

LEWIS KAMAU NDERU

lewiskamau@gmail.com / kamau2325@yahoo.com

CS-SA10-25029

Link: <https://academy.hackthebox.com/module/details/49>

WINDOWS FUNDAMENTALS HTB MODULE

INTRODUCTION

The Windows Fundamentals module is designed to provide learners with a deeper understanding of the Windows operating system, including its structure and navigation. It equips students with the foundational skills needed to interact with the OS effectively and confidently.

History:

Windows Operating System including was first introduced by Microsoft on November 20, 1985 as a graphical shell for MS-DOS which stands for Microsoft Disk Operating System (a command-line based Operating System).

Since the first roll out, Microsoft has released a number of other versions with notable improvements, the latest one being Windows 11.

Windows not only caters for casual consumers but also supports enterprise customers with the first version of Windows Server (Windows NT 3.1 Advanced Server) being released in 1993. The versions have improved over time, with addition of features IIS, Active Directory, built-in firewalls, e.t.c, and later versions from 2019 supporting Kubernetes (K8s), Linux containers and more advanced security features. The Latest version is Windows Server 2025, released in November 2024.

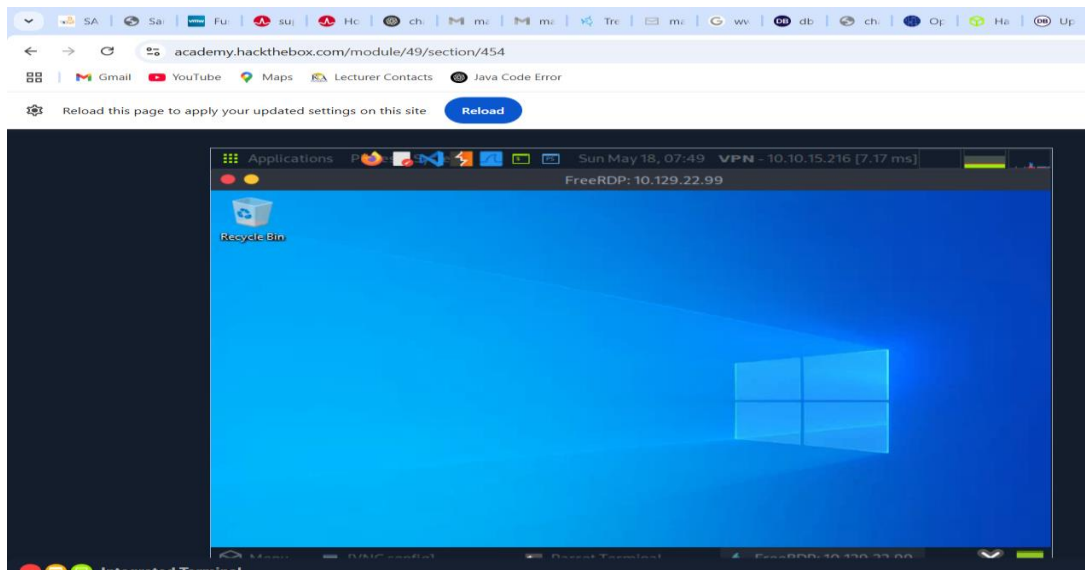
ANSWERS TO LABS

TOPIC 1: Remotely Accessing Windows Systems:

I first downloaded the ovpn file for the lab and used terminal to navigate to the Downloads folder where the file was stored and used the command *sudo openvpn filename.ovpn*.

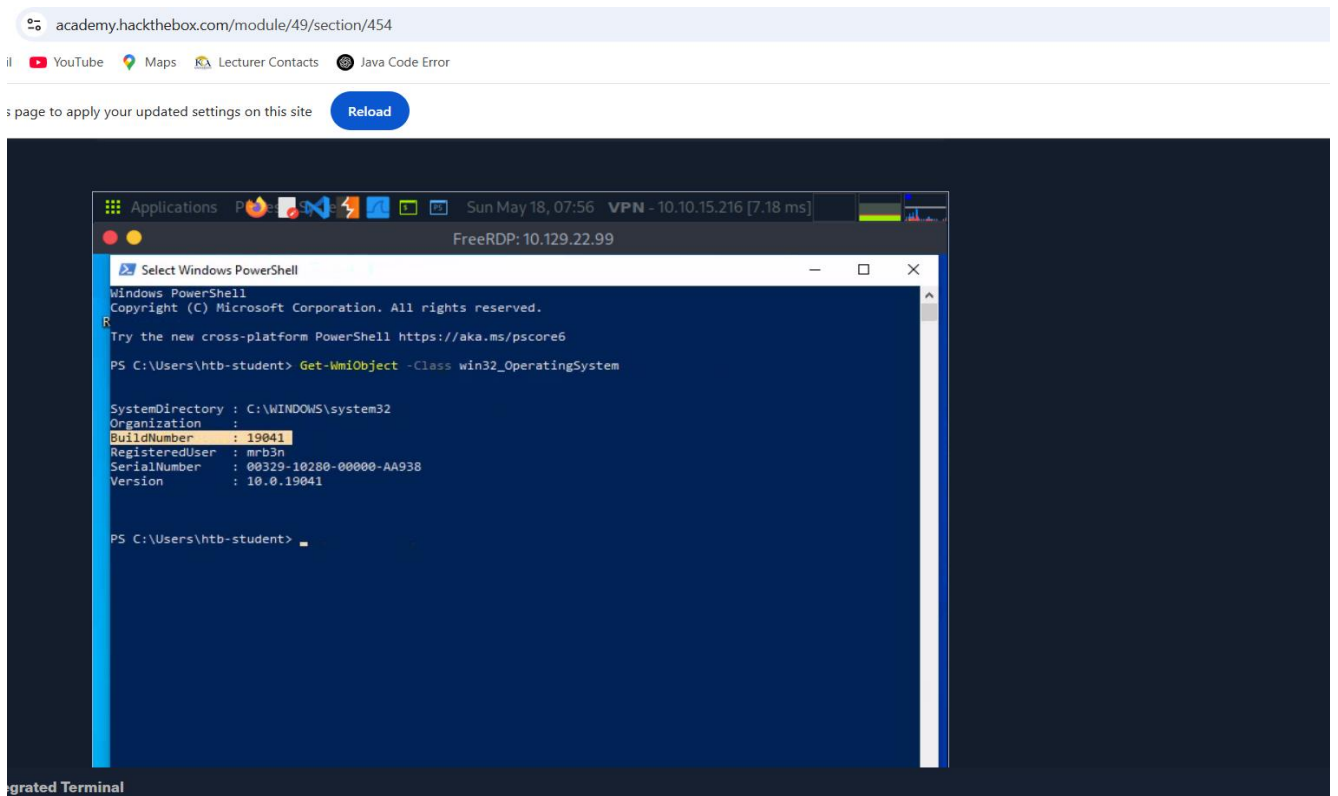
Opened another tab on the terminal and used the command *xfreerdp3 /v:box`s_ipaddress /u:name_to_our_target /p:password_to_machine*

We finally have access to our target as shown in the snippet below:

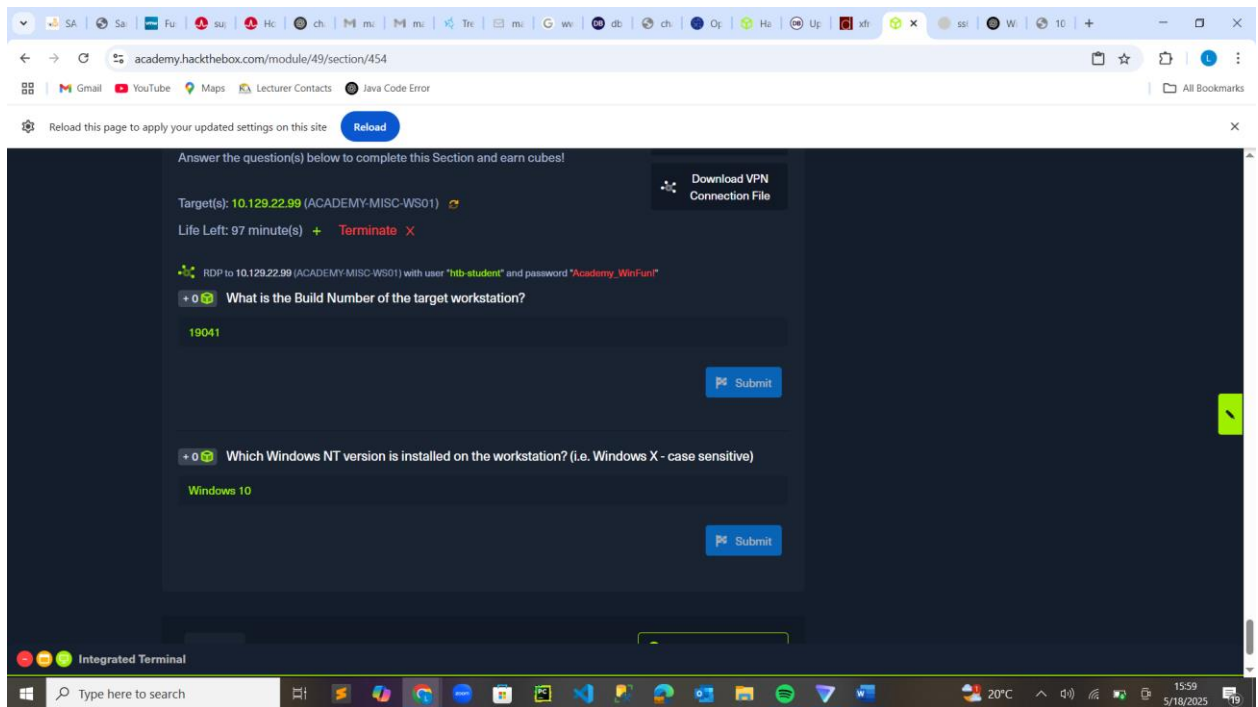


The next steps were to get the Build Number and the Windows NT version of the target workstation.

To get them, I launched shell on the remote machine and used the Get-WmiObject cmdlet (as shown below) to get more information about the Operating system.

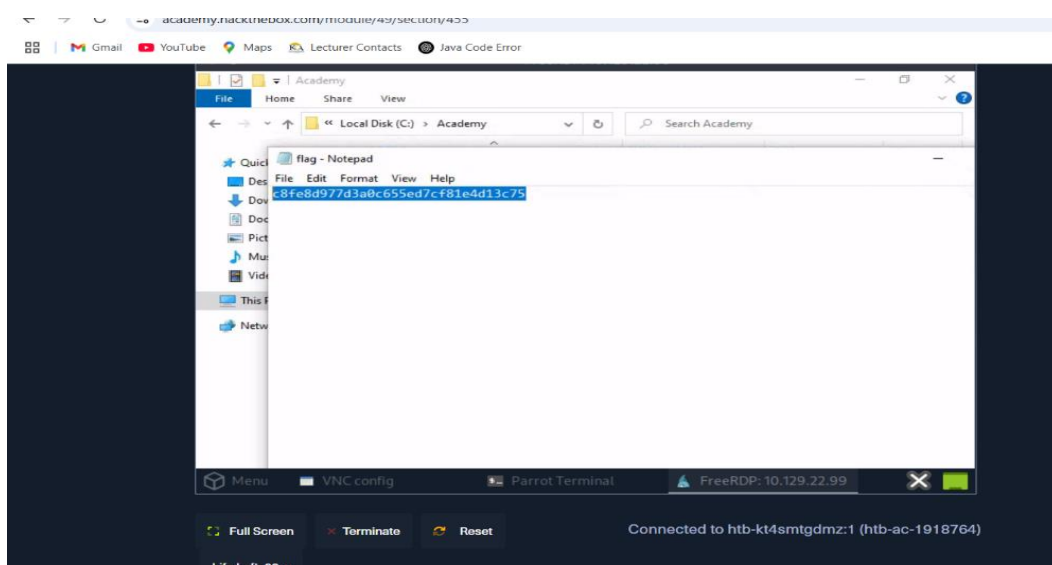


HTB Answers from snippet above



TOPIC 2: Operating system structure:

In this section, the task was to find the non-standard directory in the C drive of our target machine. To do that, I simply used the GUI, opened file explorer and navigated to the C drive (Boot Partition) and there was a folder (Academy) that does not meet the Directory Structure of C drive. Opened the folder and as shown below, there was a text file with our flag.

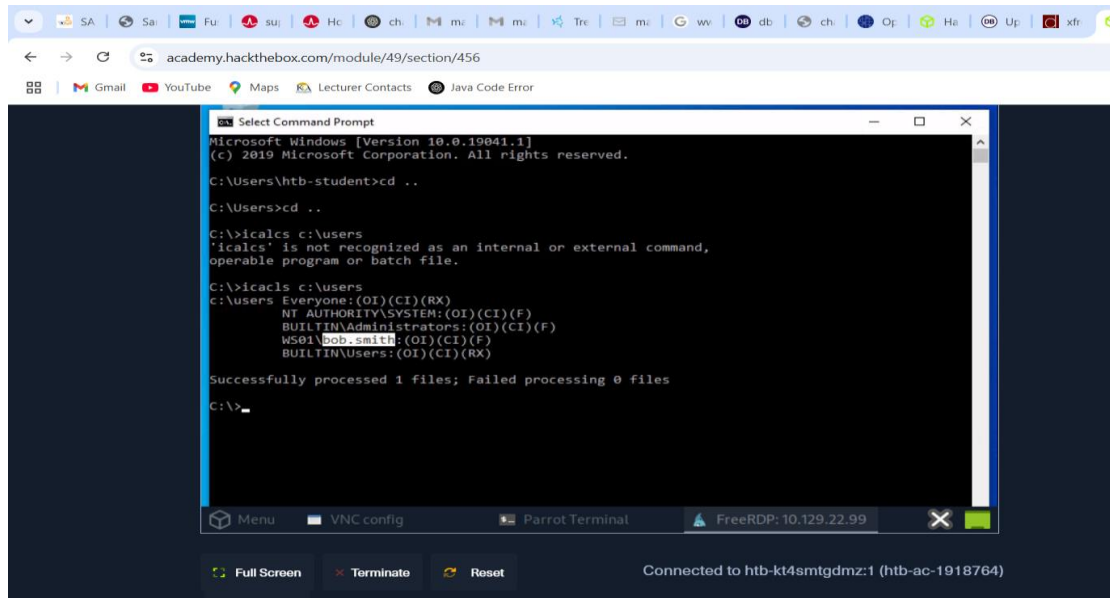


TOPIC 3: File System:

In this task, we are supposed to find the system user that has full control over the `c:\users` directory.

To do that, I opened command prompt on the target machine and navigated to the users folder using the command `cd ..` then used the `icacls` (Integrity Control Access Control List) command as shown below to list the NTFS permissions.

On the Access permission brackets, bob.smith indicates f which means he has full access



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

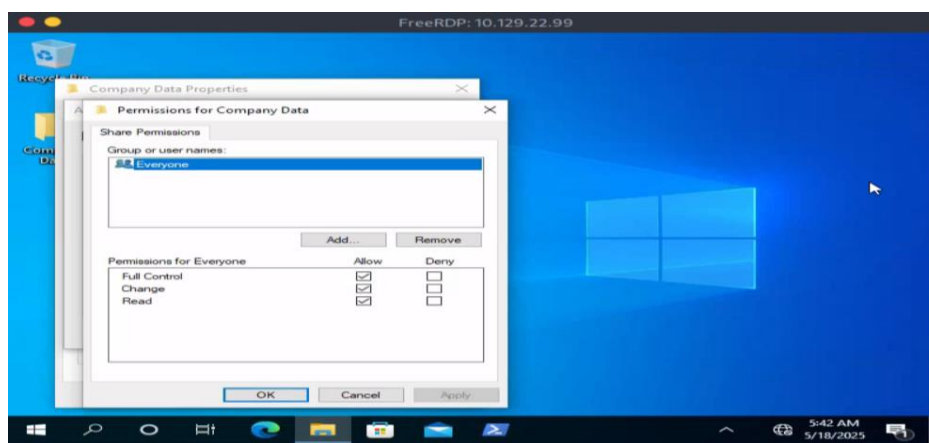
C:\Users\htb-student>cd ..
C:\Users>cd ..
C:\Users>icacls c:\users
'icacls' is not recognized as an internal or external command,
operable program or batch file.
C:\Users>icacls c:\users
C:\Users Everyone:(OI)(CI)(RX)
NT AUTHORITY\SYSTEM:(OI)(CI)(F)
BUILTIN\Administrators:(OI)(CI)(F)
WSO1 bob.smith:(OI)(CI)(F)
BUILTIN\Users:(OI)(CI)(RX)

Successfully processed 1 files; Failed processing 0 files
C:\Users>
```

TOPIC 4: NTFS vs Share Permissions:

This lab explores Windows file sharing via SMB and the relationship between NTFS and Share permissions.

I started by first creating a folder and named it “Company Data”, went to advanced sharing and shared the folder and left the Access Control List (ACL) as default as shown below



Navigated to the kali box and used the smbclient tool to try and access the shares from our target **command:** `smbclient -L SERVER_IP -U htb-student` to try and list available shares but I ran into a problem indicating that connection to our windows machine failed.

```
kali@kali: ~[~]
$ ping 10.129.92.146
PING 10.129.92.146 (10.129.92.146) 56(84) bytes of data:
64 bytes from 10.129.92.146: icmp_seq=1 ttl=127 time=200 ms
64 bytes from 10.129.92.146: icmp_seq=2 ttl=127 time=236 ms
64 bytes from 10.129.92.146: icmp_seq=3 ttl=127 time=193 ms
64 bytes from 10.129.92.146: icmp_seq=4 ttl=127 time=2024 ms
64 bytes from 10.129.92.146: icmp_seq=5 ttl=127 time=194 ms
64 bytes from 10.129.92.146: icmp_seq=6 ttl=127 time=192 ms
64 bytes from 10.129.92.146: icmp_seq=7 ttl=127 time=193 ms
64 bytes from 10.129.92.146: icmp_seq=8 ttl=127 time=189 ms
64 bytes from 10.129.92.146: icmp_seq=9 ttl=127 time=306 ms
^C
--- 10.129.92.146 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8368ms
rtt min/avg/max/mdev = 188.730/414.039/2024.034/570.345 ms

(kali@kali)-[~]
$ smbclient
Usage: smbclient [-?EgqBNPKv] [-?|help] [--usage] [-M message=HOST] [-I ip-address=IP] [-E stderr] [-t
[-b send-buffer=BYTES] [-t timeout=SECONDS] [-p port=PORT] [-g grepable] [-q quiet] [-B t
[--option=name=value] [-l log-basename=LOGFILEBASE] [--leak-report] [--leak-report-full] [-R name
[-m max-protocol=MAXPROTOCOL] [-n netbiosname=NETBIOSNAME] [--netbios-scope=SCOPE] [-W workgrou
[--password=STRING] [--pw-nt-hash] [-A authentication-file=FILE] [-P machine-pass] [--simple-bind
[--use-winbind-ccache] [--client-protection=sign|encrypt|off] [-k kerberos] [-V version] [OPTIONS
do_connect: Connection to 10.129.92.146 failed (Error NT_STATUS_IO_TIMEOUT)

(kali@kali)-[~]
$
```

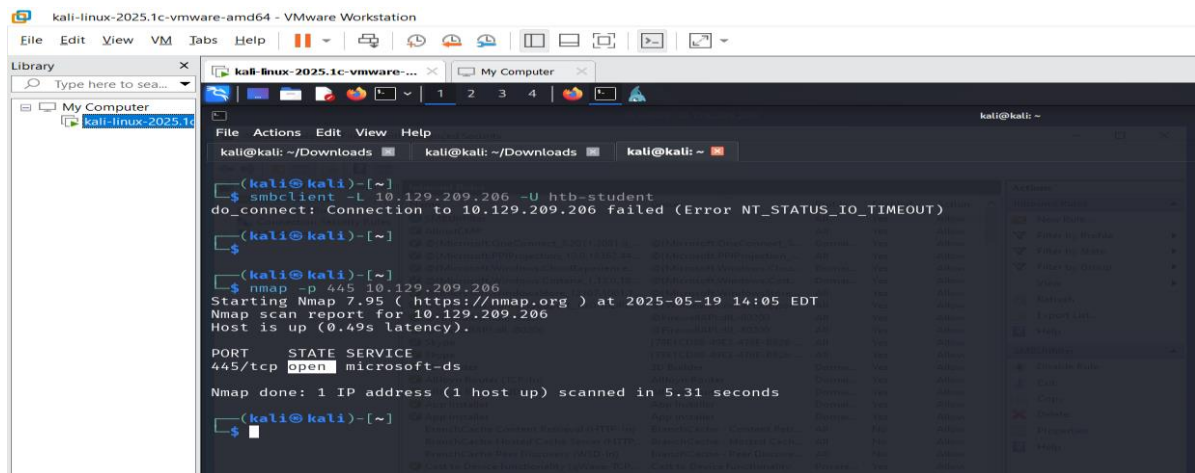
Tried to troubleshoot and first used nmap to scan if port 445 on windows is open, and realized it was open but filtered. After researching I realized the port being filtered could cause connection failure while using smbclient

```
kali@kali: ~[~]
$ nmap -p 445 10.129.92.146
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-19 09:24 EDT
Nmap scan report for 10.129.92.146
Host is up (0.19s latency).
PORT      STATE SERVICE
445/tcp   filtered microsoft-ds

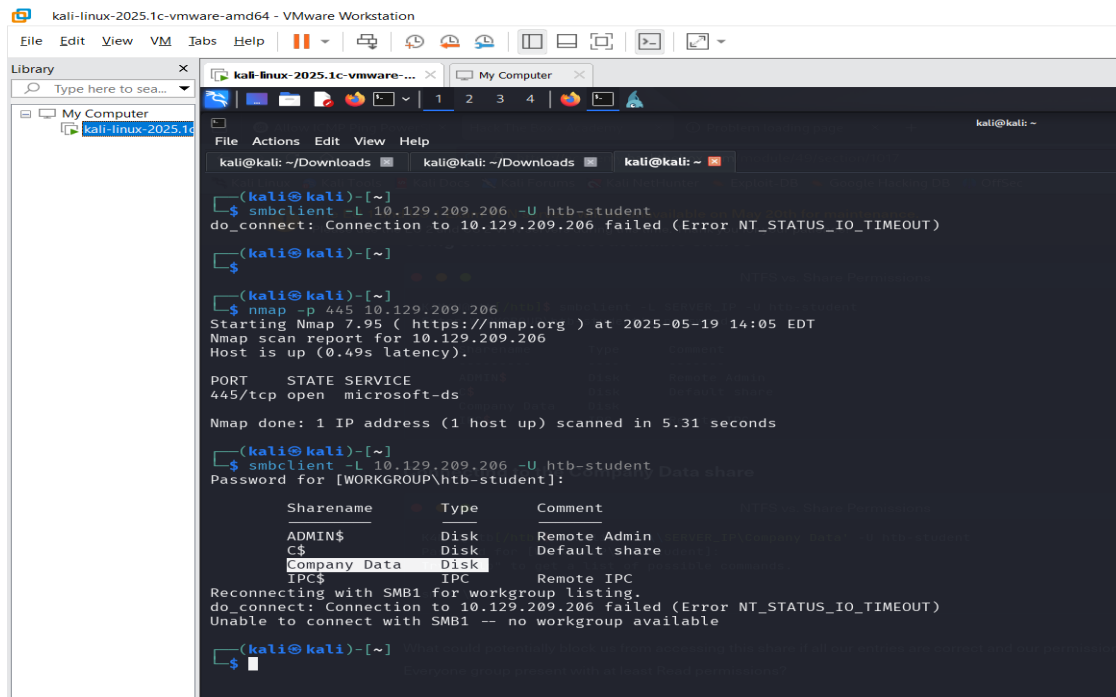
Nmap done: 1 IP address (1 host up) scanned in 2.29 seconds

(kali@kali)-[~]
$
```

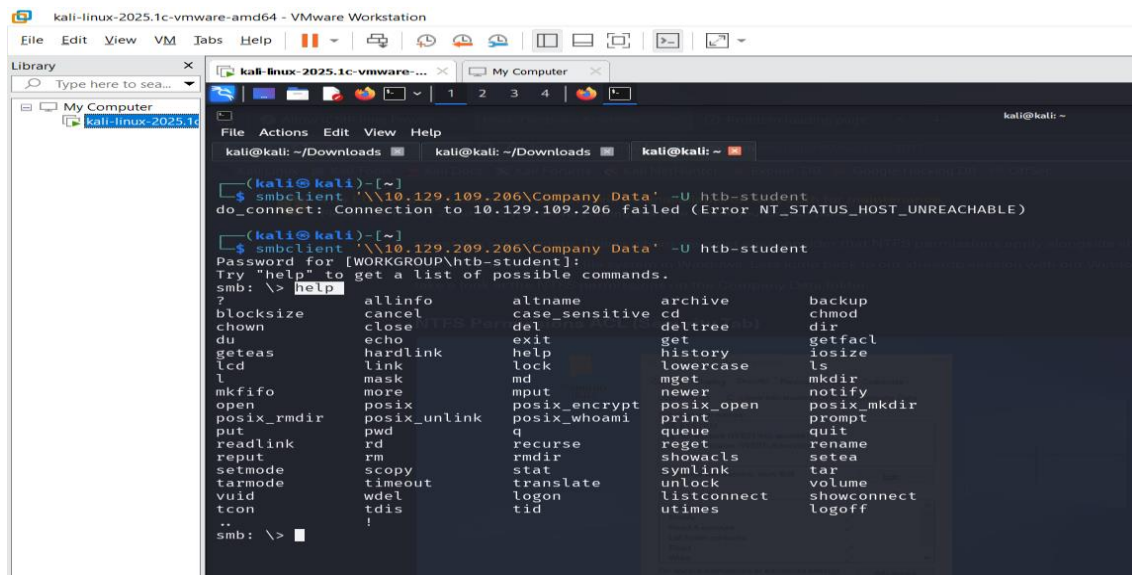
After creating a new inbound rule that unfilters port 445 on the windows firewall, I was able to open the port and tried using the smbclient tool again



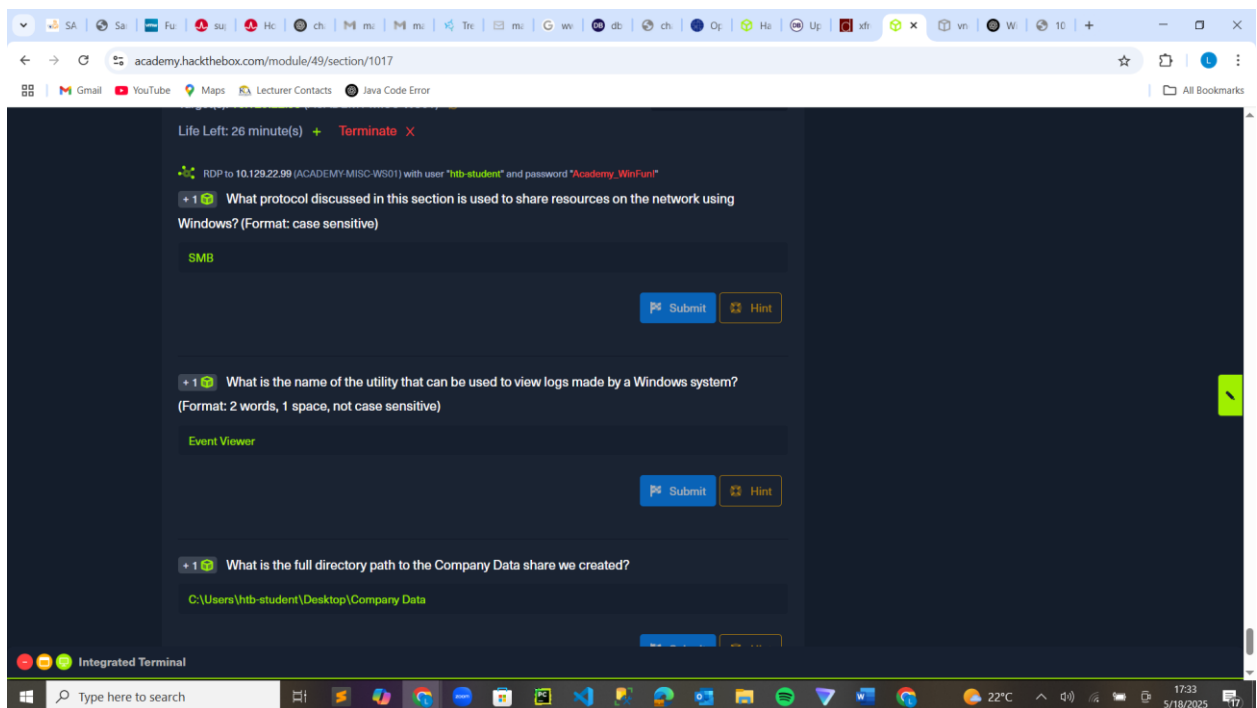
Tried the command ***smbclient -L SERVER_IP -U htb-student*** and this time it was successful and after providing a password to the machine, a list of shared directories from our windows machine are displayed including the folder “Company Data” that I had created earlier.



Used the **help** command to get a bunch of commands I can use with smbclient



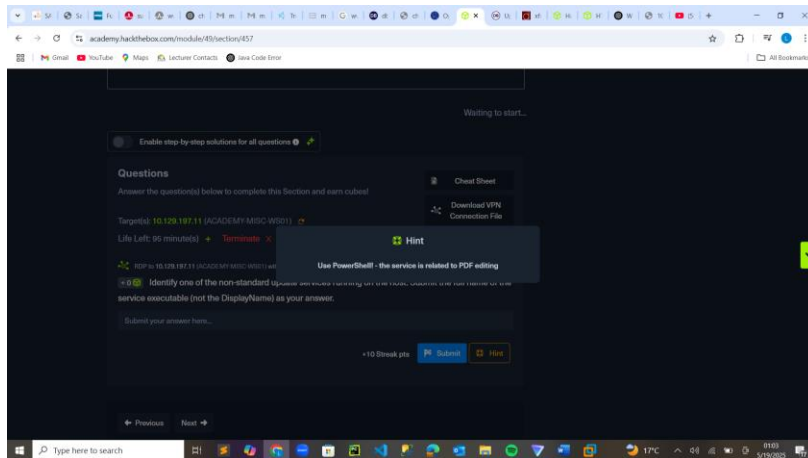
Answers to the module:



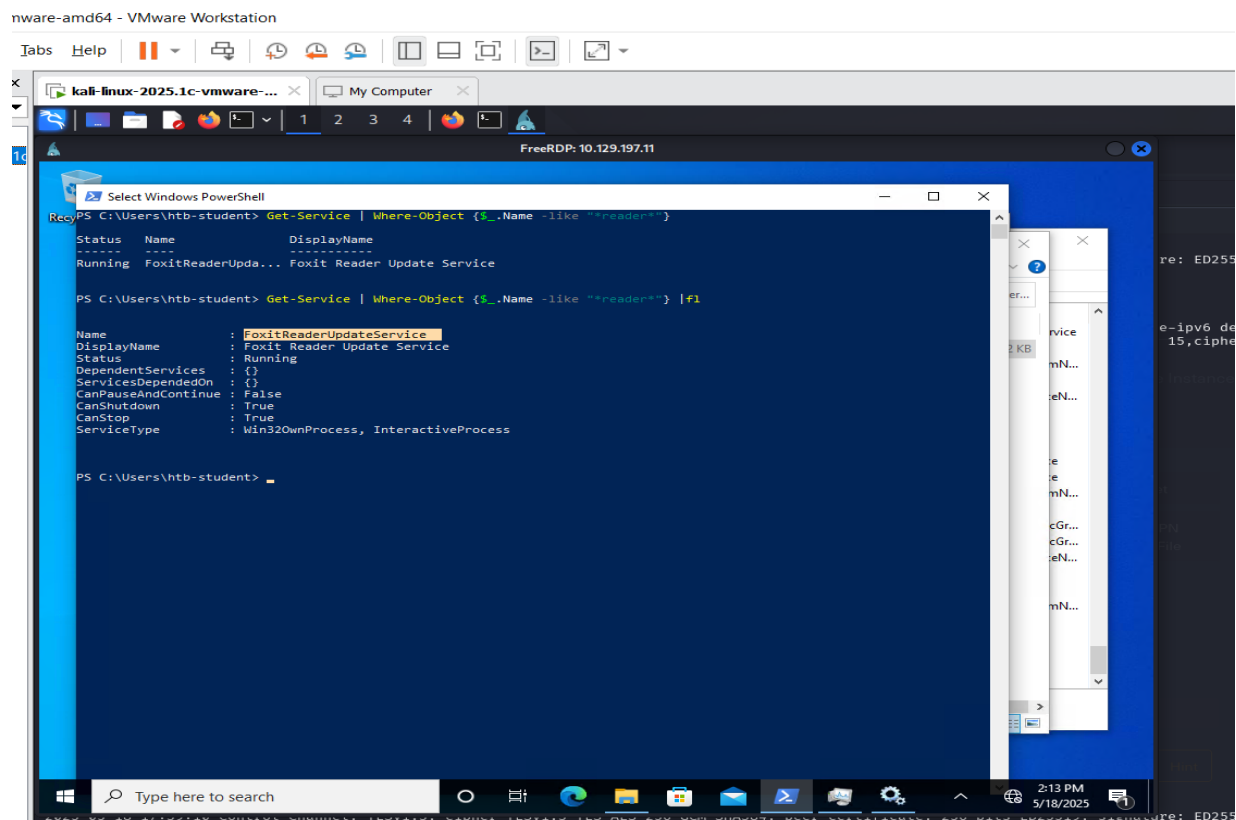
TOPIC 5: Windows Services and Processes

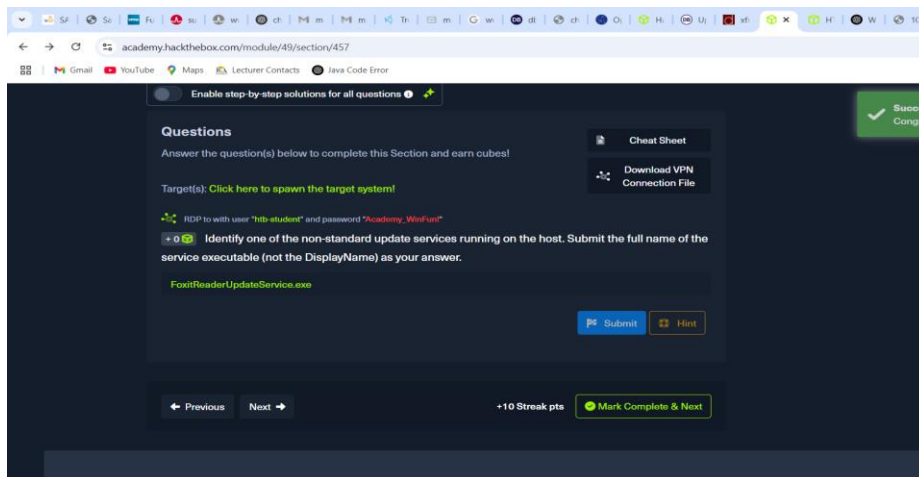
In this section, the task was to Identify one of the non-standard update services running on the host. Submit the full name of the service executable.

I used the hint option to get an idea of how to go about it, and the recommendation was: Use PowerShell! - the service is related to PDF editing



Launched powershell and used cmdlet: `Get-Service | Where-Object {$_.Name -like "*reader*"} | fl` to get any service that the name property has any text before or after reader





TOPIC 6: Service Permissions

Windows services are essential background processes that keep systems running smoothly, but they can also become hidden security risks if not managed carefully. Many cyberattacks such as malware injections, privilege escalation, and persistence techniques exploit misconfigured services, often due to admin oversight or poorly designed third-party software.

A common mistake is running critical services like DHCP or Active Directory under personal user accounts instead of dedicated service accounts. If that user leaves the organization and their account is disabled, the service crashes, potentially causing major disruptions. Attackers can also manipulate services by replacing executable files in weakly secured directories, turning a trusted process into a malicious tool.

To stay secure, here are best practices:

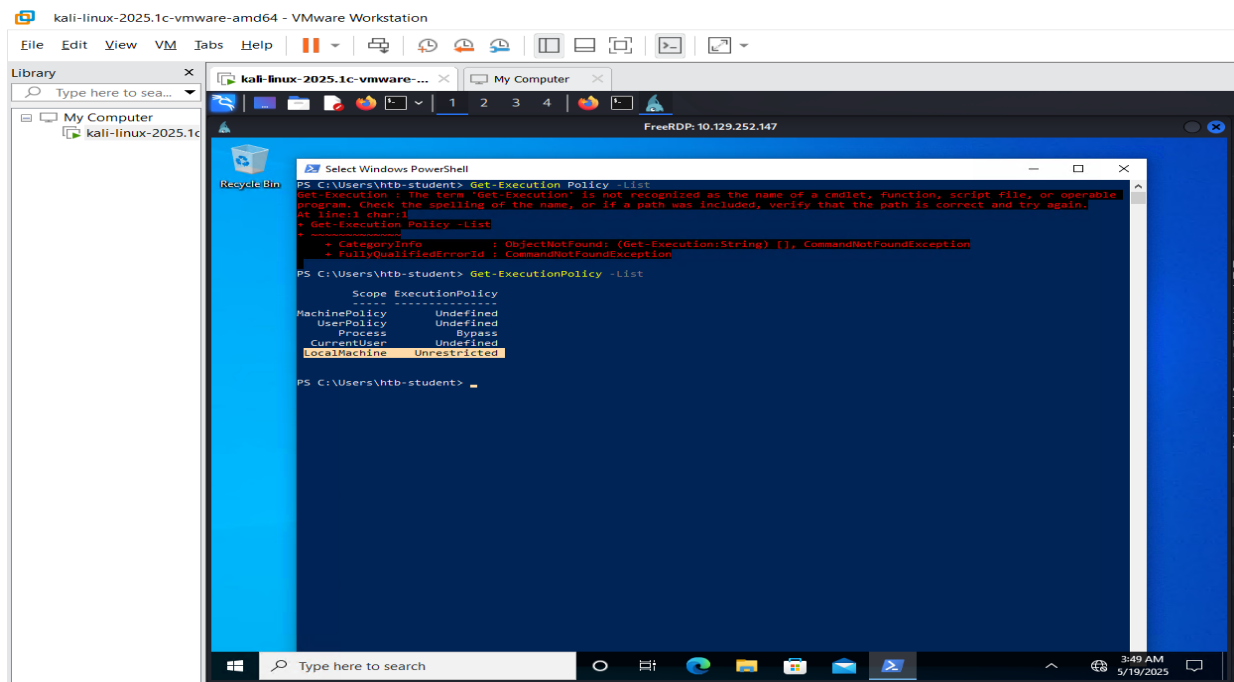
- Use service accounts – Never run critical services under personal or admin accounts.
- Apply least privilege – Avoid unnecessary LocalSystem access, that is, limit permissions.
- Audit regularly – Use tools like services.msc, and PowerShell (Get-Service, Get-Acl) to check configurations.

TOPIC 7: Windows Sessions

TOPIC 8: Interacting with the Windows Operating System

The concept of Graphical User Interface was first added to Apple and Microsoft Operating Systems to address usability concerns for everyday users that had difficulty navigating the command line

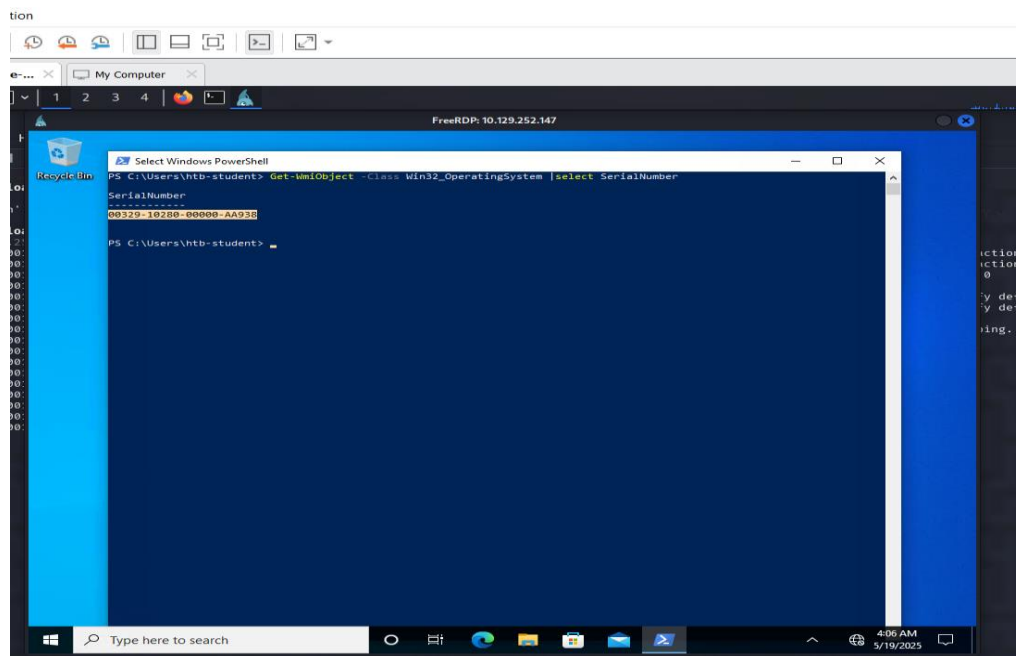
The next task was to Find the Execution Policy set for the LocalMachine scope. To do that, I launched powershell and used the command `Get-ExecutionPolicy -List` and the Execution policy for the Local Machine is given as Unrestricted as shown in the snippet below



TOPIC 9: Windows Management Instrumentation (WMI)

In this task, we are supposed to Use WMI to find the serial number of the system.

To do that, I opened powershell and used the command **Get-WmiObject -Class Win32_OperatingSystem | select SerialNumber** and the serial number is displayed



TOPIC 10: Microsoft Management Console (MMC)

NO LABS

TOPIC 11: Windows Subsystem for Linux (WSL)

NO LABS

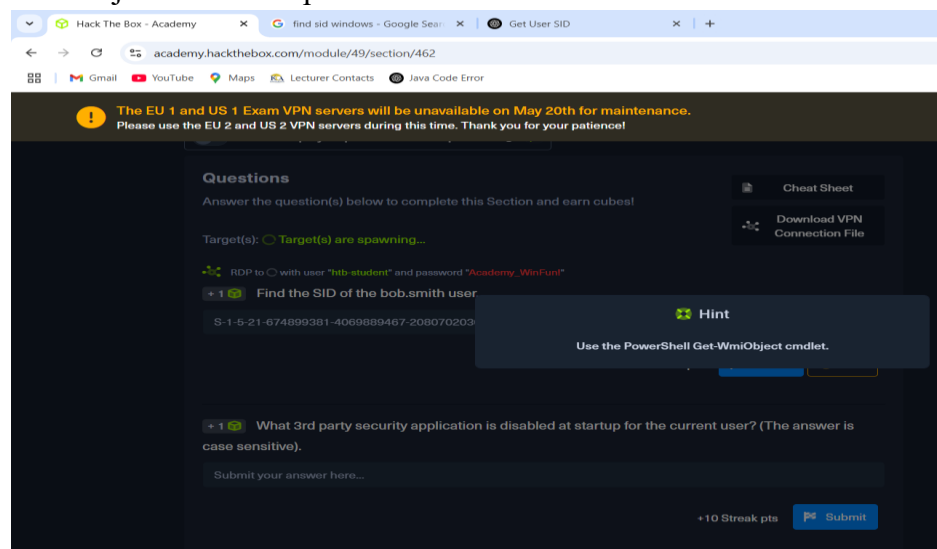
TOPIC 12: Desktop Experience vs. Server Core

NO LABS

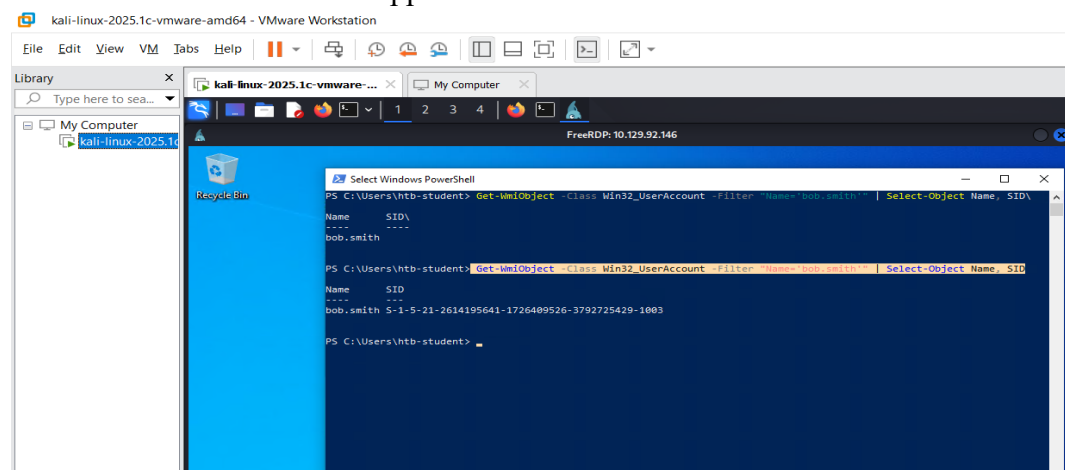
TOPIC 13: Windows Security

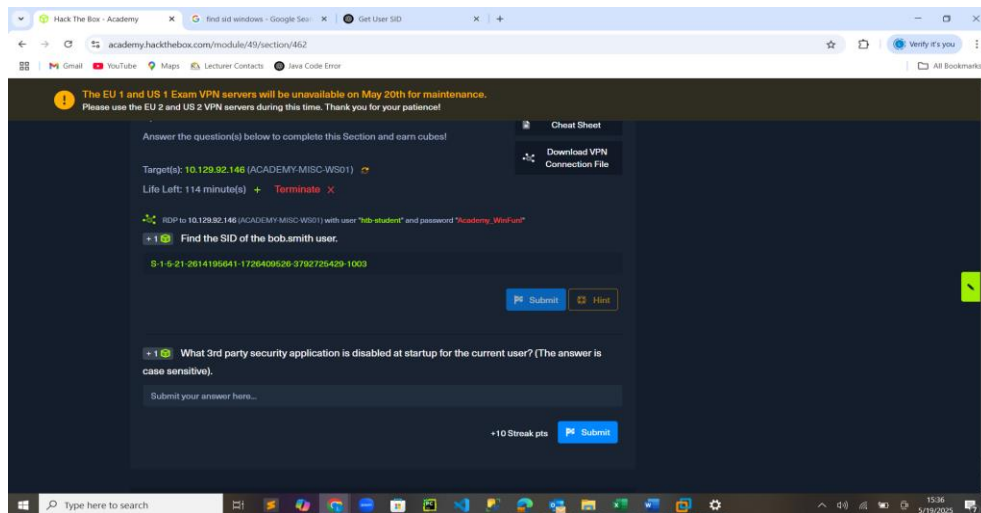
In this section, the task is Find the SID of the bob.smith user.

I used the hint option to get an idea of how to go about it and I had to use the Get-WmiObject cmdlet on powershell.



I launched the powershell and used the Get-WmiObject cmdlet using the UserAccount class to get the SID of the user bob.smith
Command is shown in the snippet below as well as the SID

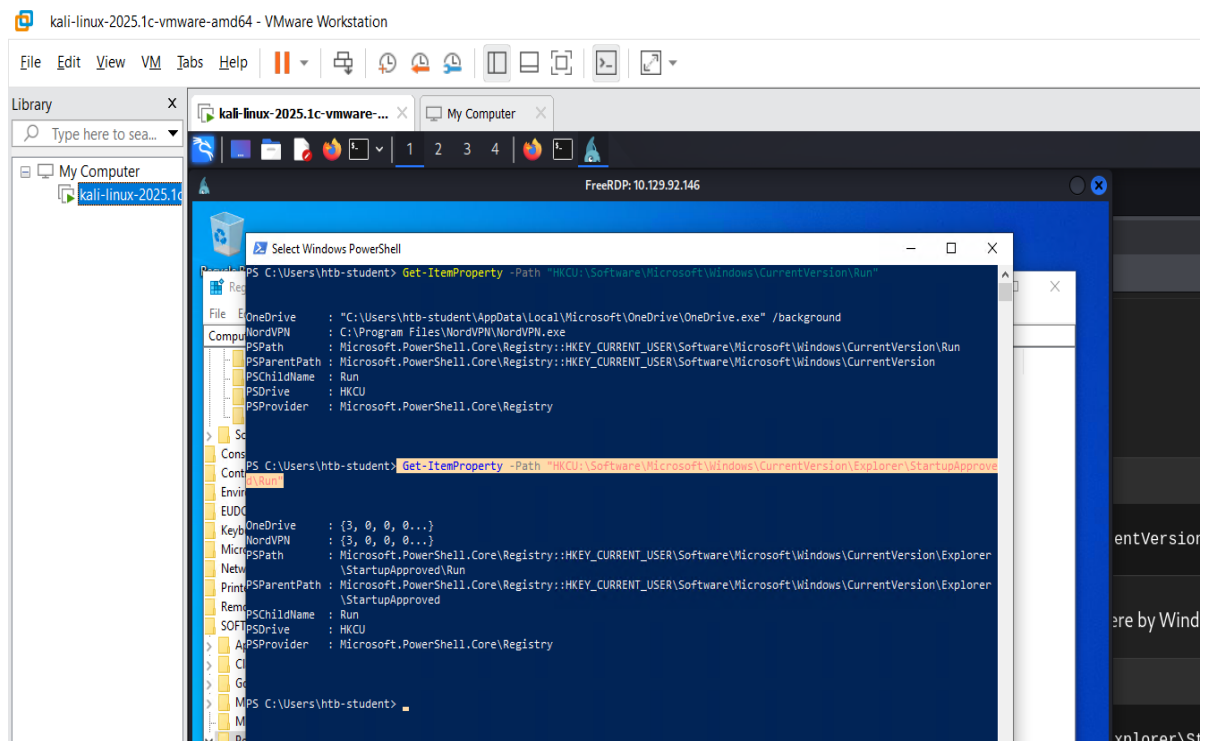


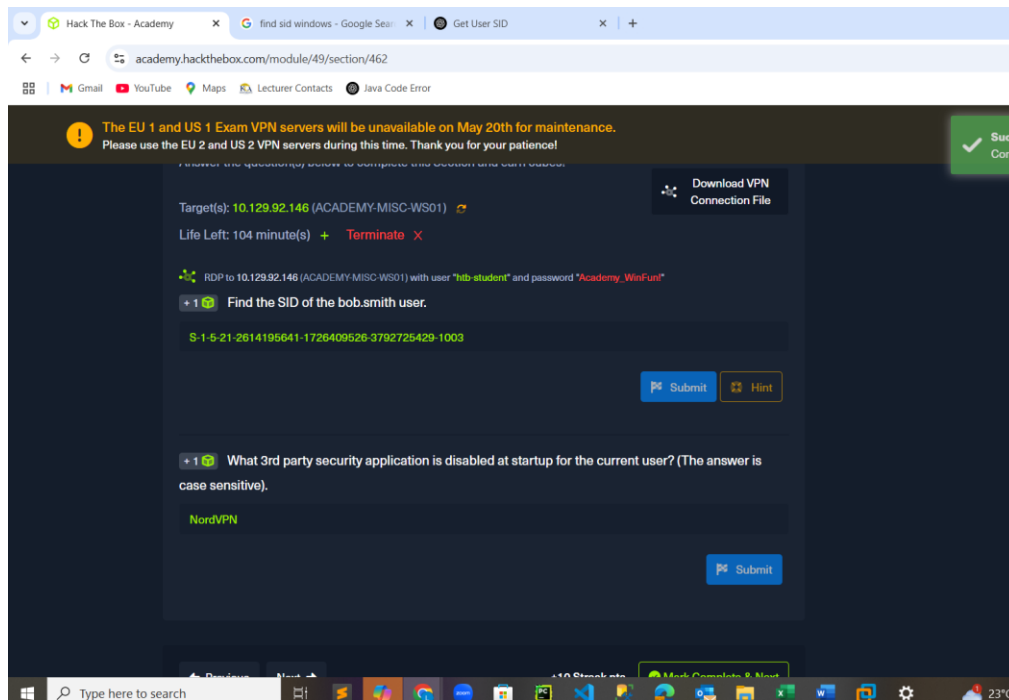


The next task was to find 3rd party security application is disabled at startup for the current user

To do that I used the command: **Get-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run"** to Retrieve registry values from the StartupApproved\Run key under the current user's (HKCU) startup settings and List programs *disabled* from auto-starting, they are marked with binary data.

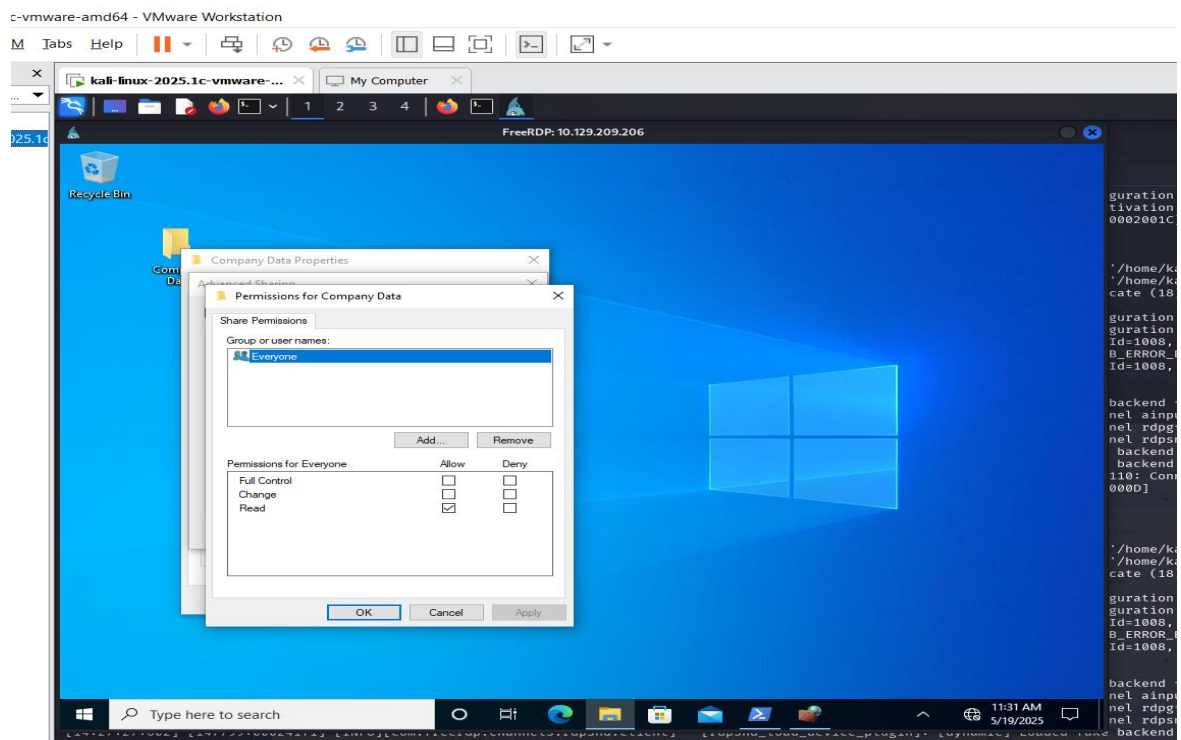
Binary data starting with 03 00 00 00 indicates disabled status and we have NordVPN that worked as my answer.



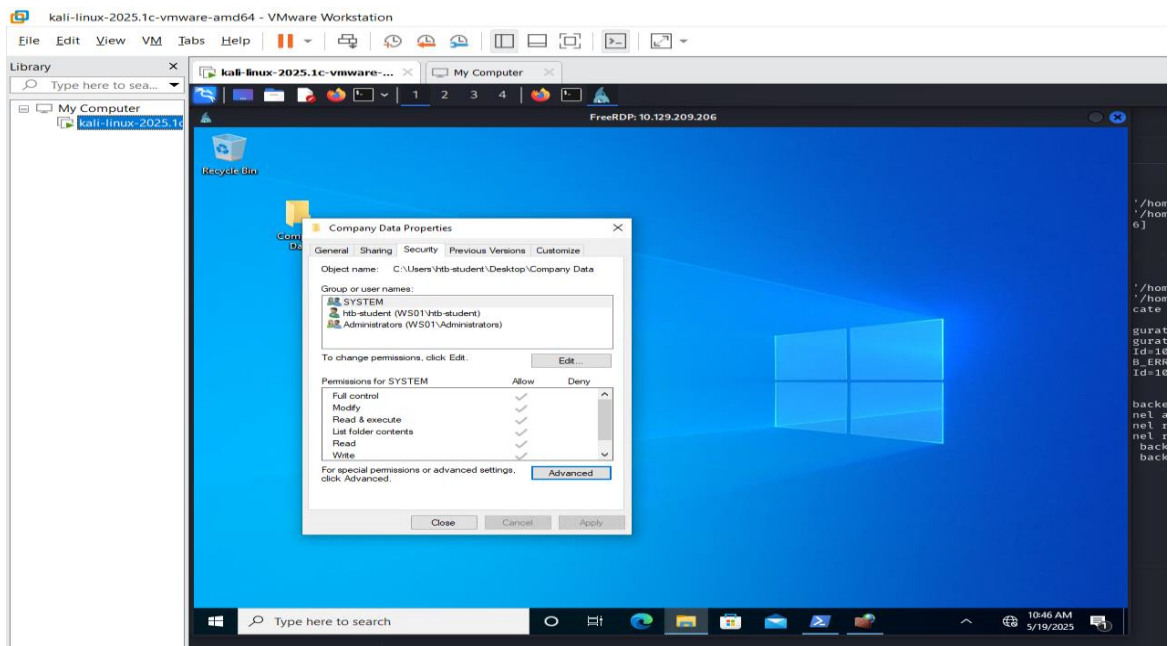


TOPIC 14: Skills Assessment:

Question 1: What is the name of the group that is present in the Company Data Share Permissions ACL by default? **Everyone**

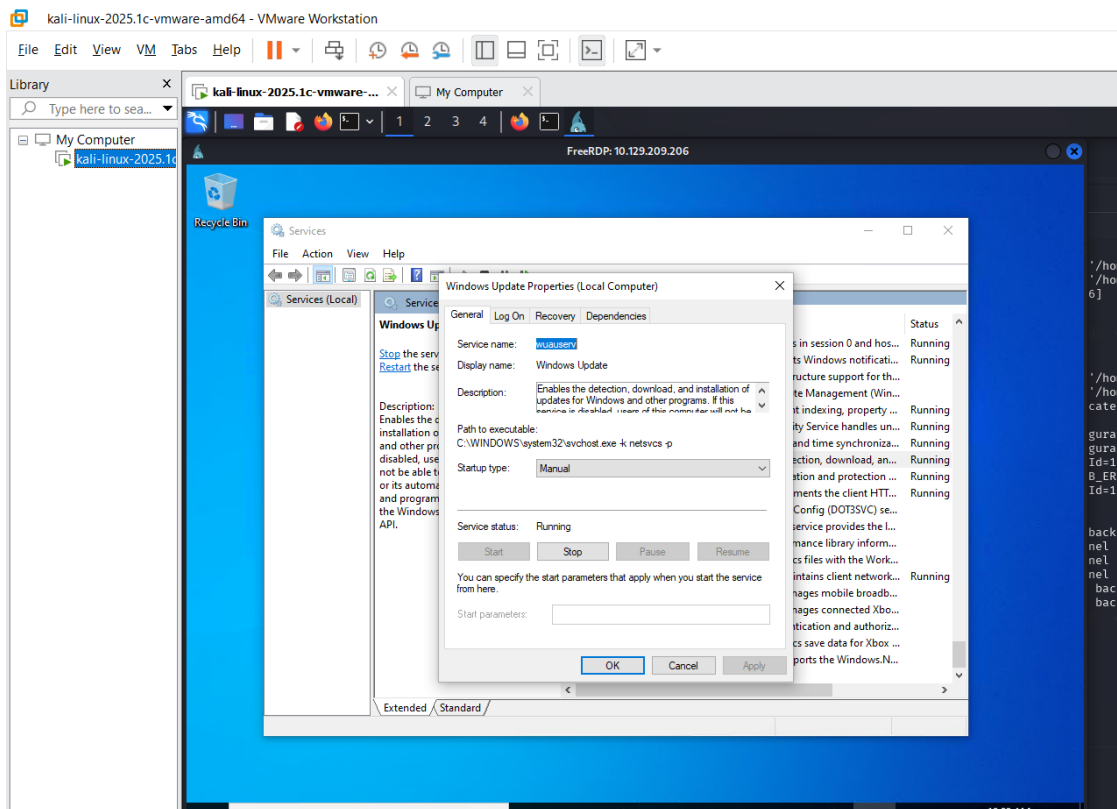


Question 2: What is the name of the tab that allows you to configure NTFS permissions? **Security**

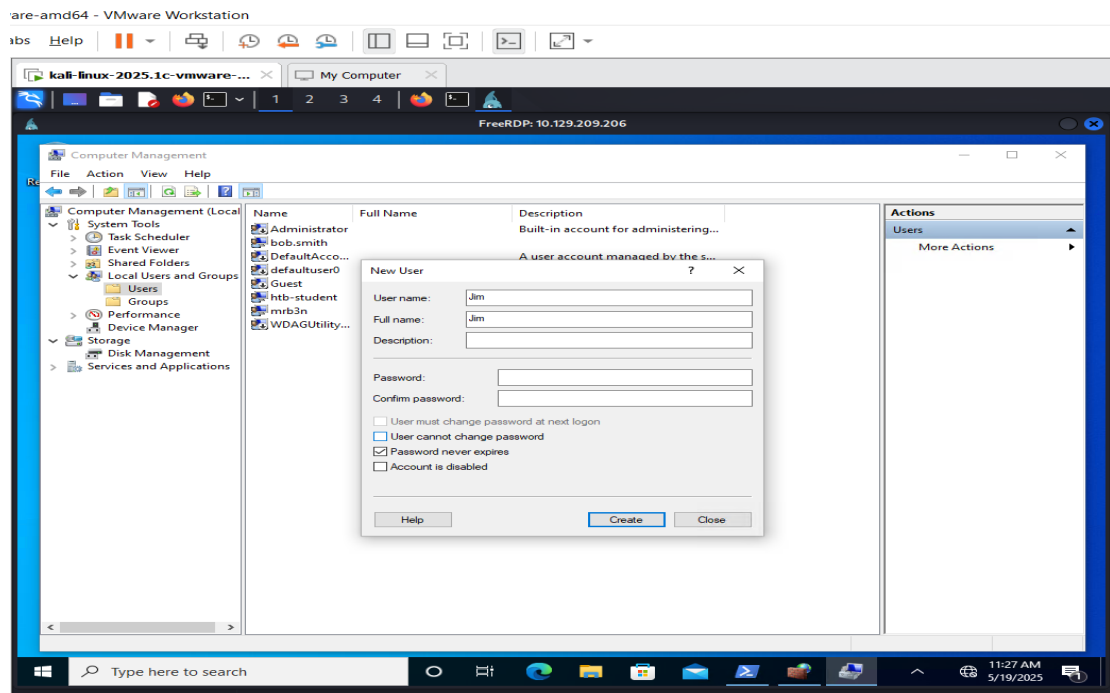


Question 3: What is the name of the service associated with Windows Update?

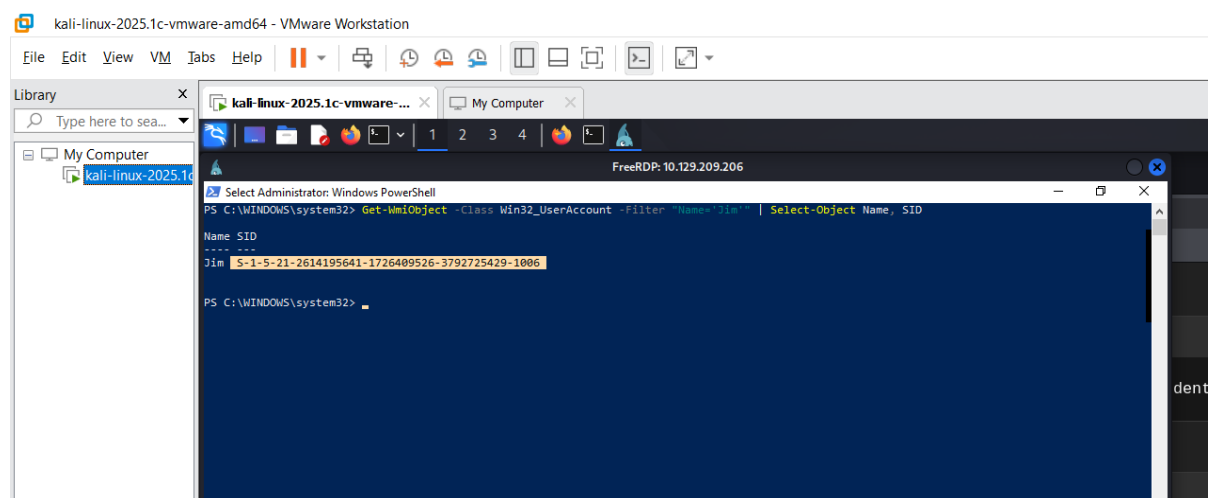
wuauserv



Question 4: List the SID associated with the user account Jim you created.
First created a User Jim



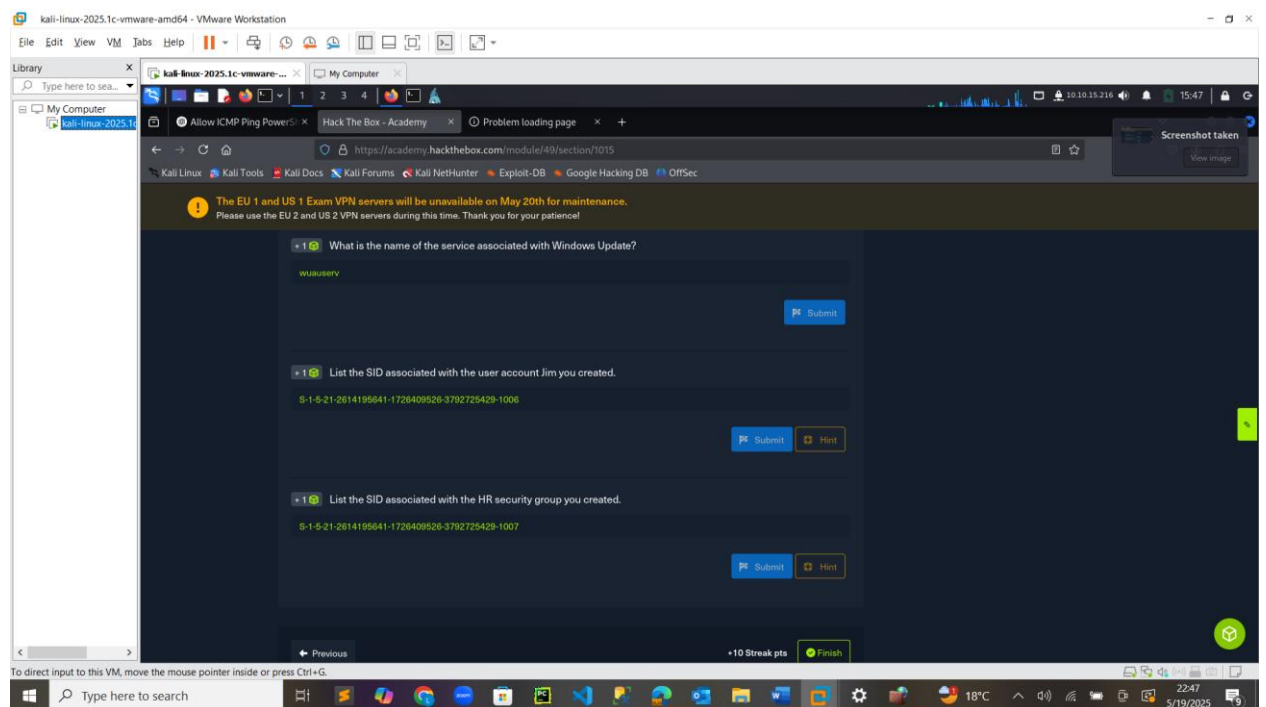
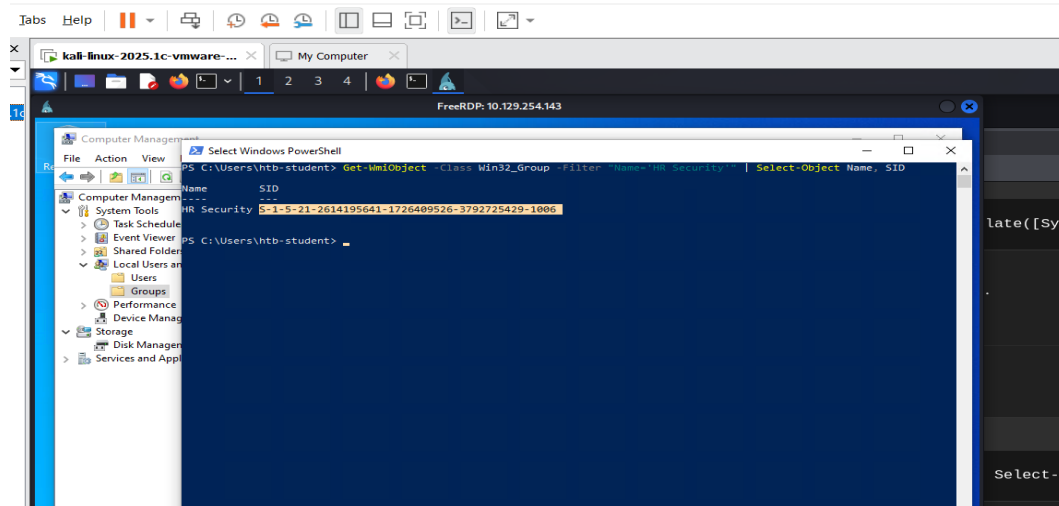
Launched powershell and used the command: `Get-WmiObject -Class Win32_UserAccount -filter "Name='Jim'" | Select-Object Name, SID` to get the SID for the user account Jim



Question 5: List the SID associated with the HR security group you created.

First launched computer management and created a new group named HR Security group. Then navigated to powershell and used the command `Get-WmiObject -Class Win32_Group -Filter "Name='HR Security'" | Select-Object Name, SID` to get the SID associated with the HR Security group that we created earlier.

vmware-amd64 - VMware Workstation



FINAL SCREENSHOT



CONCLUSION:

This module provided me with a strong foundation in understanding how the Windows operating system functions from both a user and system perspective. Key areas such as user and group management, file system structure, networking, and system processes were clearly explained and reinforced through practical tasks. The hands-on experience helped bridge the gap between theory and real-world application, especially in navigating the command line and interpreting system behavior.

Overall, the knowledge I gained here is essential for interacting with Windows environments more effectively and sets a foundation for tackling more advanced system and security challenges.