NAME: DAMIAN MUTISYA

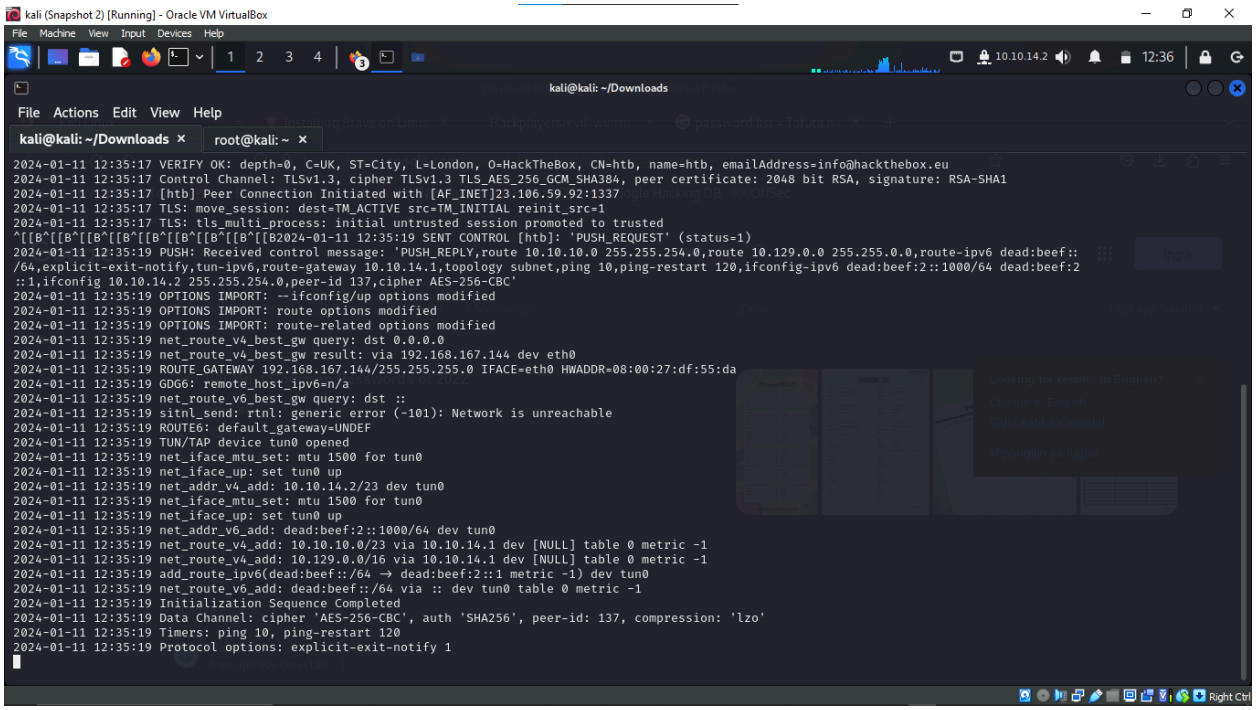
ASSIGNMENT = WINDOWS FUNDAMENTAL

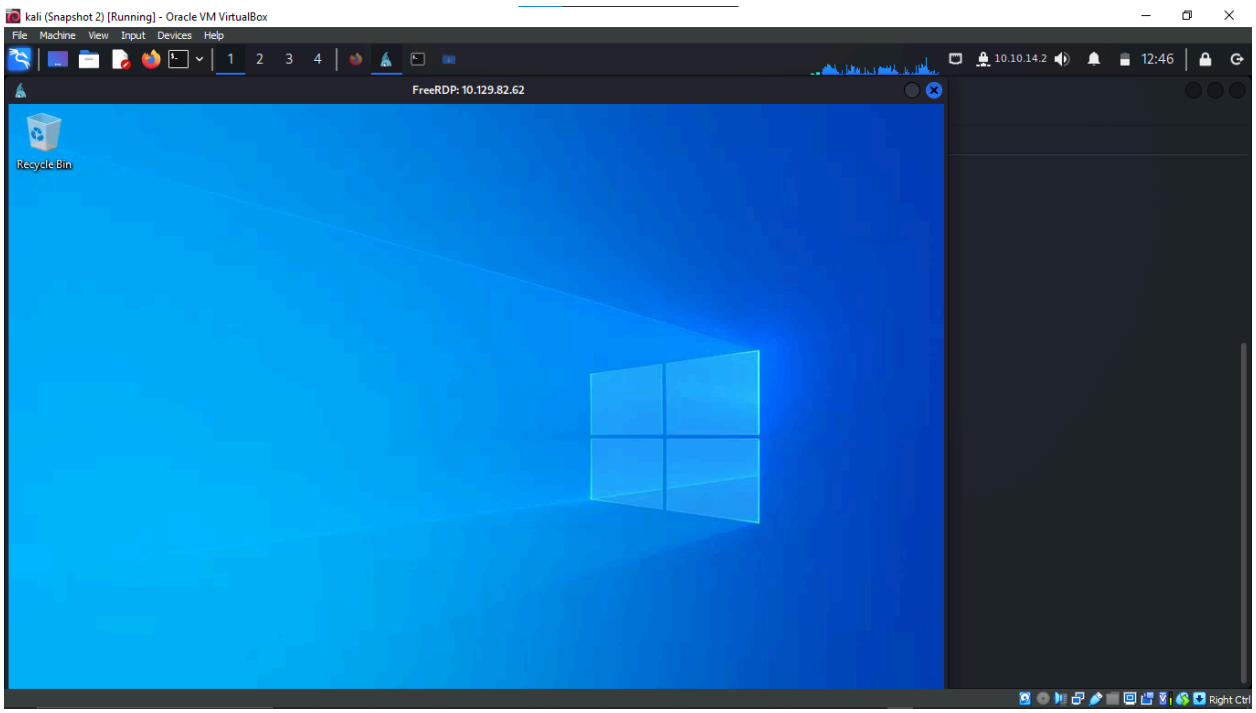
Introduction

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.

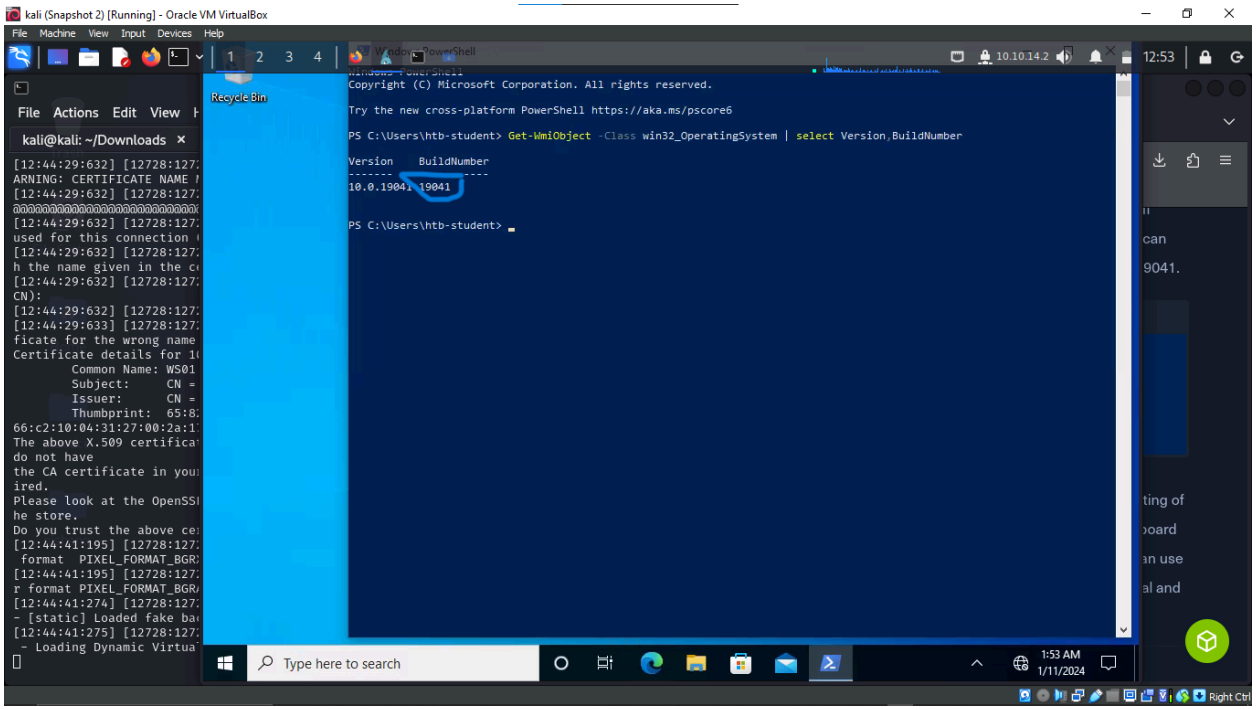
Remote Connection and System Instability

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.

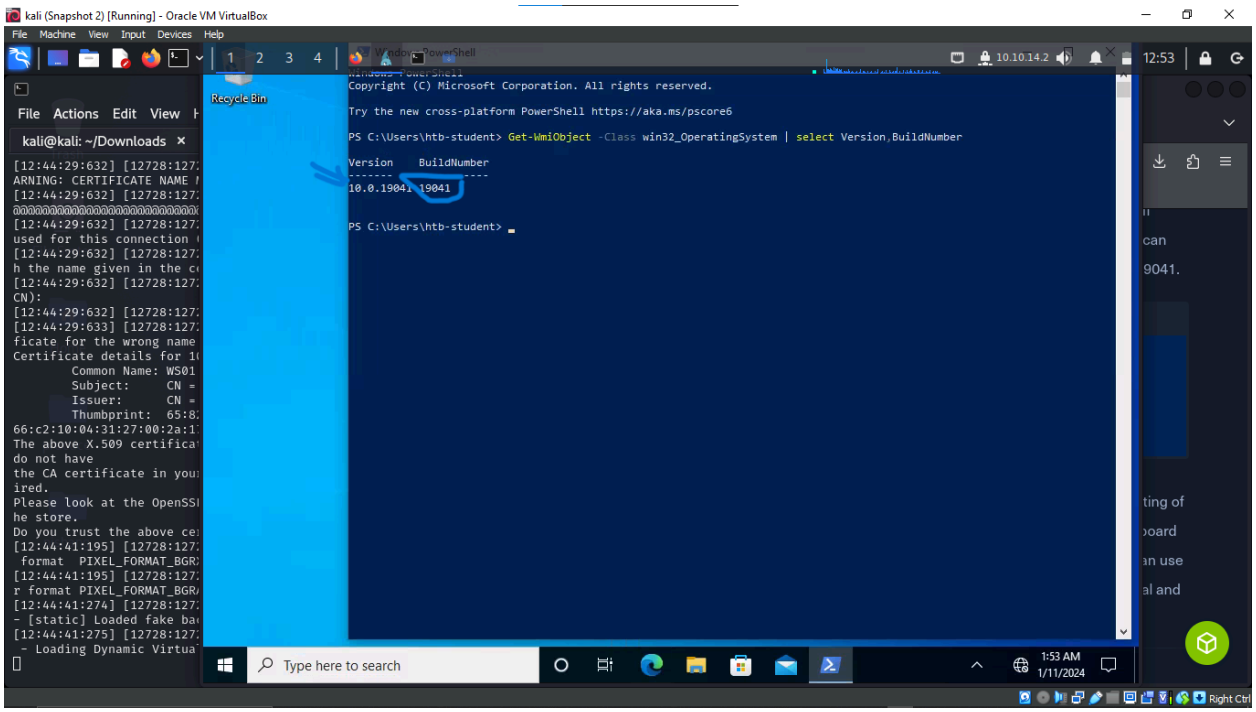




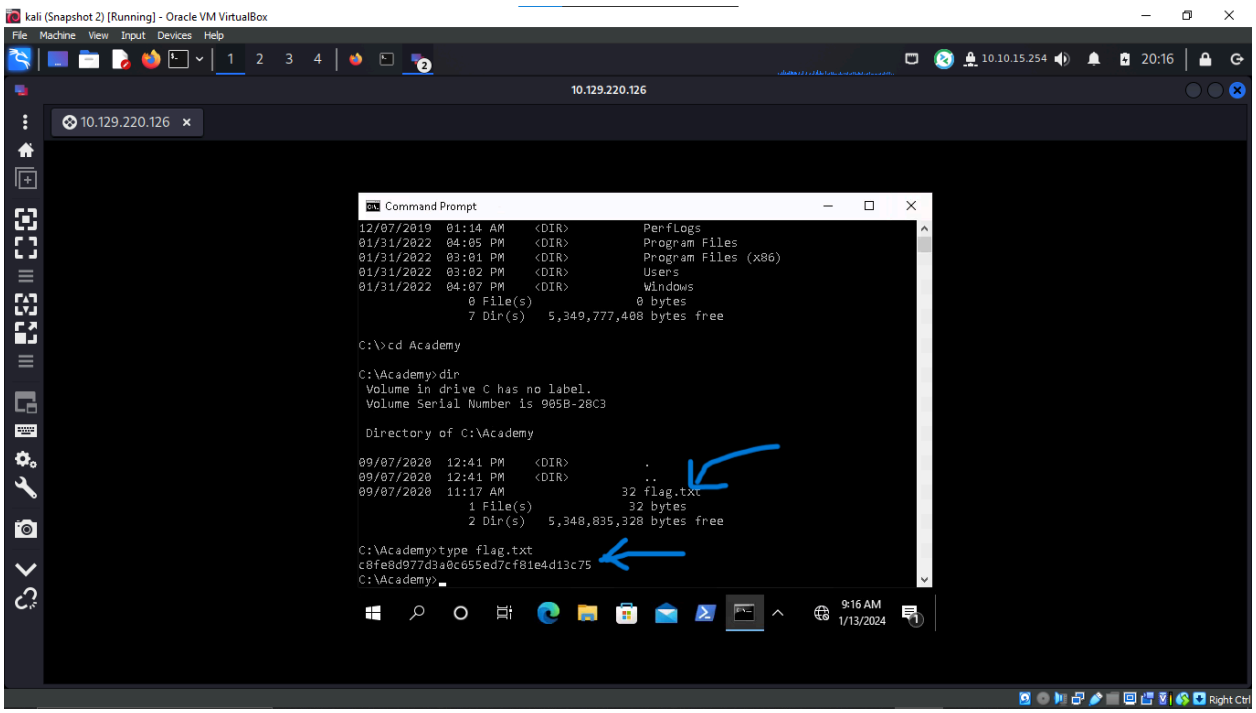
1. **Question**: What is the Build Number of the target workstation? **Answer**: 19041. This refers to the specific version of the Windows 10 operating system installed on the workstation, indicating its update and feature status.



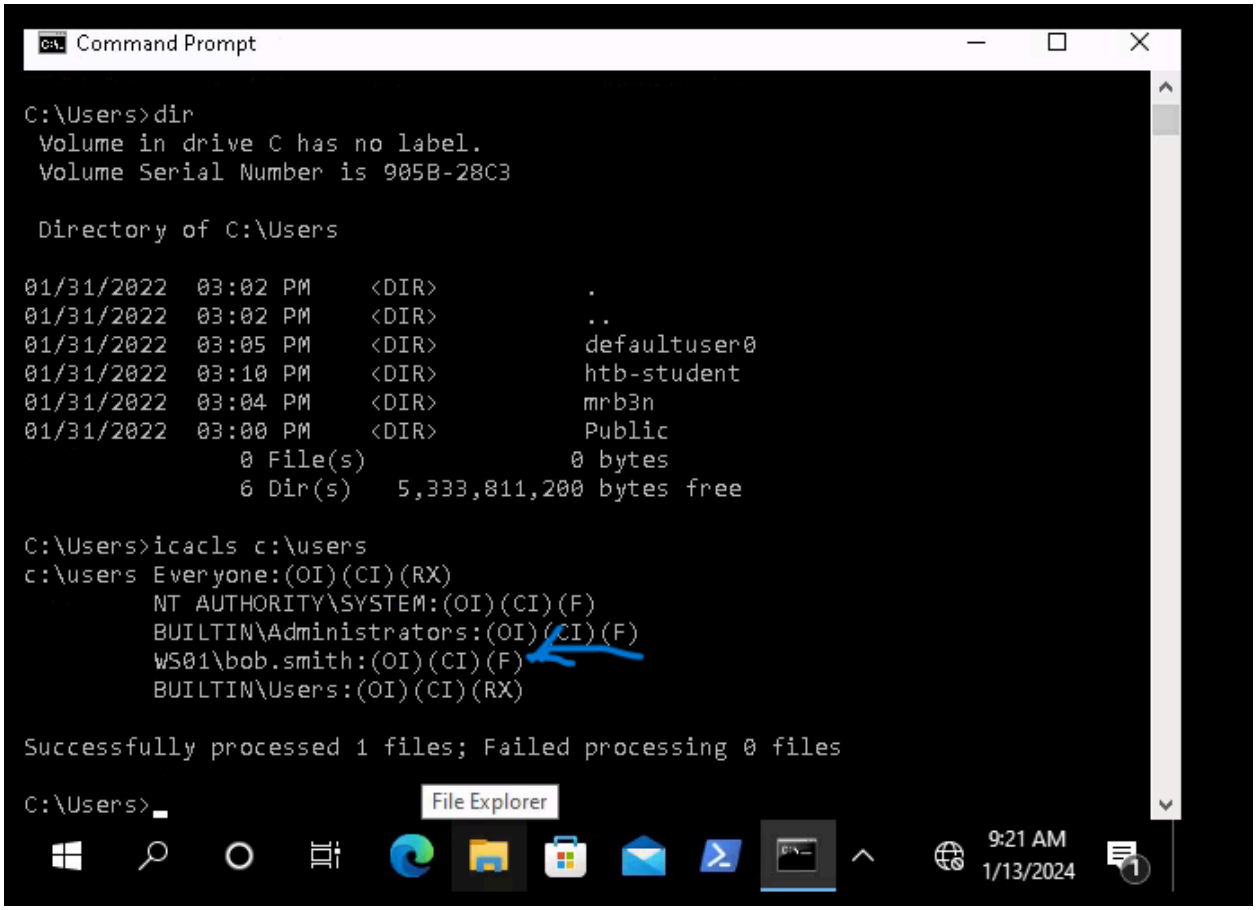
2. **Question**: Which Windows NT version is installed on the workstation? **Answer**: Windows 10. This identifies the major release version of the Microsoft Windows NT operating system on the workstation.



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.



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.



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

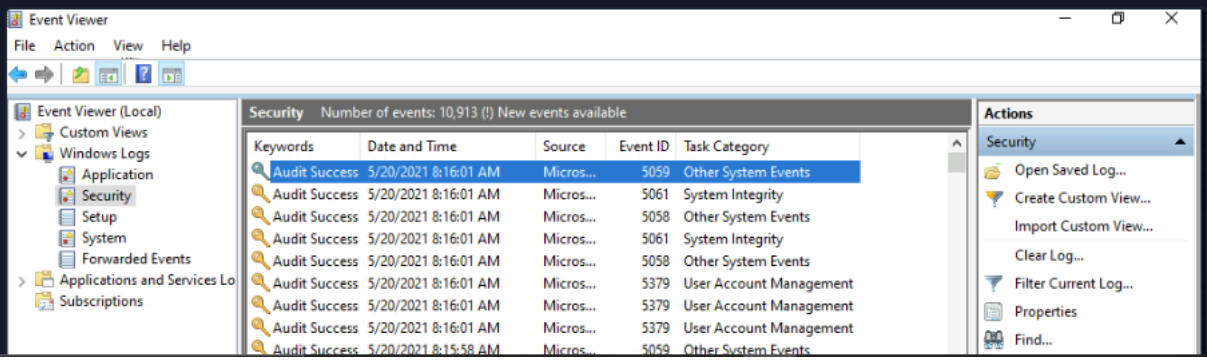
Microsoft owns over 70% of the global market share on desktop operating systems with Windows. This explains why most malware authors choose to write malware for Windows and why many perceive Windows as less secure than other operating systems. From a business perspective it just makes sense for malware 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:

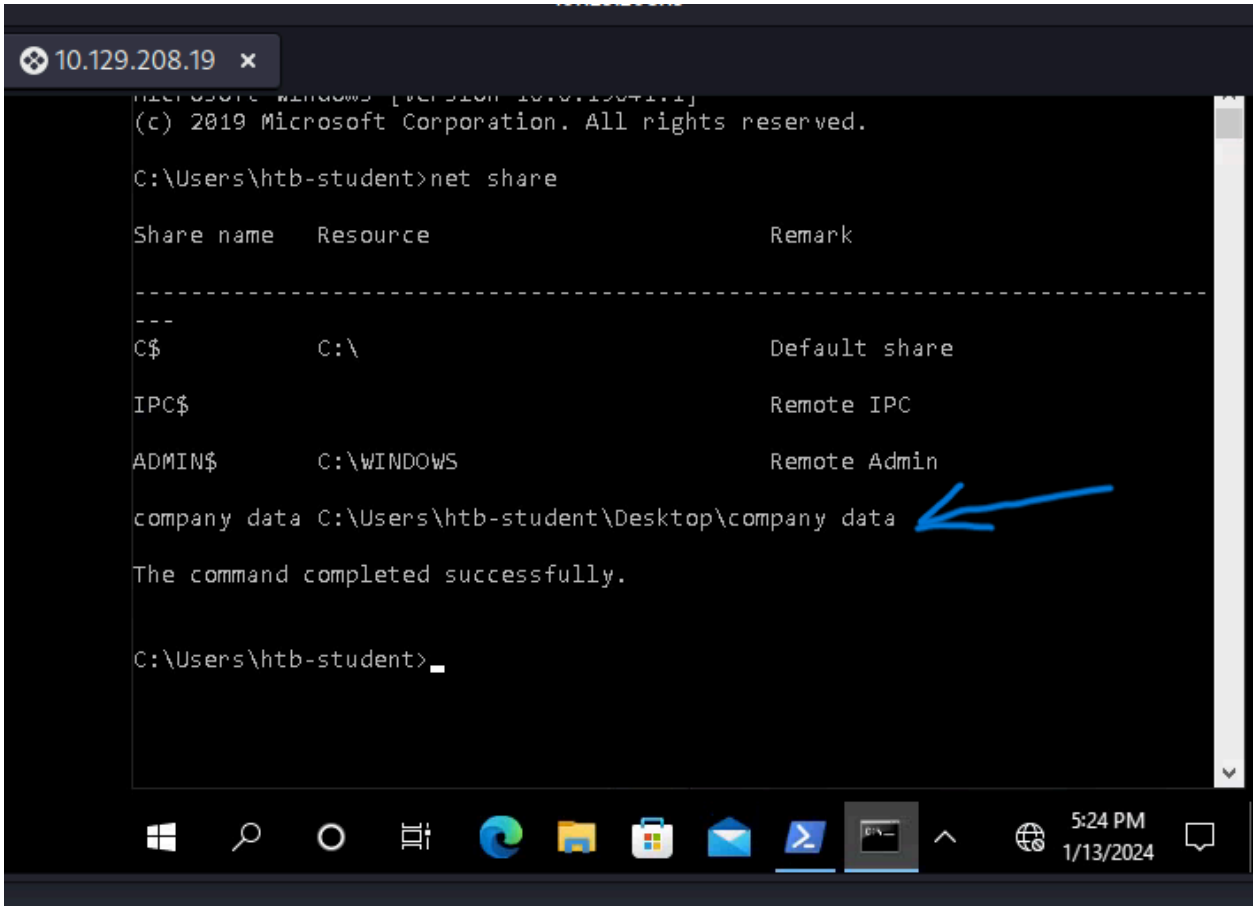
6. **Question**: What is the name of the utility that can be used to view logs made by a Windows system? **Answer**: Event Viewer. This essential tool allows for the inspection of system logs, aiding in troubleshooting and system monitoring.

Viewing Share access logs in Event Viewer

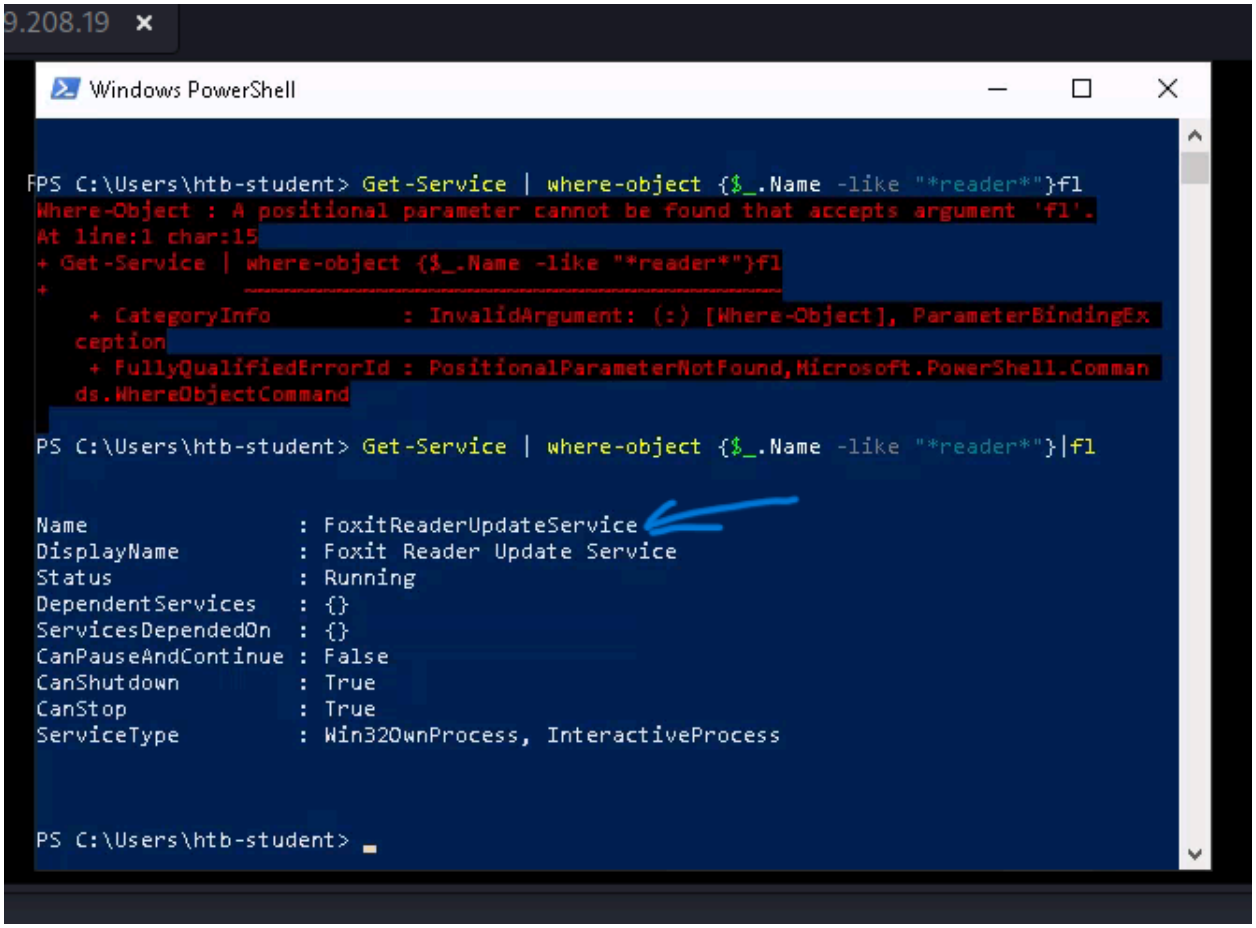
`Event Viewer` is another good place to investigate actions completed on Windows. Almost every operating system has a logging mechanism and a utility to view the logs that were captured. Know that a log is like a journal entry for a computer, where the computer writes down all the actions that were performed 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.



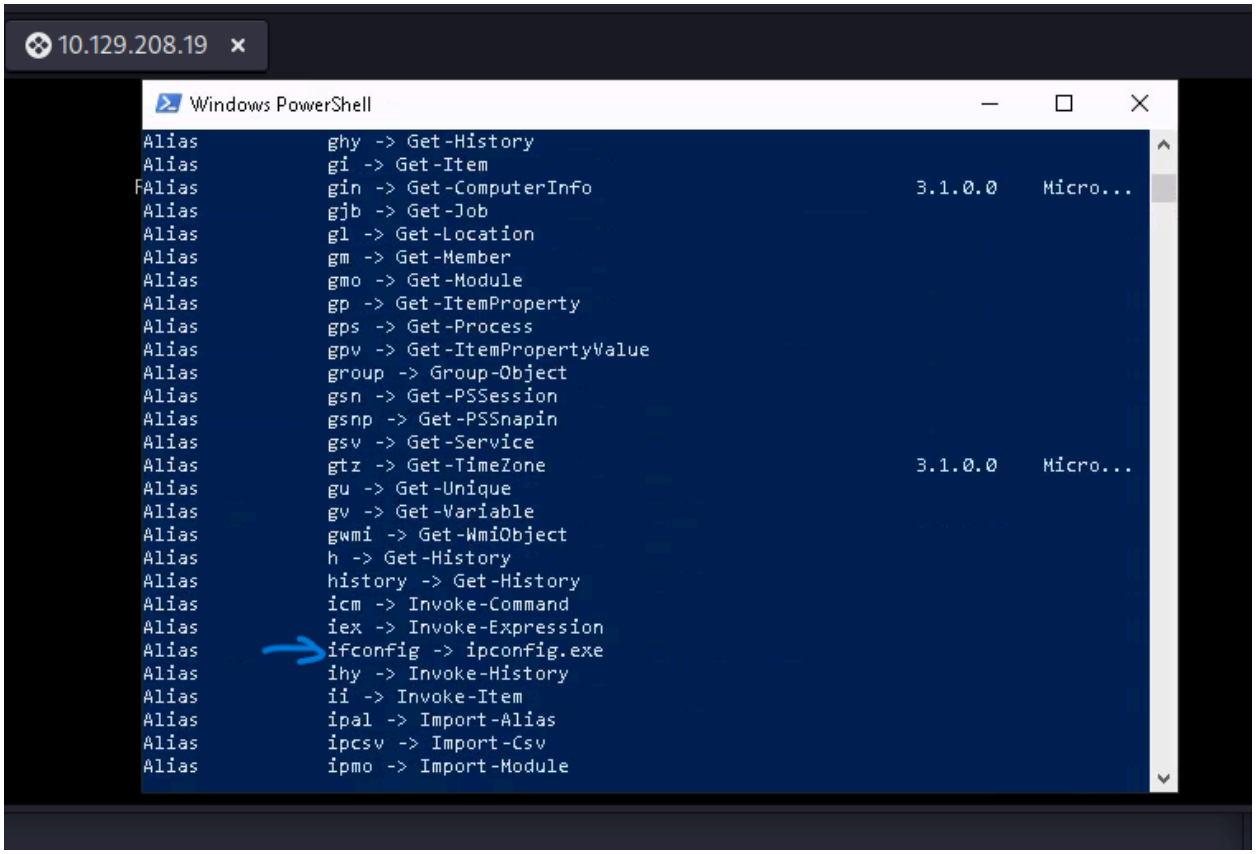
7. **Question**: What is the full directory path to the Company Data share we created? **Answer**: C:\Users\htb-student\Desktop\company data. This path specifies the location of a shared data directory, likely used for storing and sharing company-related documents.



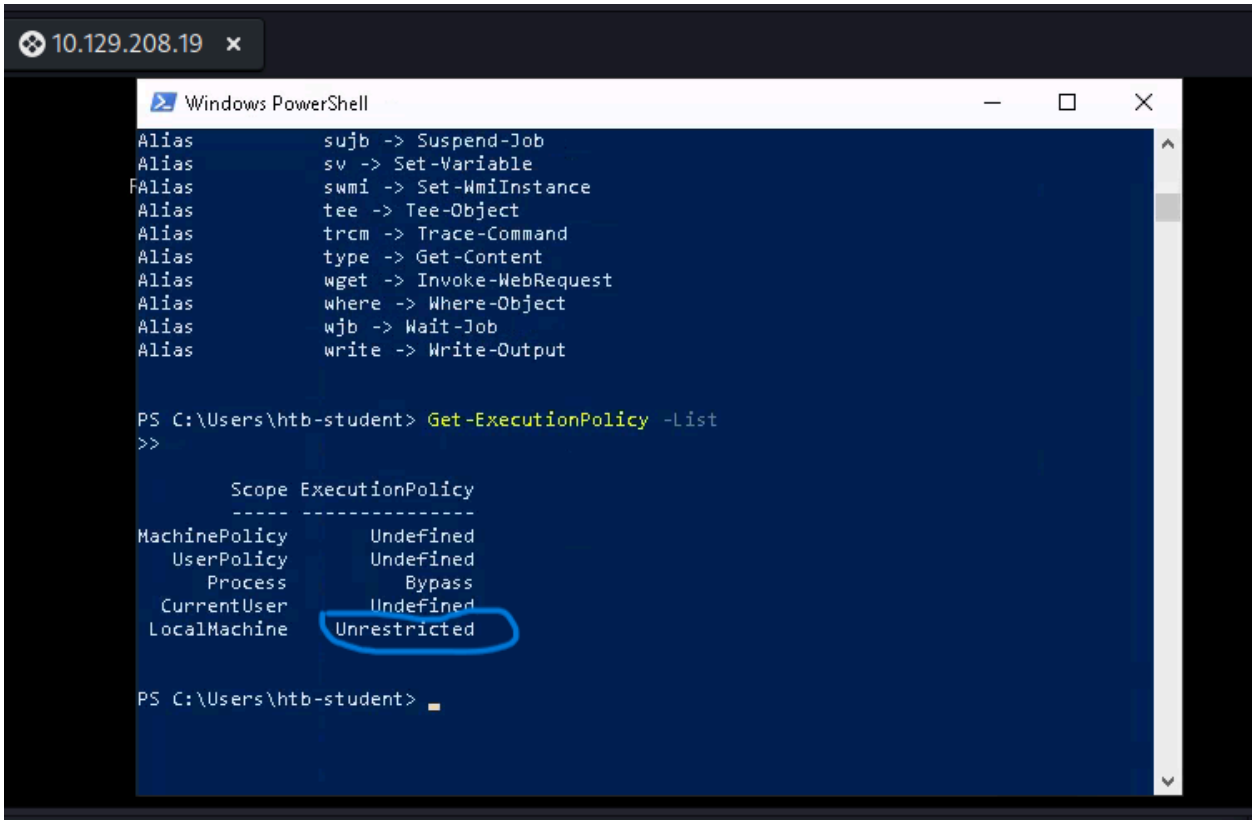
8. **Question**: Identify one of the non-standard update services running on the host. What is the full name of the service executable? **Answer**: FoxitReaderUpdateService.exe. This executable is part of a third-party application, Foxit Reader, and is not a native Windows service.



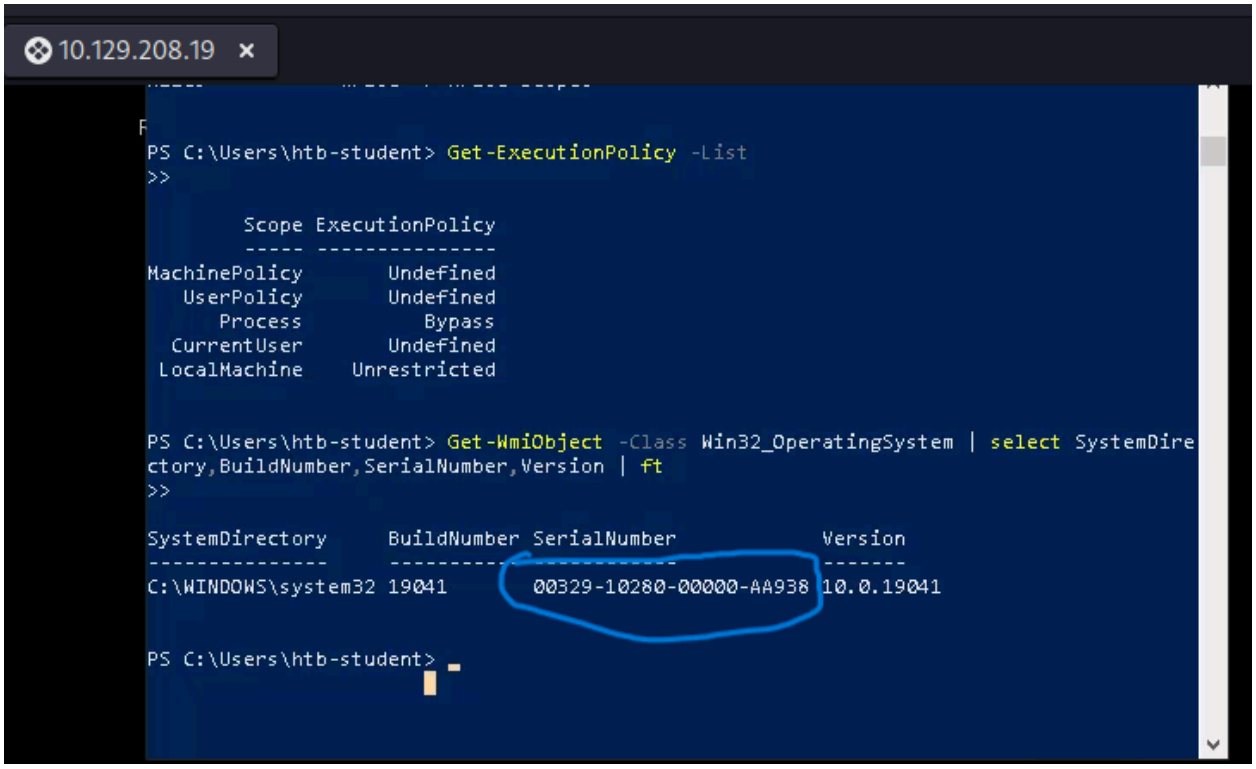
9. **Question**: What is the alias set for the ipconfig.exe command? **Answer**: ifconfig. This alias, typically used in Unix-like systems, has been set for convenience in the Windows environment.



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.



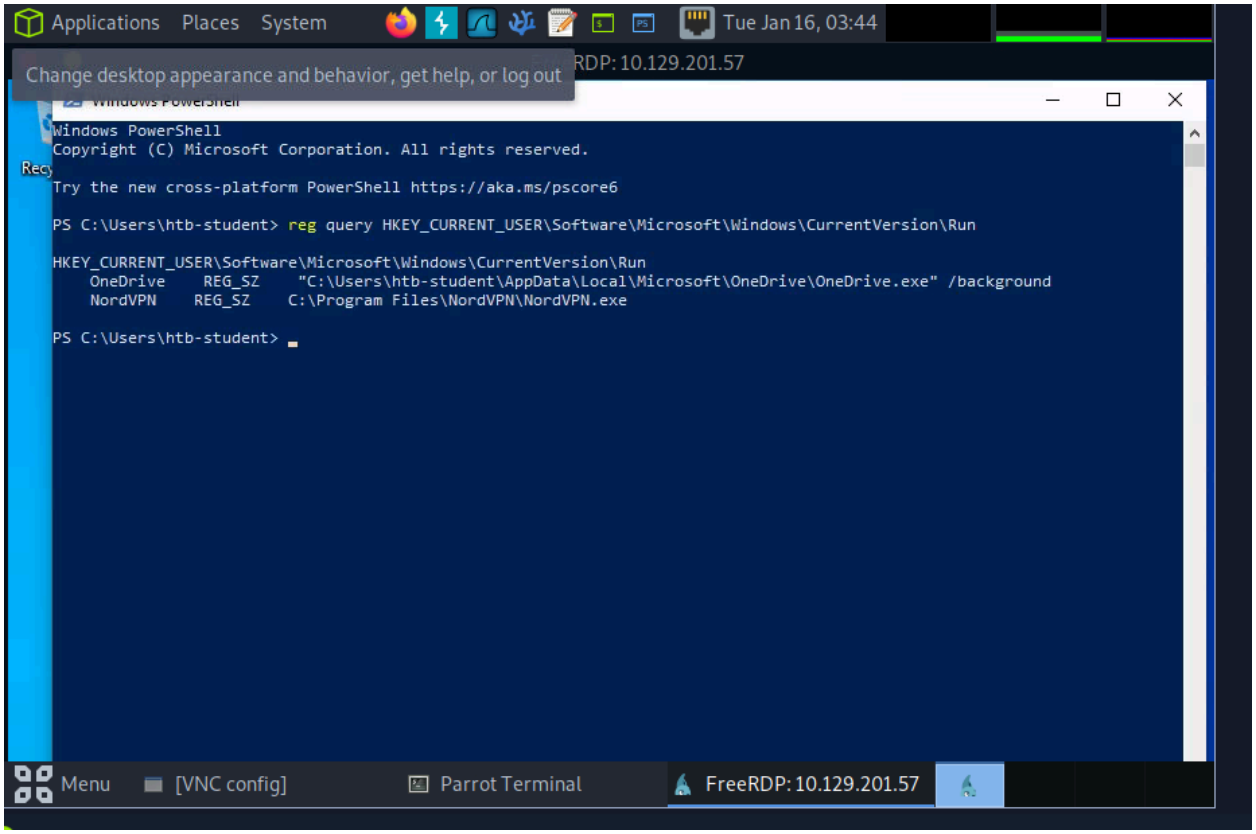
11. **Question**: Use WMI to find the serial number of the system. **Answer**: 00329-10280-00000-AA938. This serial number, unique to this system, is retrieved via Windows Management Instrumentation (WMI).



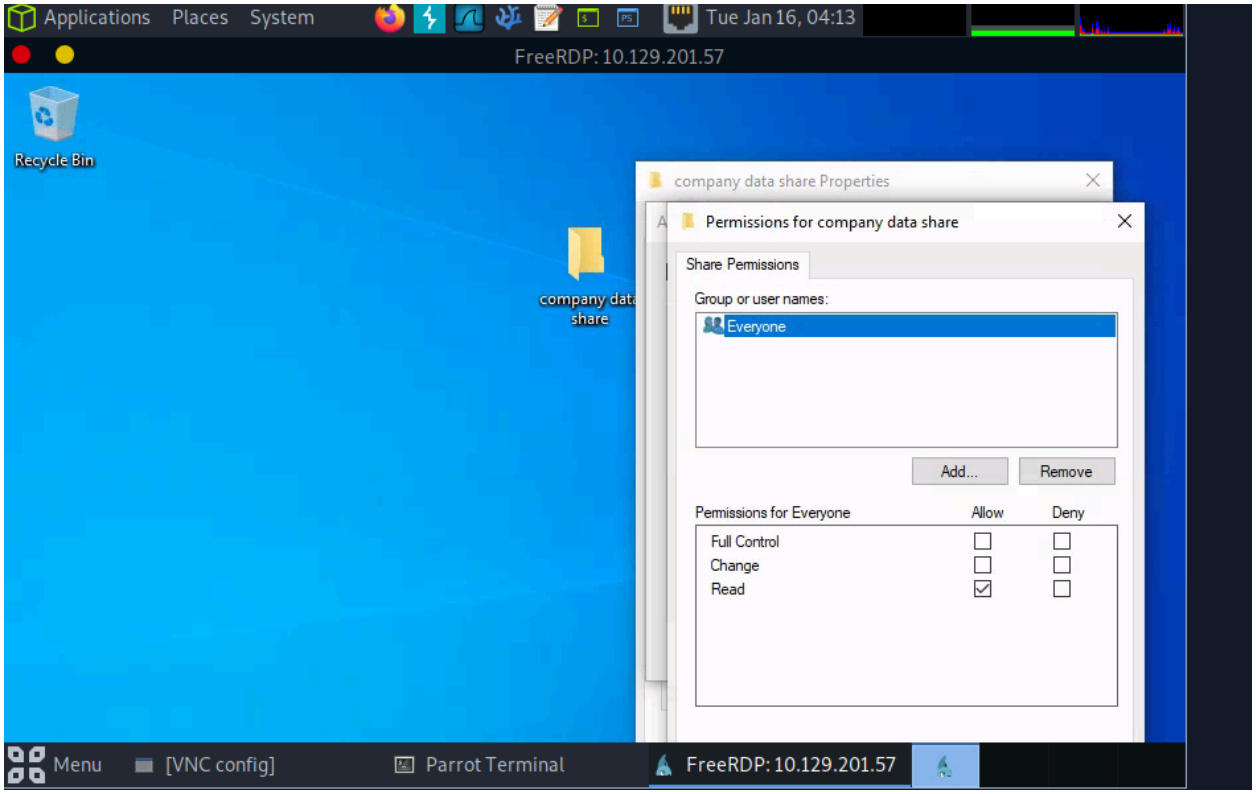
12. **Question**: Find the SID of the bob.smith user. **Answer**: S-1-5-21-2614195641-1726409526-3792725429-1003. This Security Identifier is unique to the 'bob.smith' user account in the Windows security architecture.

```
10.129.208.19 ×
(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>
```

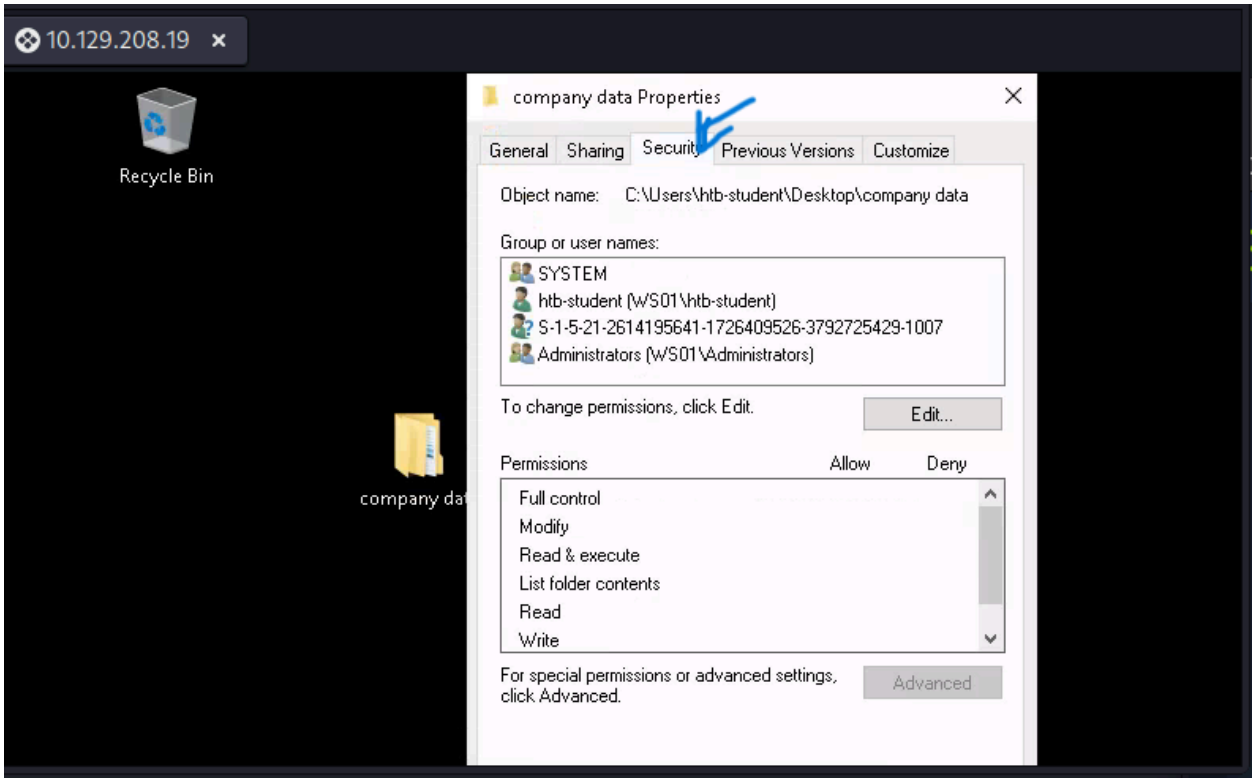
13. **Question**: What 3rd party security application is disabled at startup for the current user? **Answer**: NordVPN. This application, a VPN service provider, is disabled at startup for the current user, impacting their online security and privacy settings.



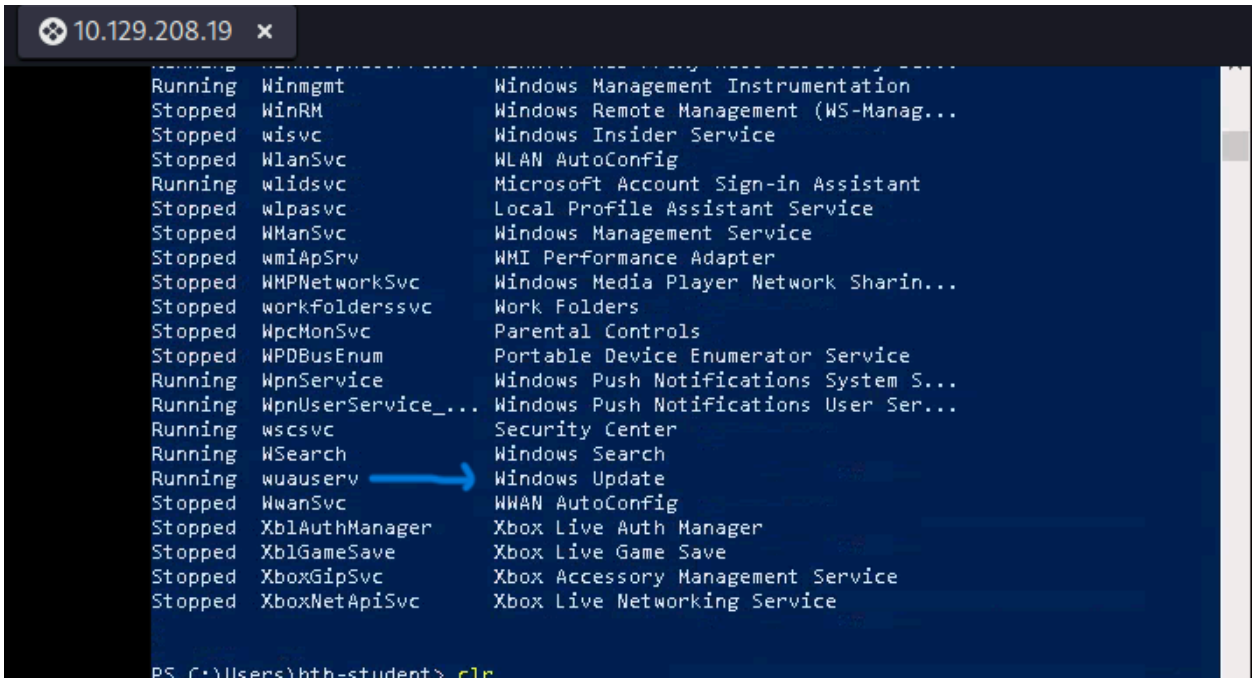
14. **Question**: What is the name of the group that is present in the Company Data Share Permissions ACL by default? **Answer**: Everyone. This default group setting in the Access Control List indicates that all users have some level of access to the Company Data Share.



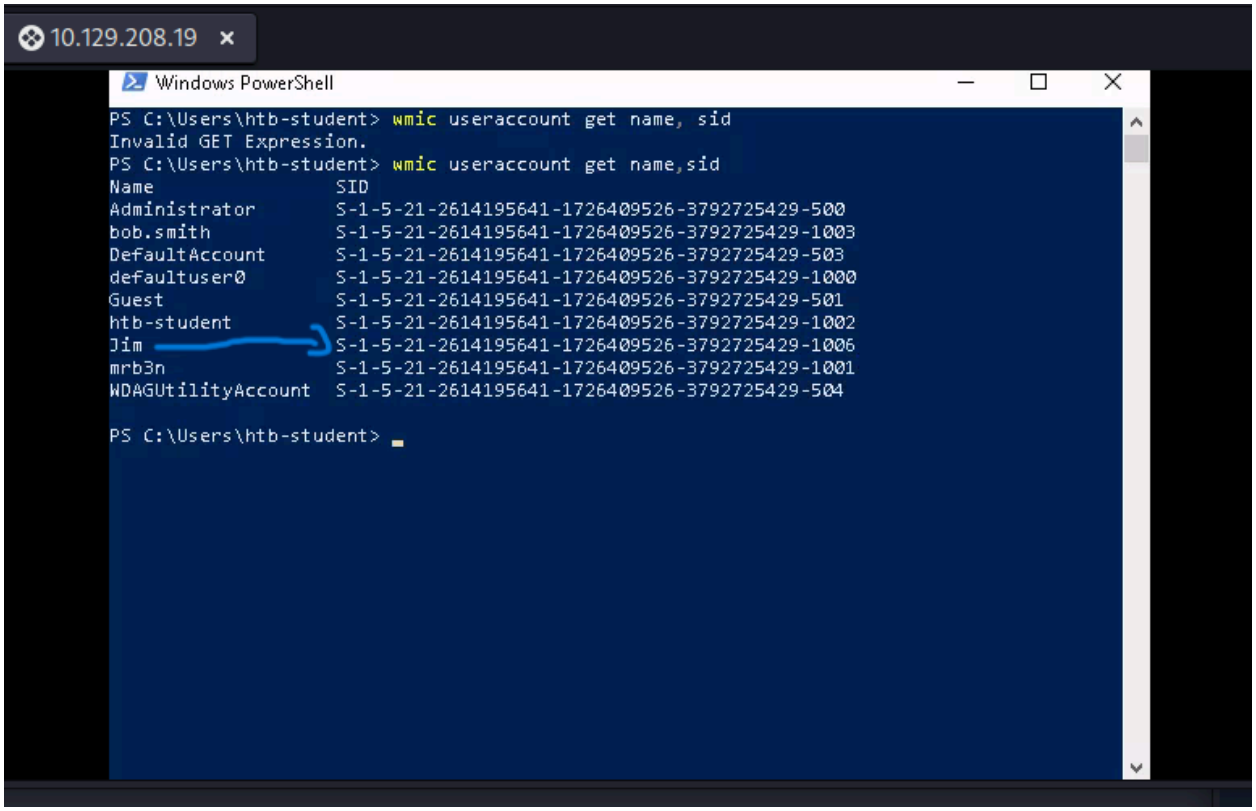
15. **Question**: What is the name of the tab that allows you to configure NTFS permissions? **Answer**: Security. This tab in Windows File Explorer is used for setting NTFS permissions, crucial for managing access to files and directories.



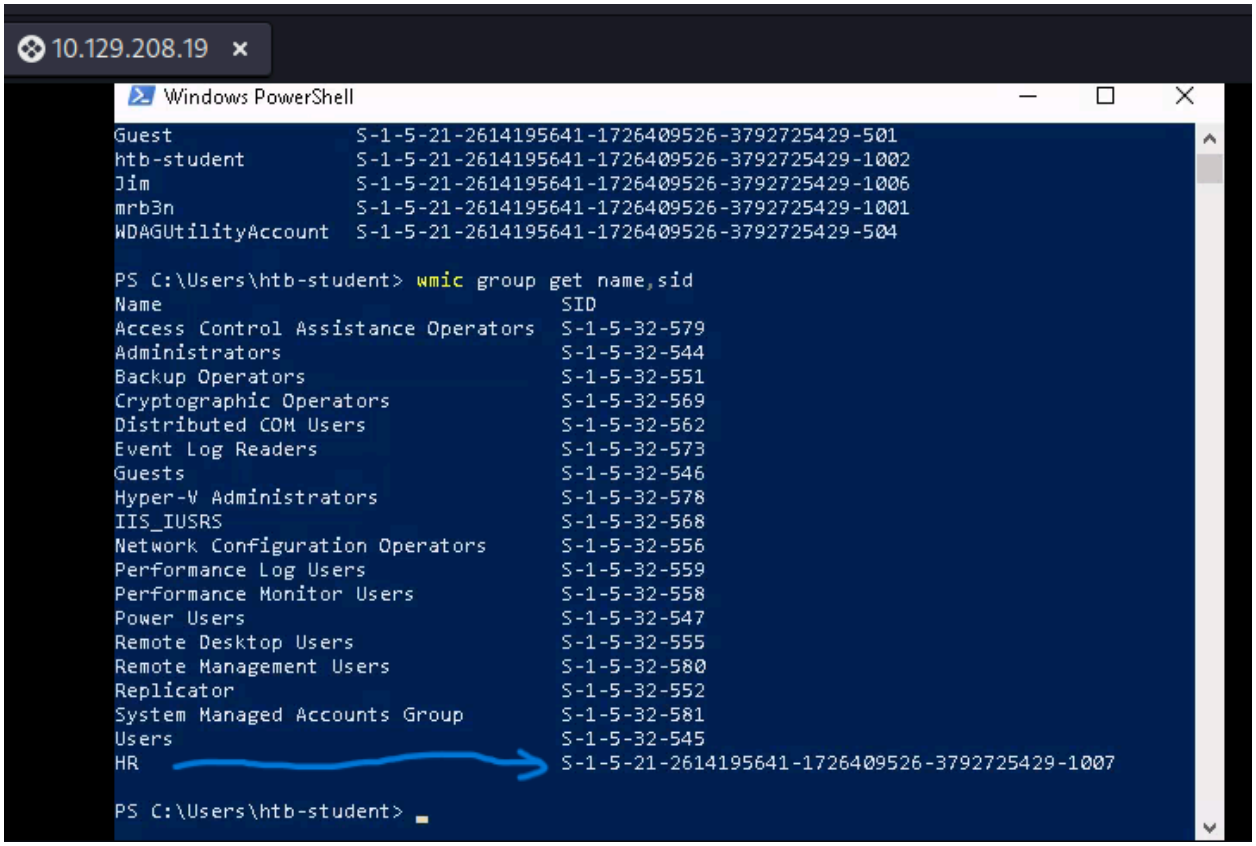
16. **Question**: What is the name of the service associated with Windows Update?
    Answer: wuauserv. The Windows Update Service (wuauserv) is responsible for managing the download and installation of updates in Windows.



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."



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.



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 Damiano254, you have completed this module!

Module: Windows Fundamentals

Difficulty: Fundamental

Exercises Completed: 18 /18

Completed at: 16 Jan 2024