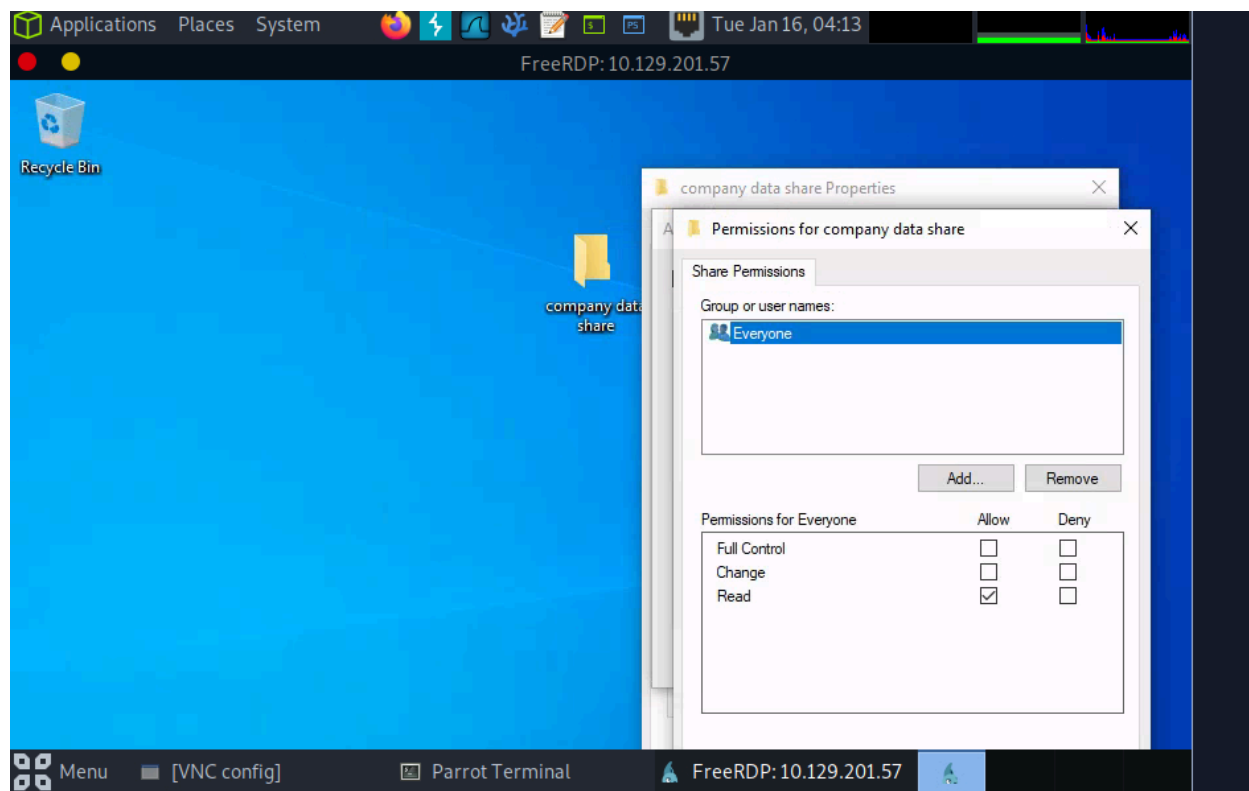
C:\Users\htb-student>wmic useraccount get name, sid
Name                SID
Administrator       S-1-5-21-2614195641-1726409526-3792725429-500
bob.smith            S-1-5-21-2614195641-1726409526-3792725429-1003
DefaultAccount       S-1-5-21-2614195641-1726409526-3792725429-503
defaultuser0         S-1-5-21-2614195641-1726409526-3792725429-1000
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>_
```

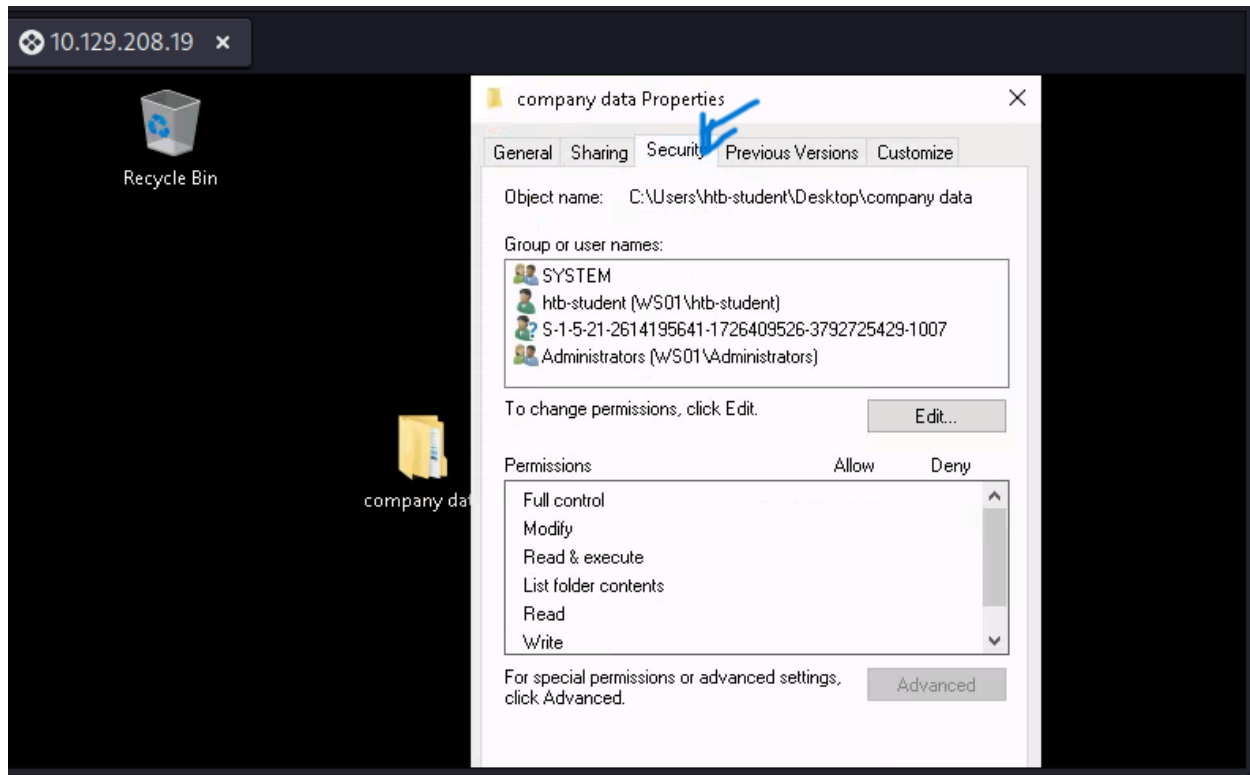
13. **Question:** What 3rd party security application is disabled at startup for the current user? **Answer:** NordVPN. This application, a VPN service provider, is disabled at startup for the current user, impacting their online security and privacy settings.



14. **Question:** What is the name of the group that is present in the Company Data Share Permissions ACL by default? **Answer:** Everyone. This default group setting in the Access Control List indicates that all users have some level of access to the Company Data Share.

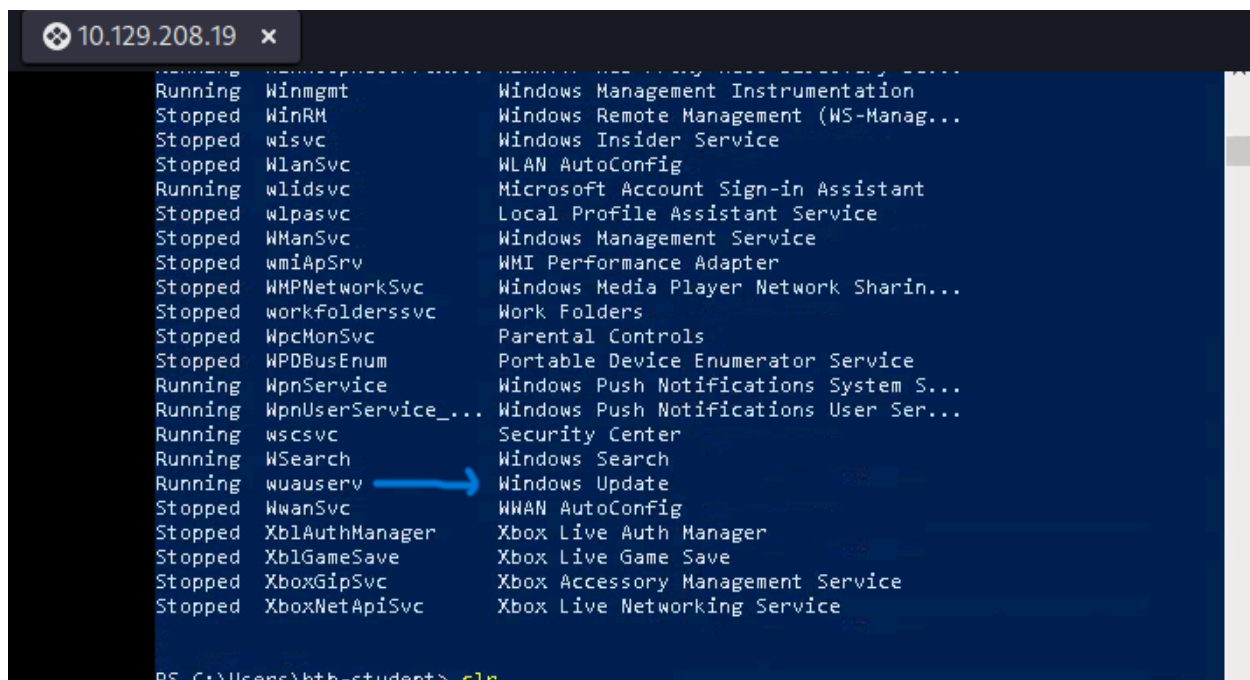


15. **Question:** What is the name of the tab that allows you to configure NTFS permissions? **Answer:** Security. This tab in Windows File Explorer is used for setting NTFS permissions, crucial for managing access to files and directories.

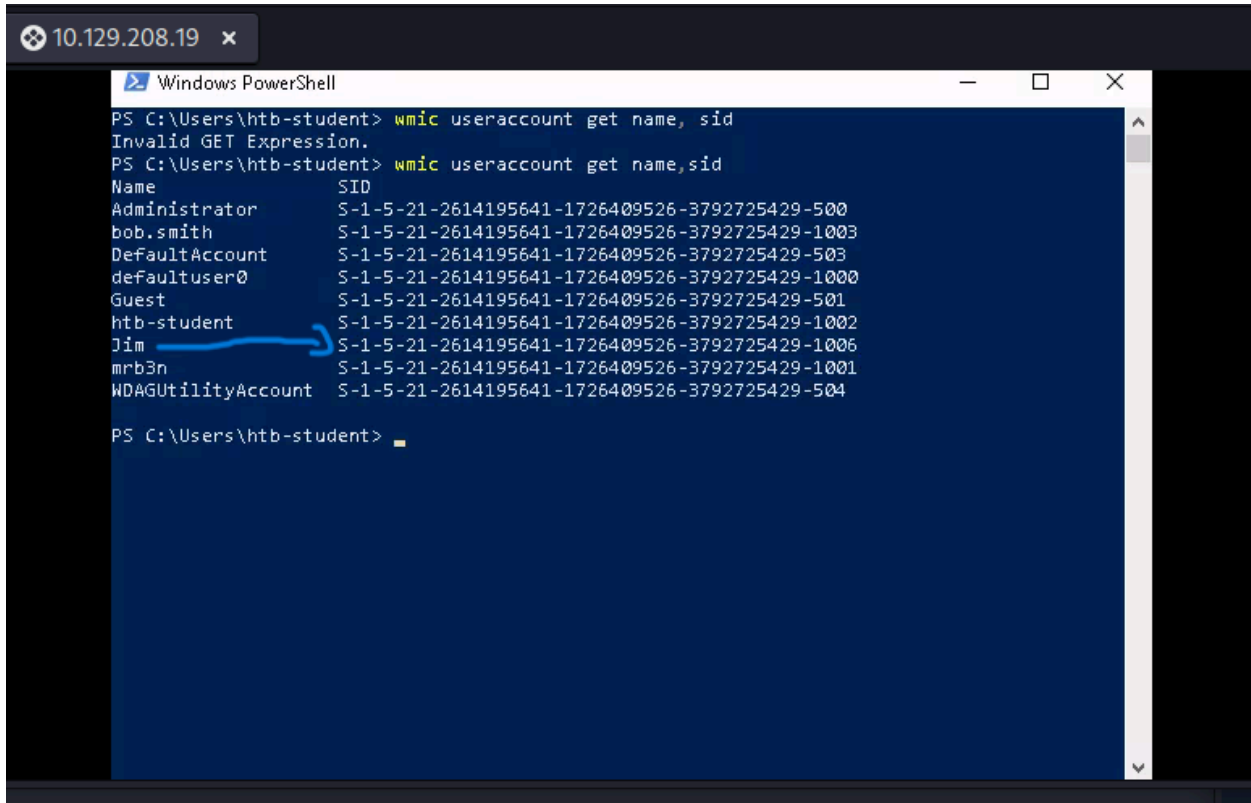


16. **Question:** What is the name of the service associated with Windows Update?

Answer: wuauserv. The Windows Update Service (wuauserv) is responsible for managing the download and installation of updates in Windows.

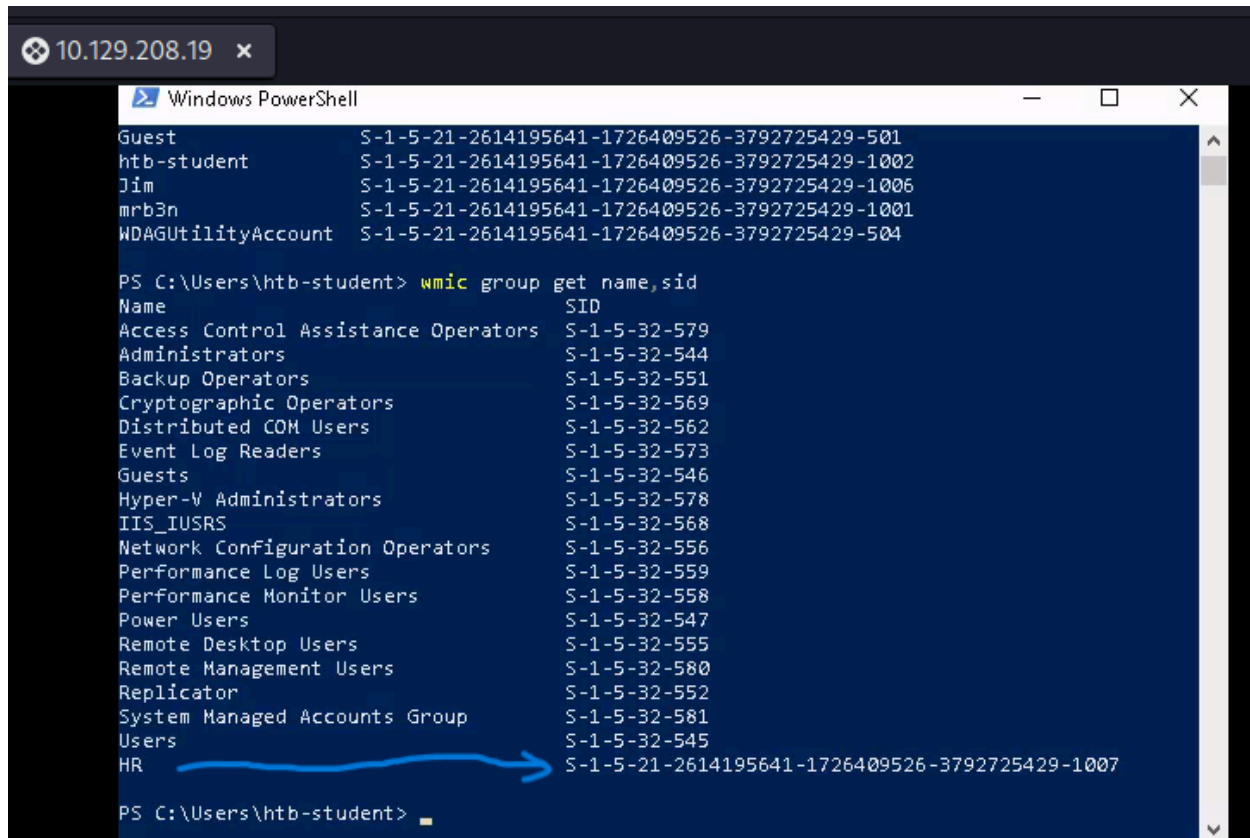


17. **Question:** List the SID associated with the user account Jim you created. **Answer:** S-1-5-21-2614195641-1726409526-3792725429-1006. This unique Security Identifier is assigned to the user account named "Jim."



```
10.129.208.19 x
Windows PowerShell
PS C:\Users\htb-student> wmic useraccount get name, sid
Invalid GET Expression.
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>
```

18. **Question:** List the SID associated with the HR security group you created. **Answer:** S-1-5-21-2614195641-1726409526-3792725429-1007. This Security Identifier represents the HR security group, designated for managing access related to Human Resources.



The screenshot shows a Windows PowerShell terminal window with a title bar indicating the IP address 10.129.208.19. The terminal displays the output of the 'wmic group get name,sid' command, listing various system groups and their Security Identifiers (SIDs). A blue arrow points to the 'HR' group, which has the SID S-1-5-21-2614195641-1726409526-3792725429-1007.

```
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>
```

Conclusion

This comprehensive report provides insights into the Windows operating system's configuration and security settings on a specific workstation. Each question and answer combination sheds light on various aspects, from system identification to user permissions and network protocols, emphasizing the importance of understanding these fundamentals for effective system management and security in a Windows environment.

Please find the sharable link:

<https://academy.hackthebox.com/achievement/949661/49>



HTB ACADEMY

Windows Fundamentals



Congratulations **Damlano254**, you have completed this module!

Module: **Windows Fundamentals**

Difficulty: **Fundamental**

Exercises Completed: **18 /18**

Completed at: 16 Jan 2024