# WINDOWS FUNDAMENTALS

## ASSIGNMENT REPORT


**Peter Kinyumu,**
**cs-sa07-24067,**
**May 12th, 2024.**

# 1. INTRODUCTION

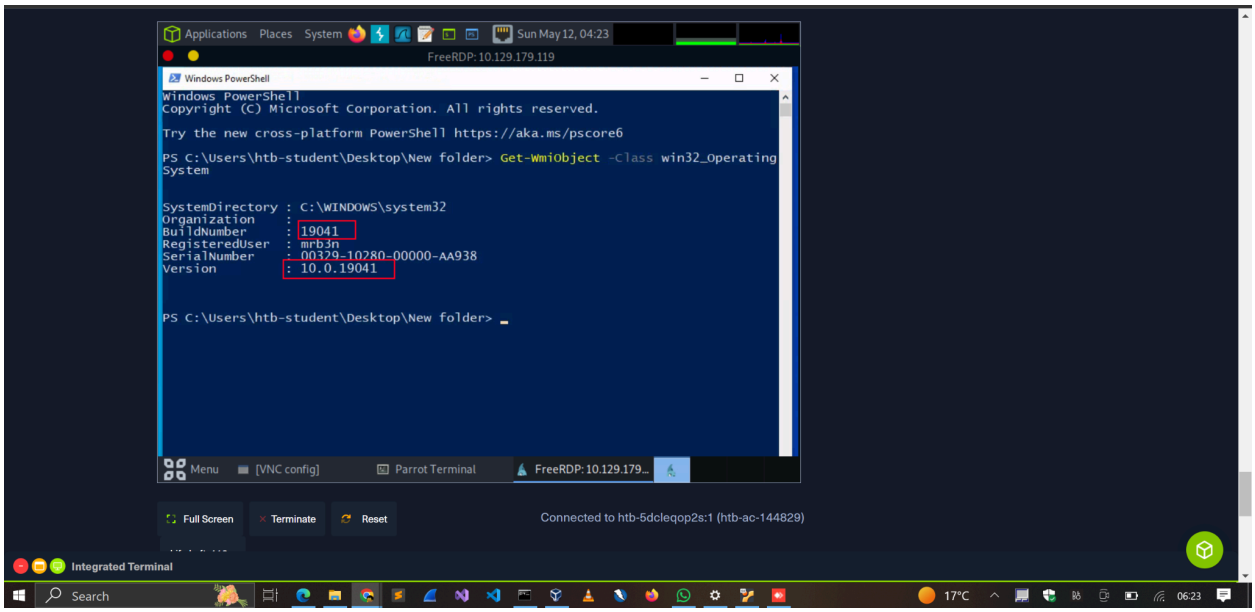
This report documents my completion of the **Windows Fundamentals** Module on the HacktheBox platform. The module covered the fundamentals required to work comfortably with the Windows operating system. It explains the Windows operating system structure and its file system, processes management, windows services and security.

Windows is heavily used across corporate environments of all sizes. As security analysts, we will be gaining access to Windows systems, and it's important to understand how to navigate and even perform privilege escalation. That all starts with grasping the essentials.

# 2. ANSWERS TO QUESTIONS

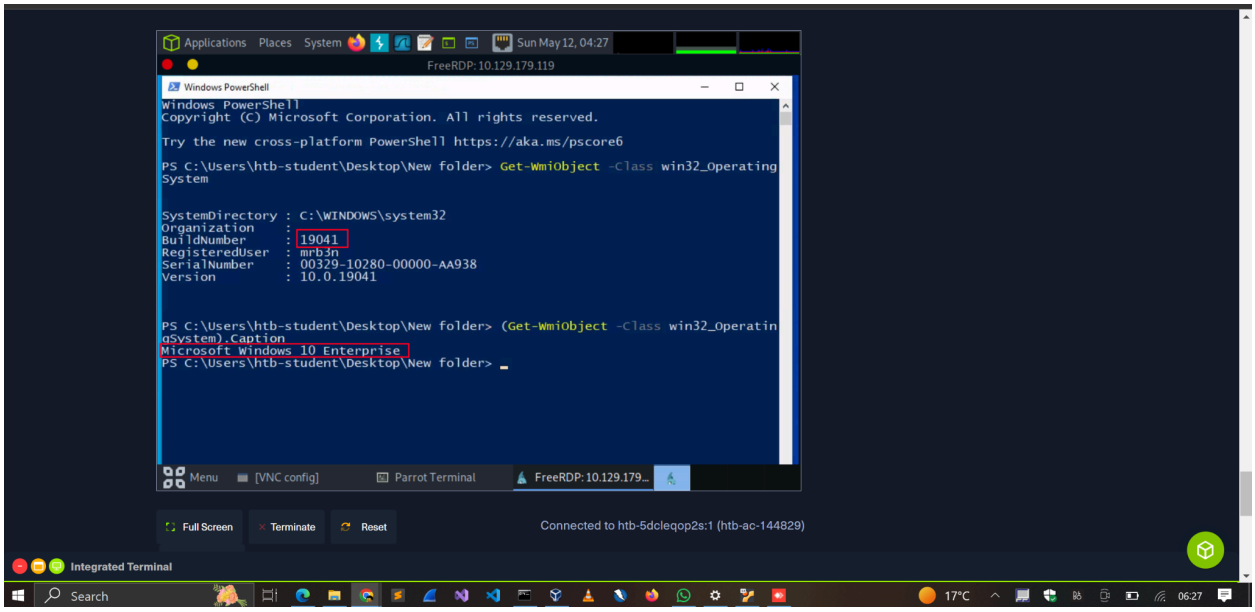
## Introduction to windows

**a. What is the Build Number of the target workstation?**




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

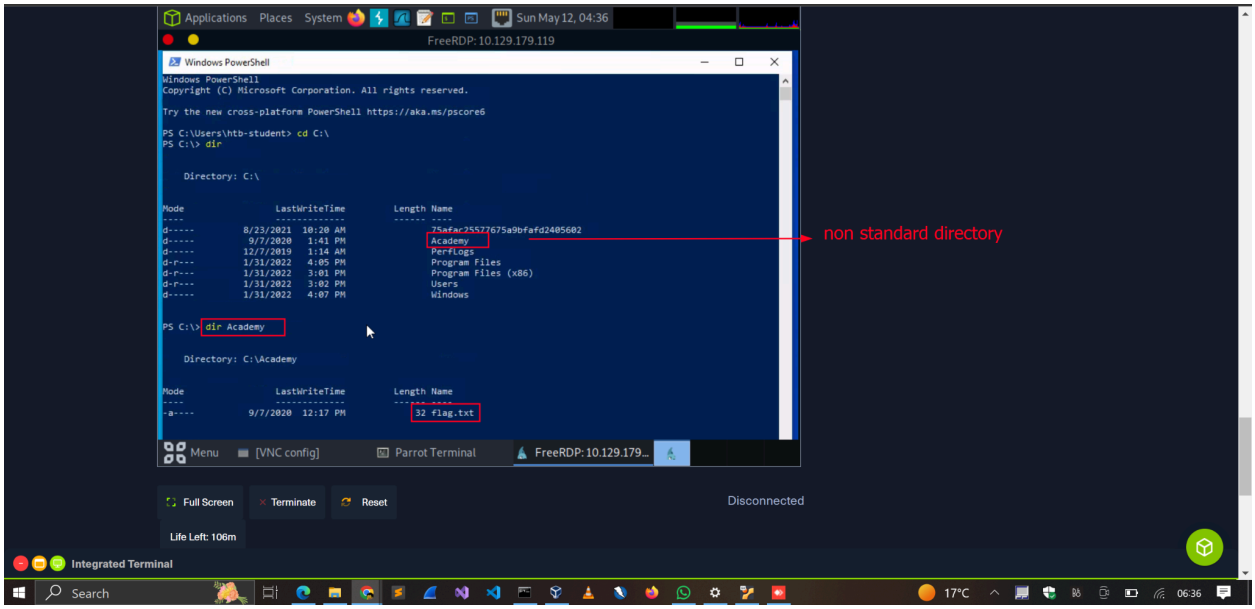
We can note from the command output that it is a Windows 10 operating system.



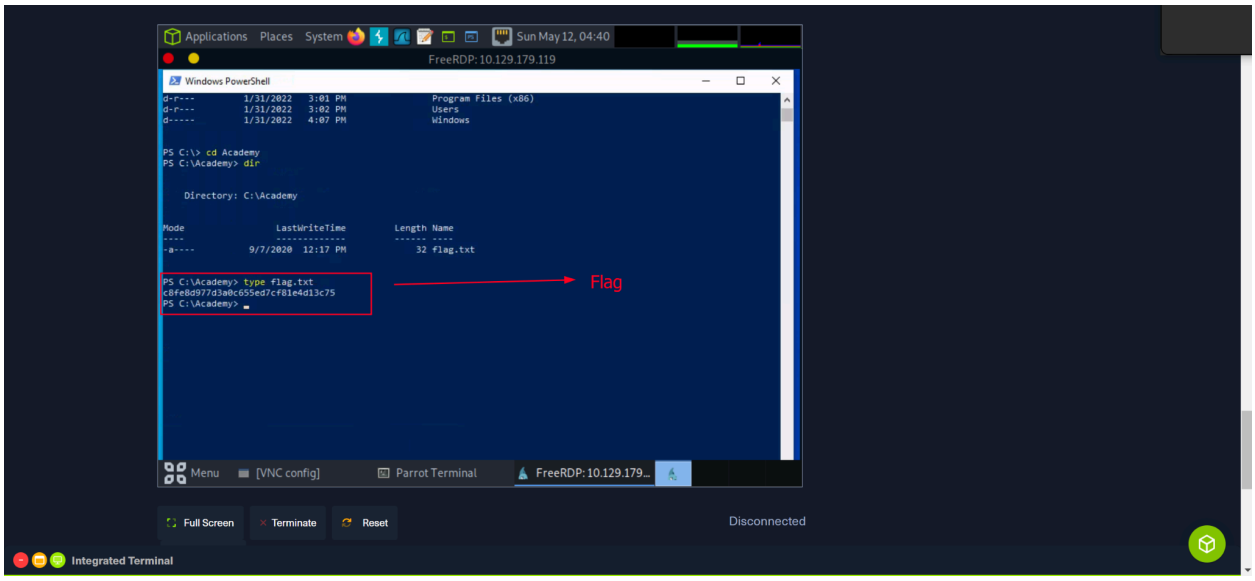

## Core of the Operating System

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

The Academy directory is non-standard to be in C drive. When we view its contents we identify ba file named “flag”.

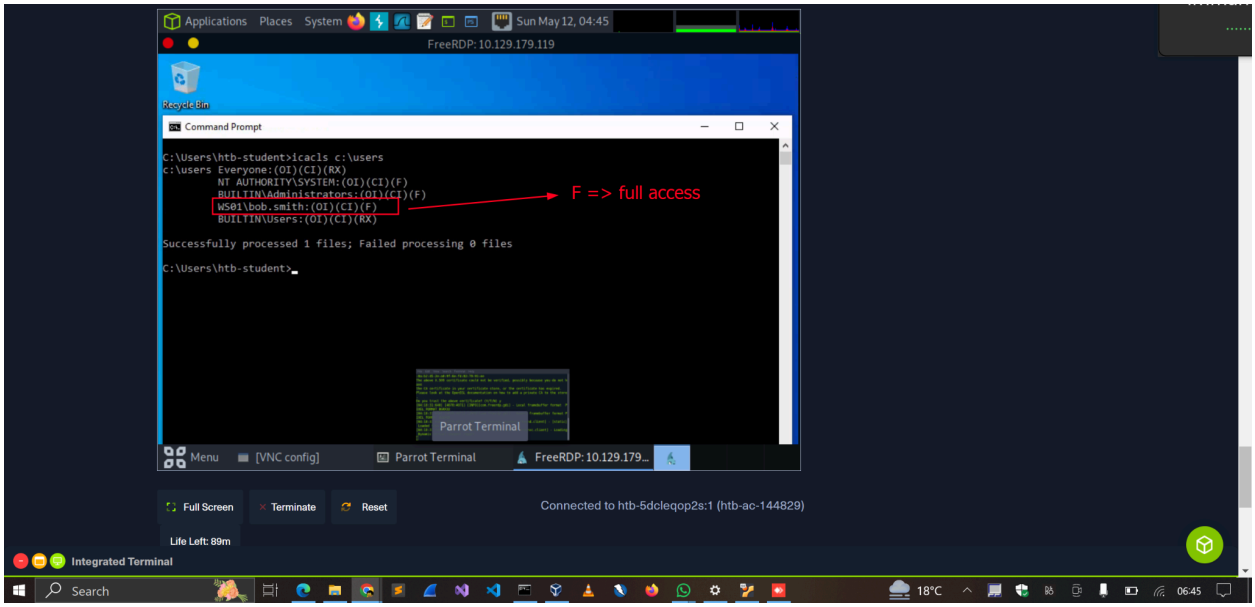



Printing out the contents of the file unveils the answer to the question.




**b. What system user has full control over the c:\users directory?**

The **icacls** command displays or modifies discretionary access control lists (DACLs) on specified files and applies stored DACLs to files in specified directories. When we display the DACLs on C:\Users we can see that **bob.smith** has Full access(F) over the directory.



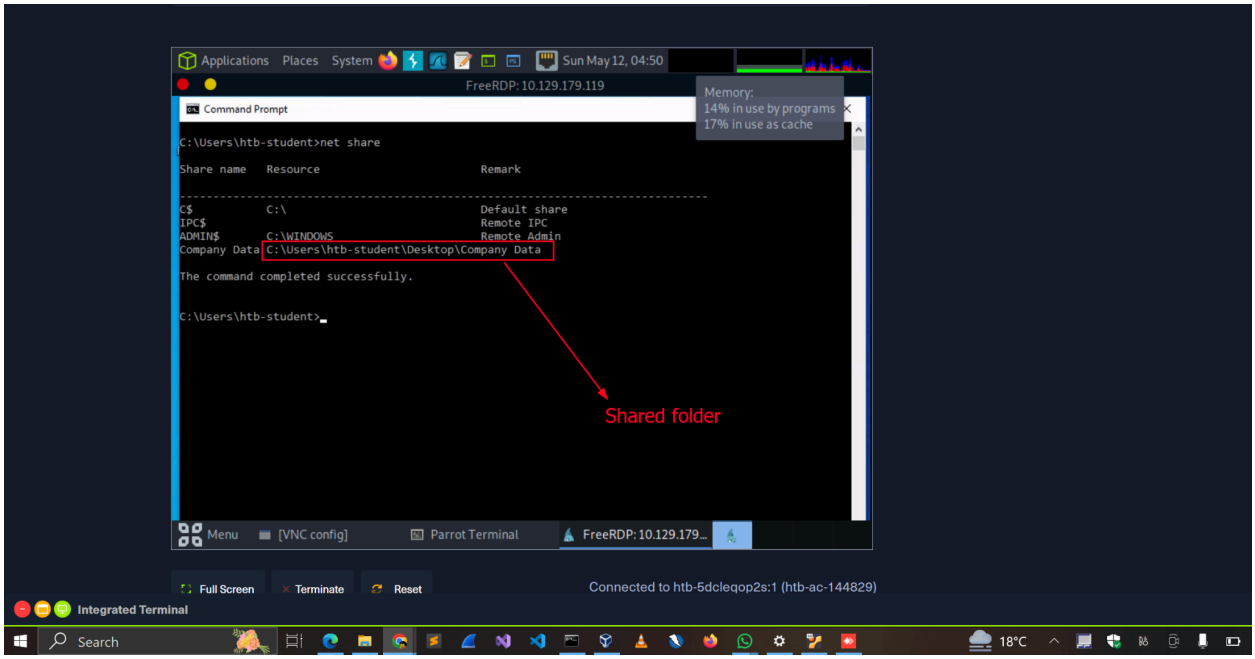

**c. What protocol discussed in this section is used to share resources on the network using Windows (Format: case sensitive)**

SMB

**d. What is the name of the utility that can help to view logs made by Windows system? (Format: 2 words, 1 space, not case sensitive)**

Event Viewer

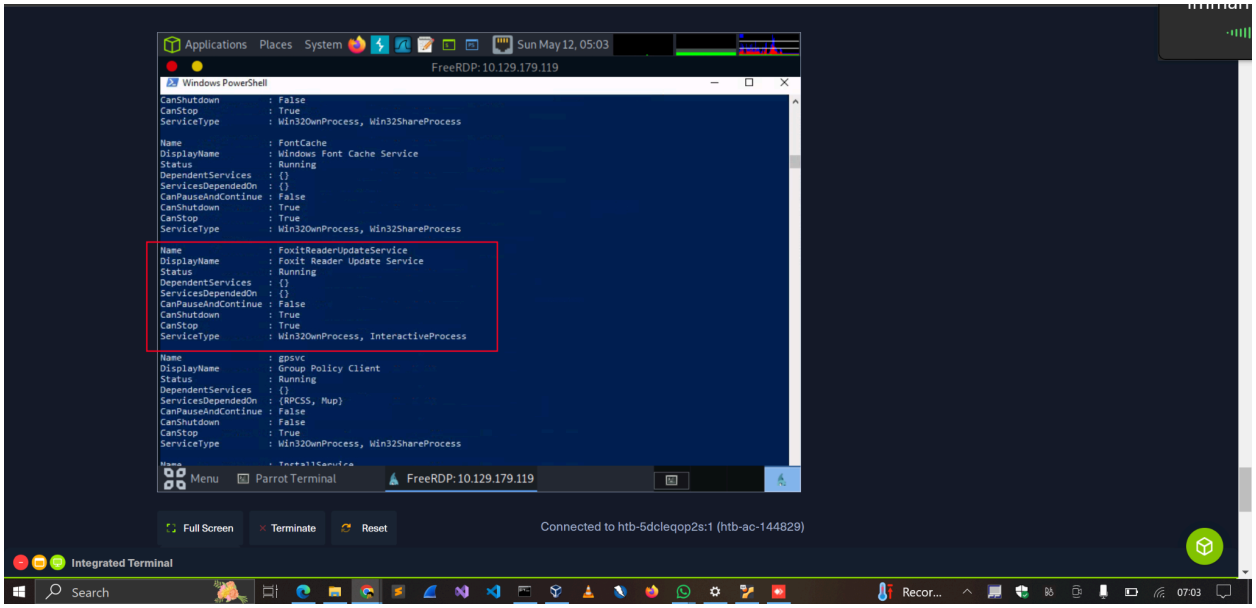
e. **What is the full directory path to the Company Data share we created?**
The **net share** command allows us to list all shared folders within the workstation.




## Working with services and processes

a. **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.**

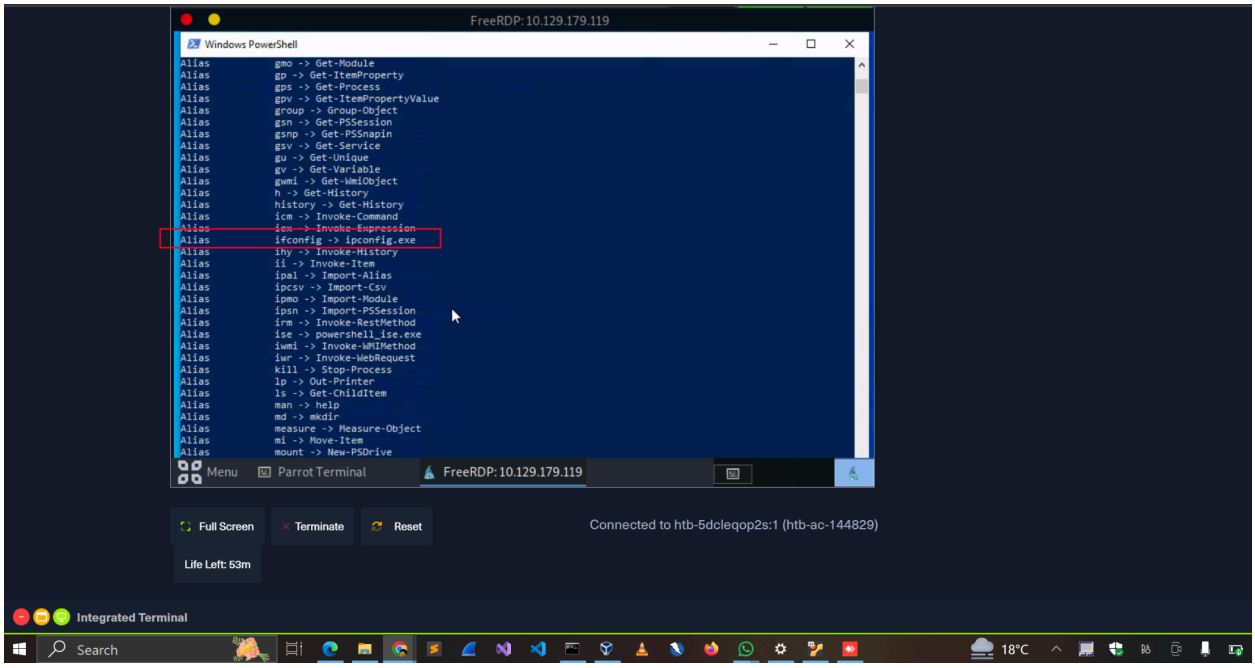
We can query all services using the following PowerShell cmdlet `Get-Service | ? {$_.Status -eq "Running"}`
We note an unusual update service with named **FoxitReaderUpdateService.exe**




## Interacting with Windows

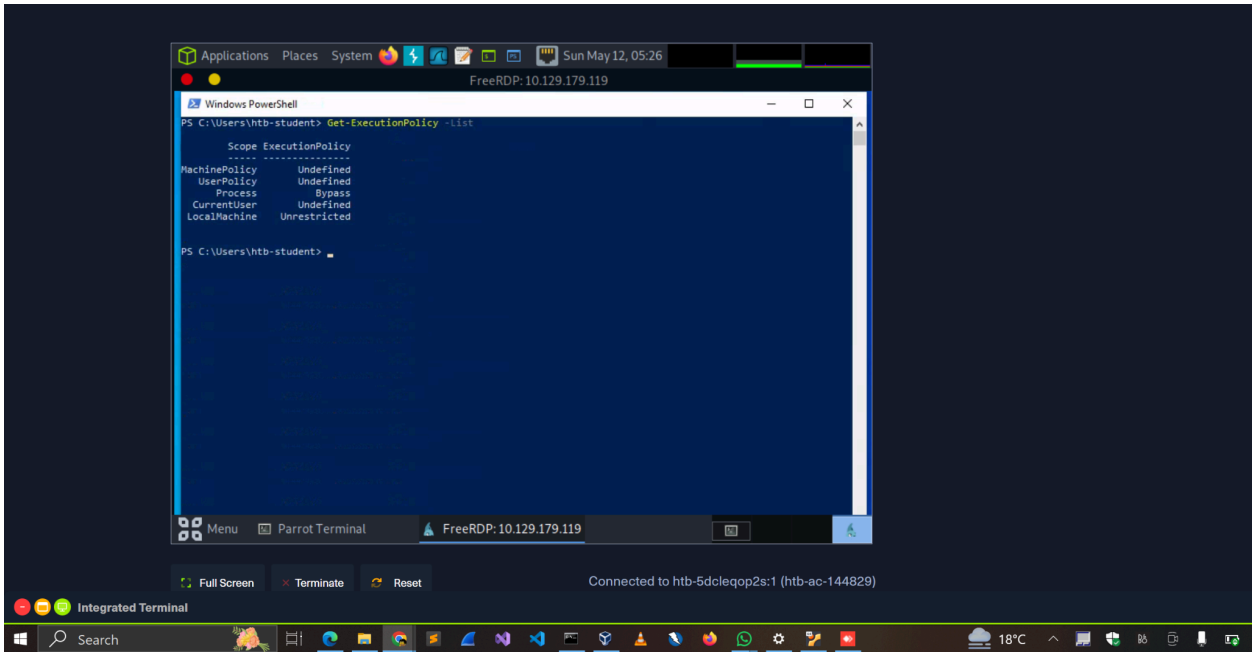
**a. What is the alias set for the ipconfig.exe command?**

The PowerShell command **get-alias** displays all aliases for all commands and cmdlets.

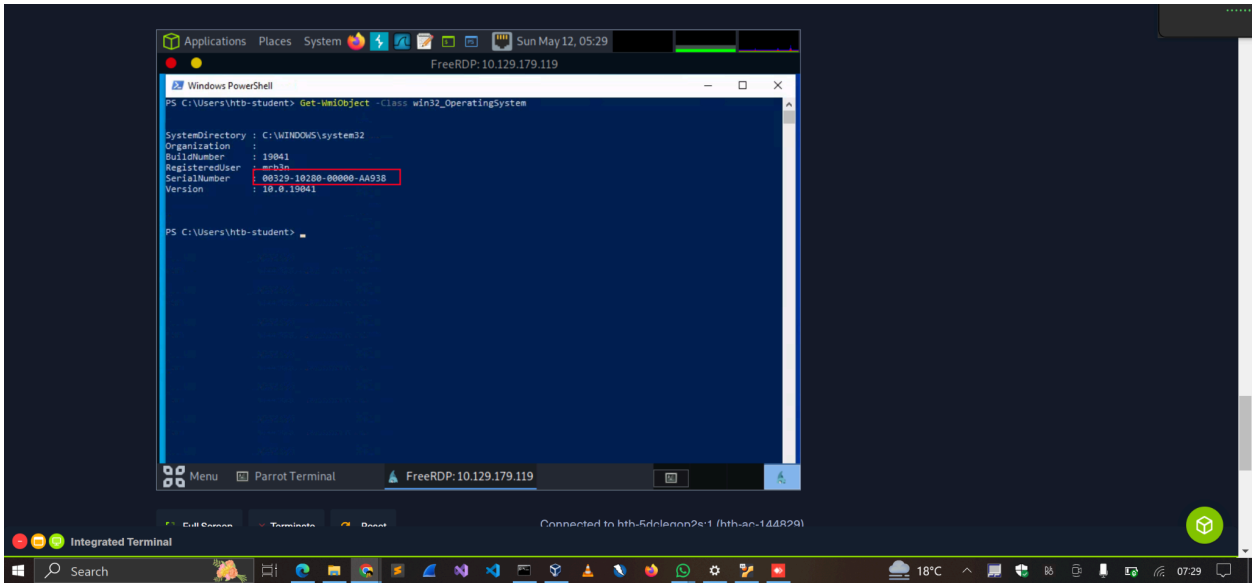



**b. Find the Execution Policy set for the LocalMachine scope.**

From the screenshot below, the execution policy of the LocalMachine is set to unrestricted.



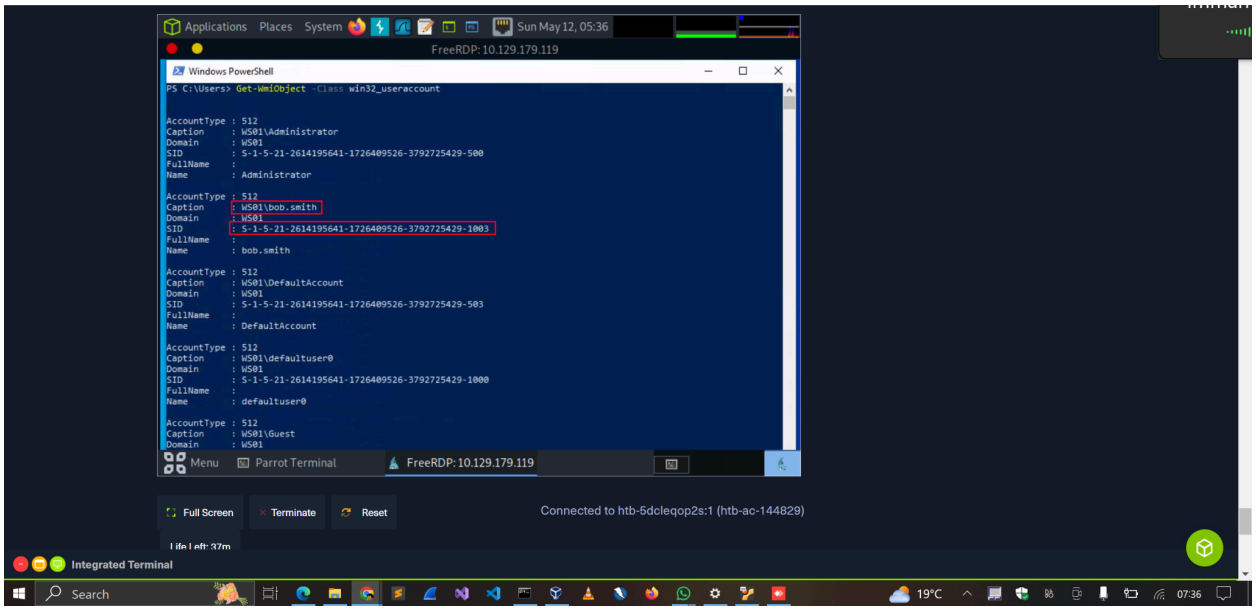

**c. Use WMI to find the serial number of the system.**



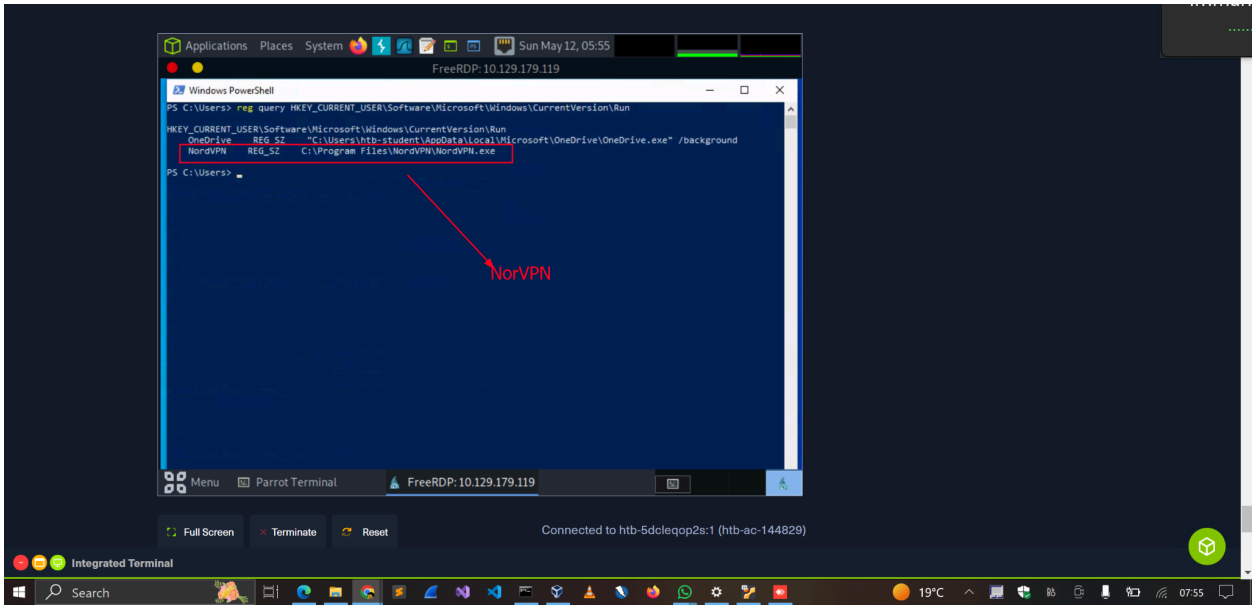

## Windows Security

**a. Find the SID of the bob.smith user.**

We can retrieve the SID of any user using the **Get-WmiObject** cmdlet by specifying the **win32_useraccount** class.

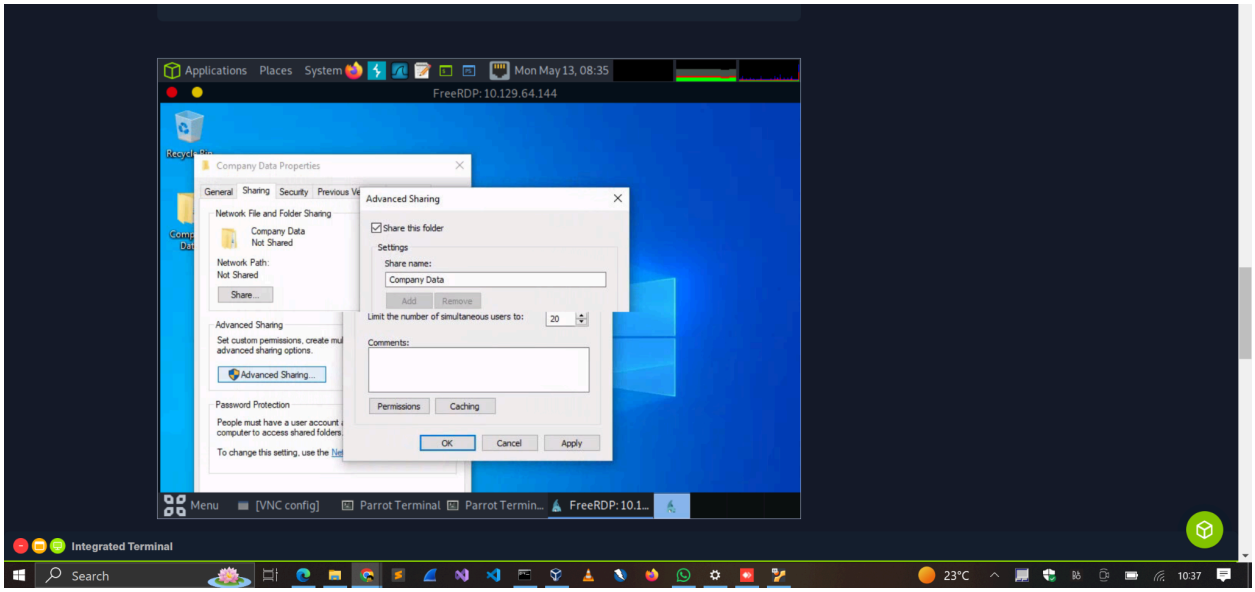



**b. What 3rd party security application is disabled at startup for the current user? (The answer is case sensitive).**

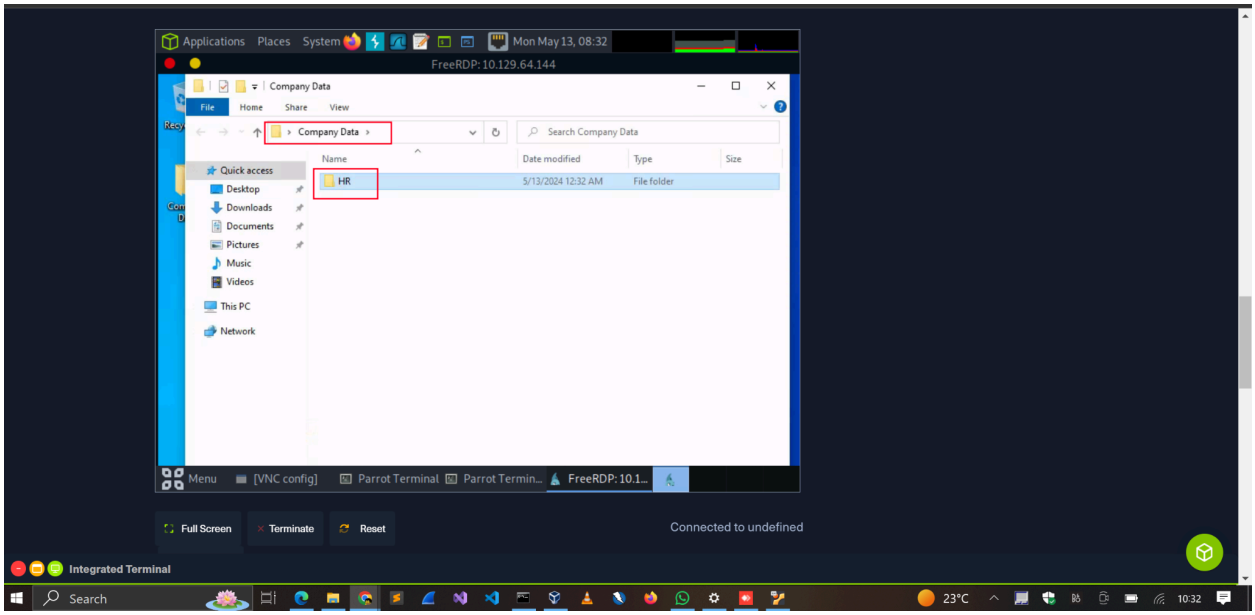


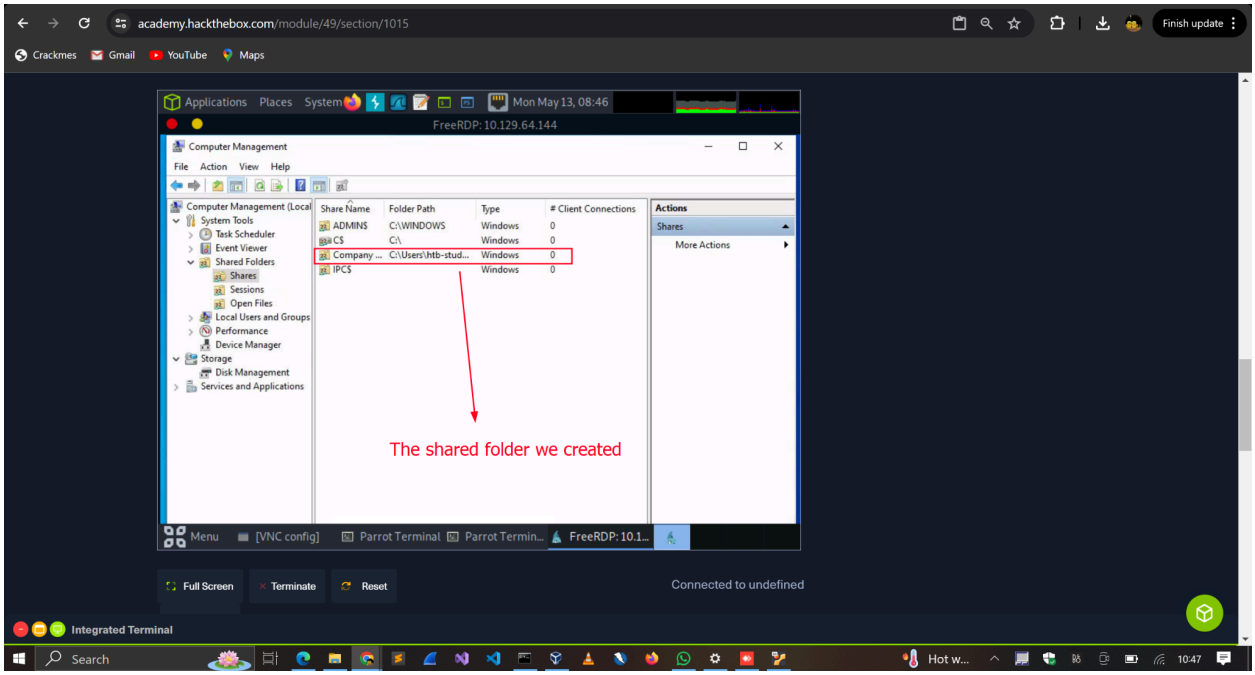

# Skills Assessment

1. **Creating a shared folder called Company Data**

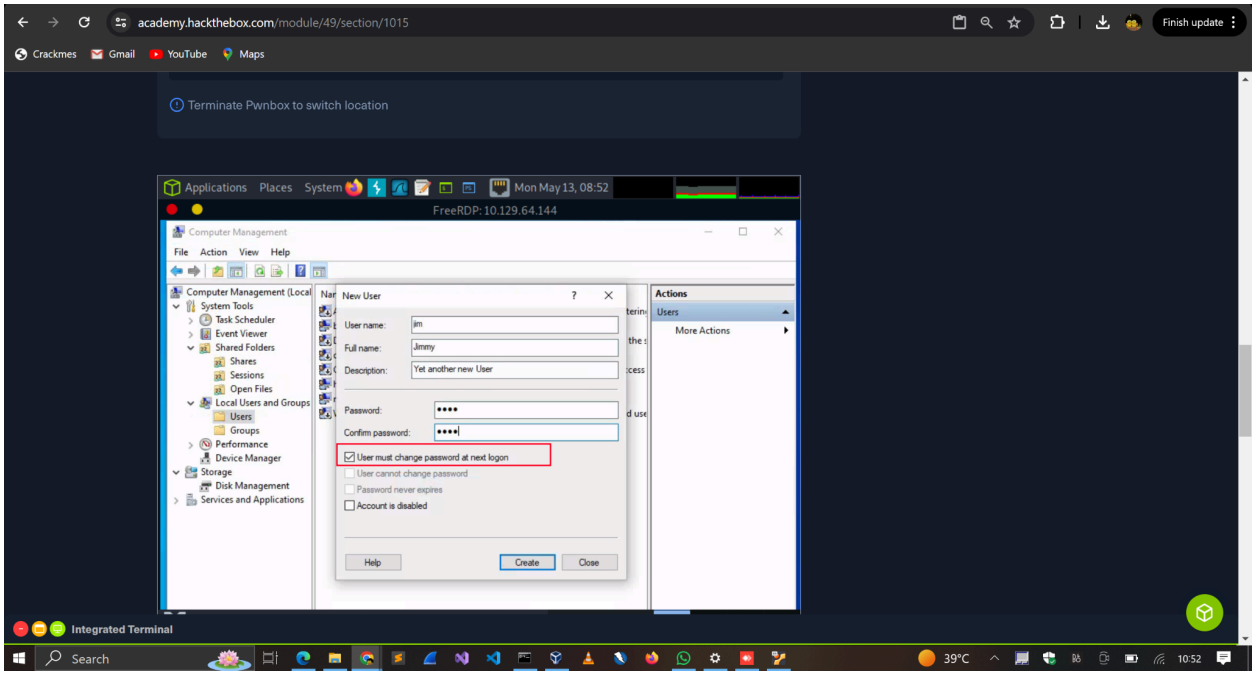



2. **Creating a subfolder called HR inside of the Company Data folder**

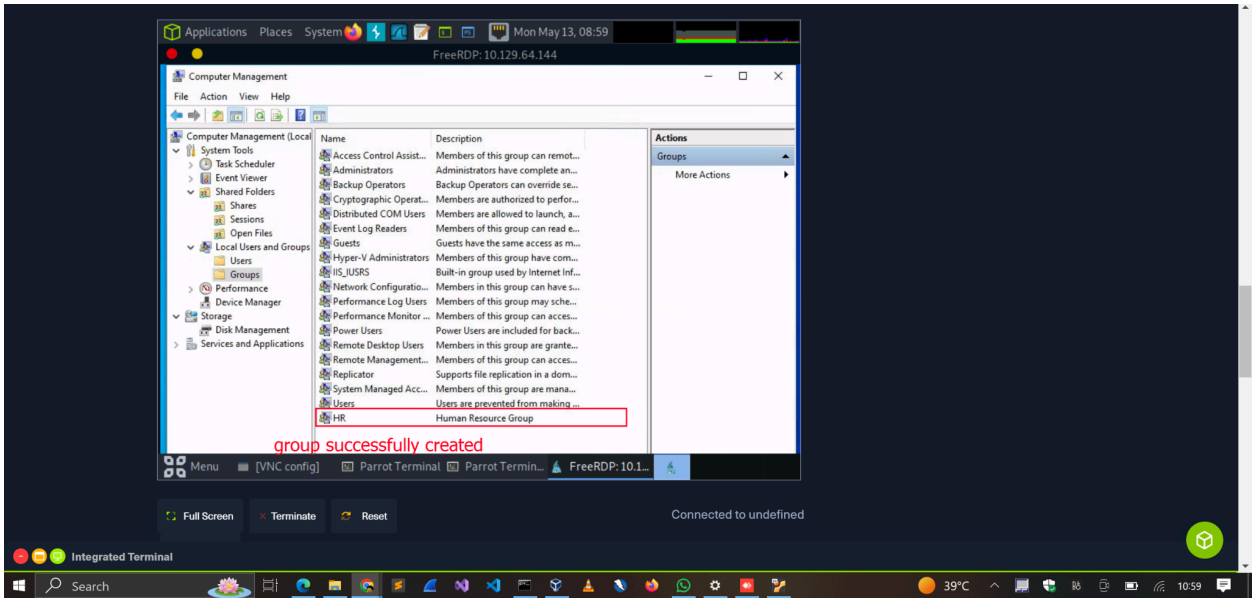





3. **Creating a user called Jim Uncheck: User must change password at logon**

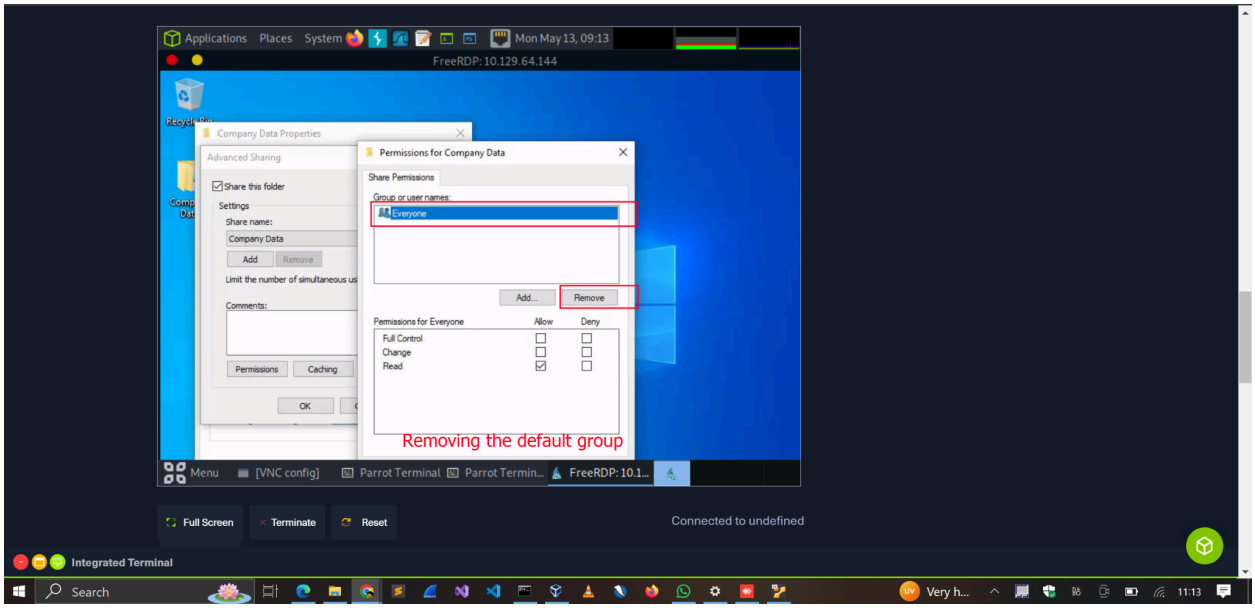


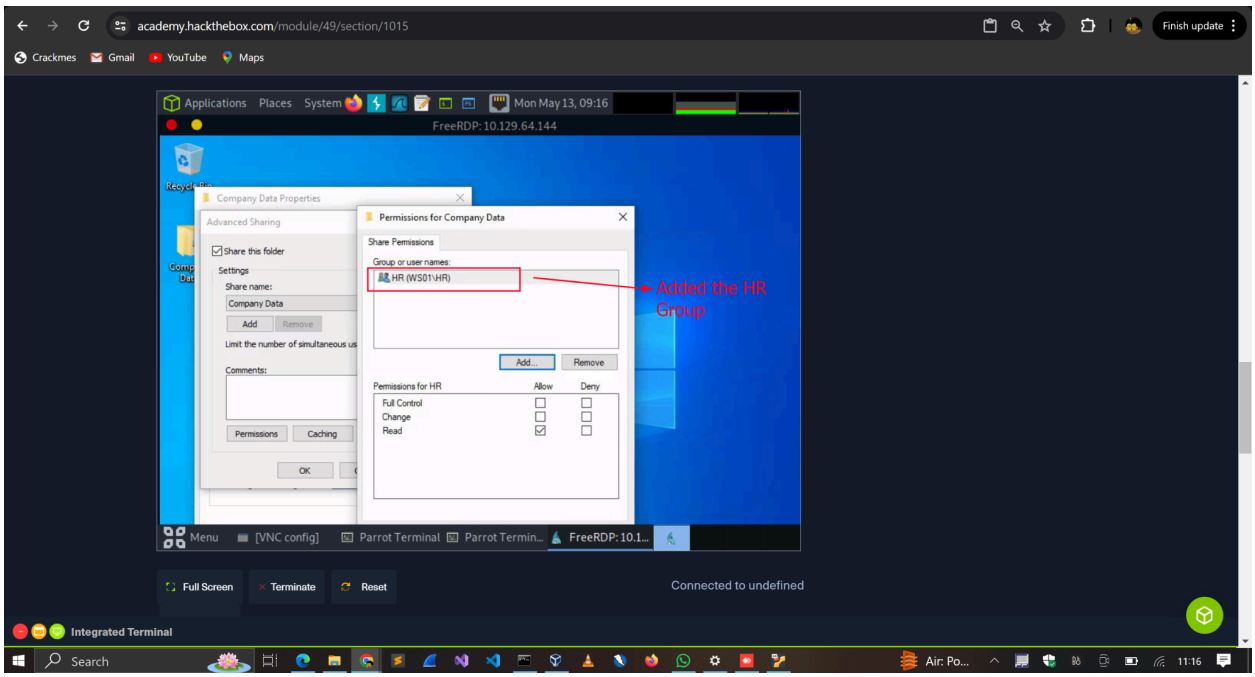

4. **Creating a security group called HR**
5. **Adding Jim to the HR security group**

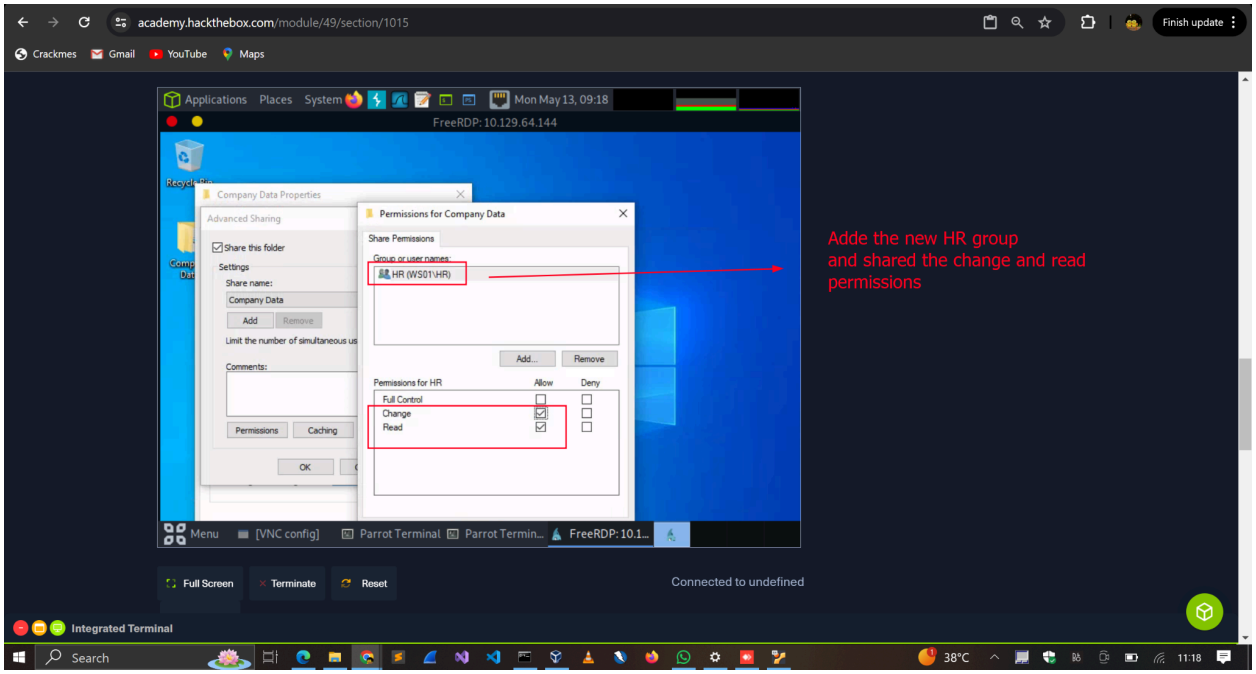


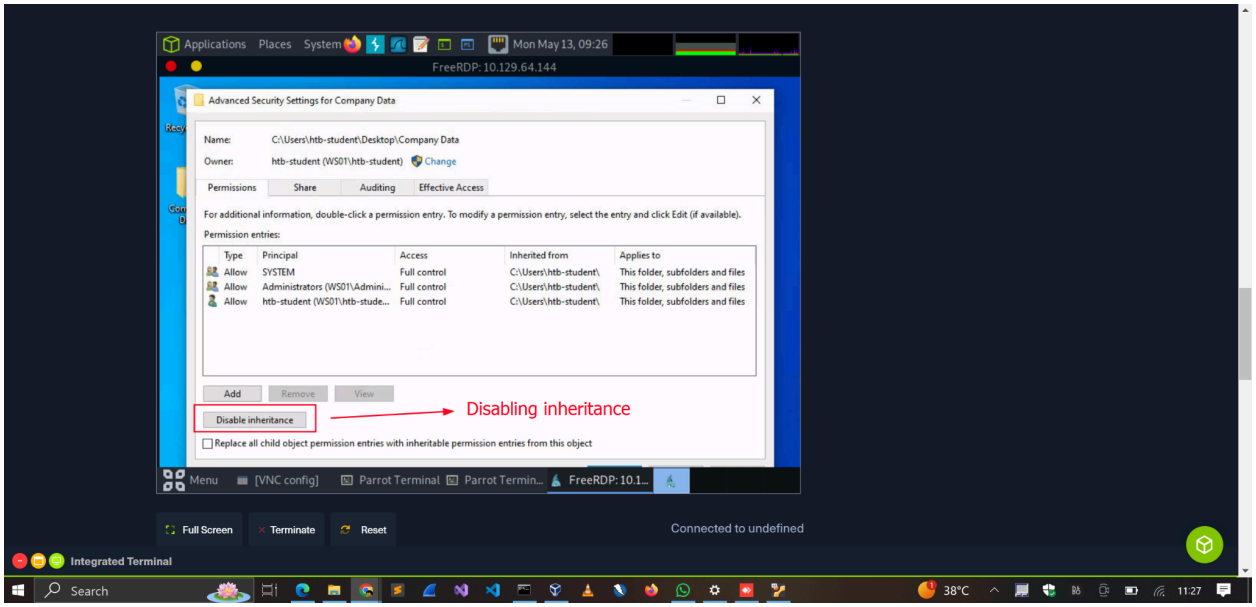

6. **Adding the HR security group to the shared Company Data folder and NTFS permissions list Remove the default group that is present Share Permissions: Allow Change & Read Disable Inheritance before issuing specific NTFS permissions NTFS permissions: Modify, Read & Execute, List folder contents, Read, Write**

7. **Adding the HR security group to the NTFS permissions list of the HR subfolder Remove the default group that is present Disable Inheritance before issuing specific NTFS permissions NTFS permissions: Modify, Read & Execute, List folder contents, Read, and Write**


Applications Places System
Mon May 13, 09:13
FreeRDP: 10.129.64.144
Company Data Properties
Advanced Sharing
Share this folder
Settings
Share name:
Company Data
Add
Remove
Limit the number of simultaneous us
Comments:
Permissions
Caching
OK
Permissions for Company Data
Share Permissions
Group or user names:
Everyone
Add...
Remove
Permissions for Everyone
Allow
Deny
Full Control
Change
Read
Removing the default group
Menu
[VNC config]
Parrot Terminal
Parrot Termin...
FreeRDP: 10.1...
Full Screen
Terminate
Reset
Connected to undefined
Integrated Terminal
Search
Very h...
11:13

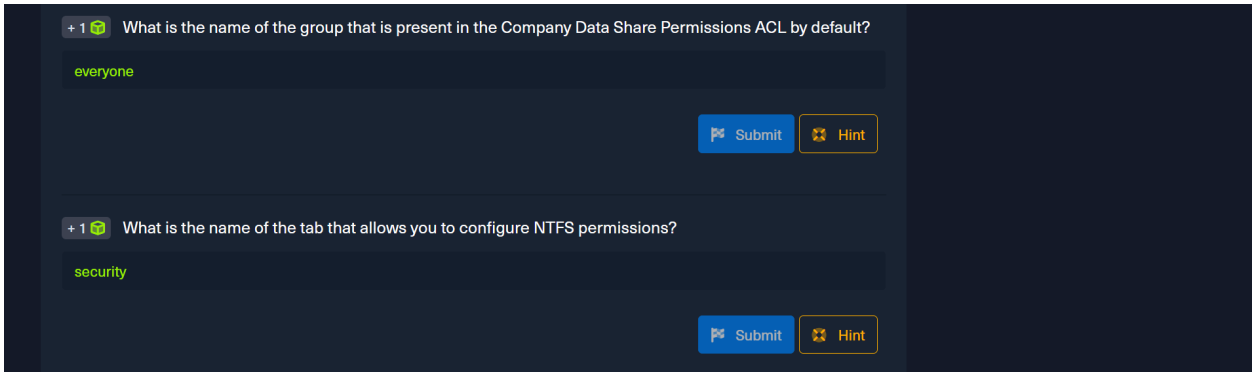

academy.hackthebox.com/module/49/section/1015
Finish update
Crackmes
Gmail
YouTube
Maps
Applications Places System
Mon May 13, 09:16
FreeRDP: 10.129.64.144
Company Data Properties
Advanced Sharing
Share this folder
Settings
Share name:
Company Data
Add
Remove
Limit the number of simultaneous us
Comments:
Permissions
Caching
OK
Permissions for Company Data
Share Permissions
Group or user names:
HR (WS01\HR)
Added the HR Group
Add...
Remove
Permissions for HR
Allow
Deny
Full Control
Change
Read
Menu
[VNC config]
Parrot Terminal
Parrot Termin...
FreeRDP: 10.1...
Full Screen
Terminate
Reset
Connected to undefined
Integrated Terminal
Search
Air: Po...
11:16




8. **Using PowerShell to list details about a service**
   The cmdlet Get-service can be used to list details about Windows services.

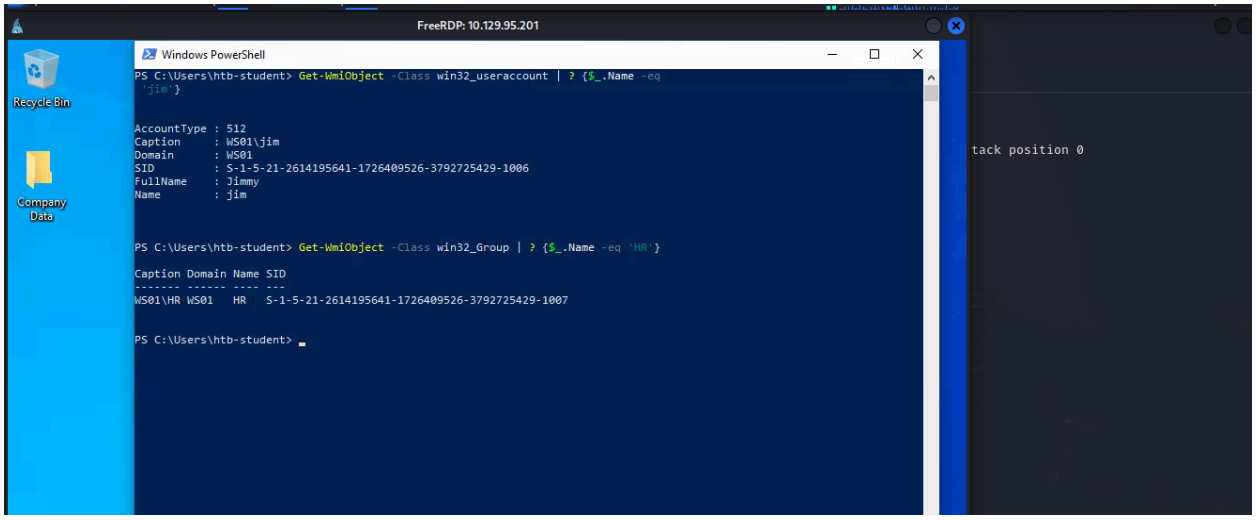
From the skills assessment above, I could answer the questions below. By default, shared folders take the group everyone.
Under Folder Properties > Security, we can configure NTFS permissions.




**What is the name of the service associated with windows Update?**

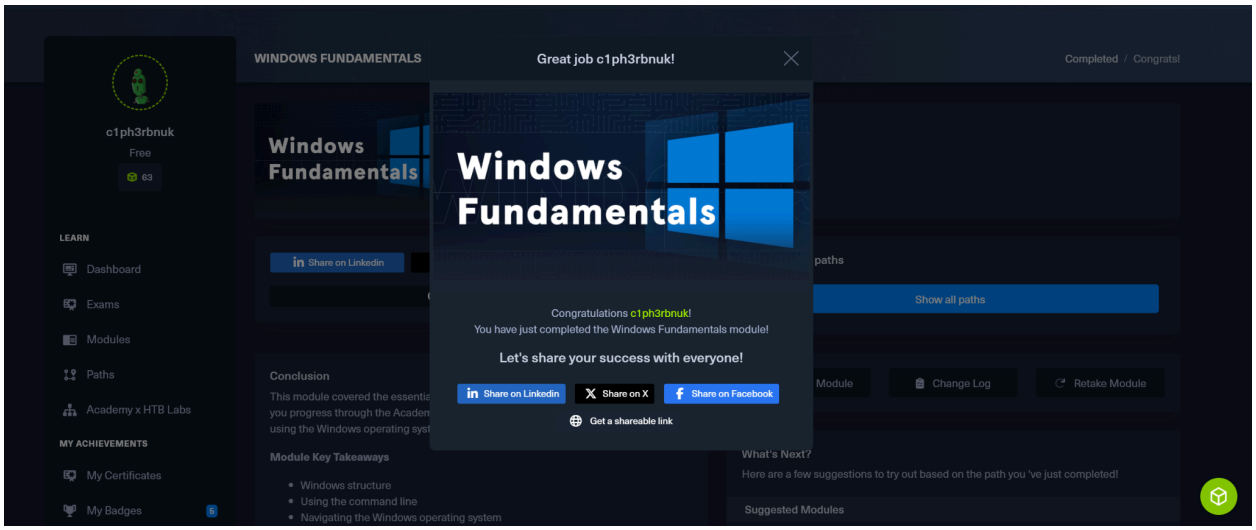
The wuauserv, which stands for (Windows update service), is a system service that is associated with Windows update.

**List the SID associated with the user account Jim and the HR group you created.**



# 3. MODULE COMPLETION

The following is a sharable link to the badge I earned after completing the module.




https://academy.hackthebox.com/achievement/144829/49

# 4. CONCLUSION

This module has taught me about Windows administrative tools like RDP connections, Powershell cmdlets like Get-Wmi-Object and Get-Service, and the native Window's commandline. I have also learned about permissions management, service management, and Windows security features. It has been an insightful journey, and I look forward to refining and enhancing my skills in Windows, hopefully in the later chapters of the course.