

MARTIN MWANGI NJOROGI

mwangimartins650@gmail.com

CS-SA08-24031

WINDOWS FUNDAMENTAL MODULE

Here's a Link to my completed module

<https://academy.hackthebox.com/achievement/1476316/49>

1. Introduction

In this module, I started with an introduction to windows history through-out the years and as the different versions were developed the security also improved and the current versions that are being used, *Windows 11* and *Windows_server_2019*.

This module gave me an understanding of operation of windows and its use in a business environment. That is for a task to takes place there are several essential processes, services and programs involved for successful completion of task. The Operating System Kernel (interacts with the hardware components of the computer) takes requests from the system services.

1.1 Windows OS

It's an OS that has user friendly interface that is just a click of button for a task to start or stop, with this feature in mind it came different version of this OS.

Windows OS can be accessed in different ways either by local access or Remote access and in this remote access both target and client use same OS. As RDP is proprietary to Microsoft, it's build-in to the OS.

And for a windows computer to accessed by Linux OS host, the Linux host uses a xfreerdp tool to access it.

First, I started off by setting the OpenVPN, Downloading and configuring the OpenVPN to create a connection with the target.

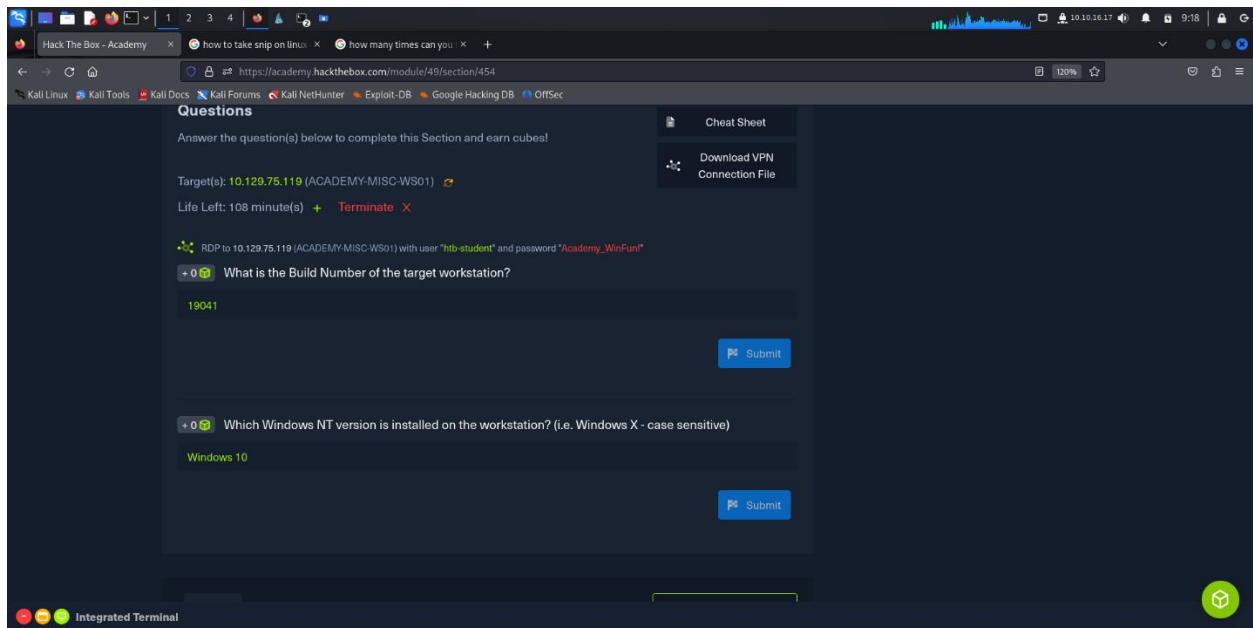
```
File Actions Edit View Help
[deustrohek@kali:~/Downloads]
[deustrohek@kali:~/Downloads]$ sudo netstat -tlnps
netstat -tlnps
2024-09-18 09:06:35 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2024-09-18 09:06:35 Note: data-ciphers-fallback with cipher AES-256-GCM will fallback to GCM ciphers if available.
2024-09-18 09:06:35 OpenSSH 2.10.122 deb 4n-gnu-linux-gnu [SSL, OpenSSL], [DIO] [DIO] [PQOSSL] [MD5/PWNTSOP] [AEAD] [DIO]
2024-09-18 09:06:35 Library versions: OpenSSL 3.2.2-dev, LZO 2.10
2024-09-18 09:06:35 SSH version: N/A
2024-09-18 09:06:35 TCPMIME: Processing recently used remote address: [AF_INET][754.57.104.180]x43
2024-09-18 09:06:35 Socket Buffer: rcv=10072>138872 w=3240w+3240w
2024-09-18 09:06:35 Attempting to establish TCP connection with [AF_INET][754.57.104.180]x43
2024-09-18 09:06:35 TCP connection established with [AF_INET][754.57.104.180]x43
2024-09-18 09:06:35 TCPMIME client link local: [af_inet][754.57.104.180]x43
2024-09-18 09:06:35 TCPMIME client link remote: [af_inet][754.57.104.180]x43
2024-09-18 09:06:35 TLS Initial packet from [AF_INET][754.57.104.180]x43, sio=4d3f3eac7ef4555
2024-09-18 09:06:35 VERIFY OK: depth=0, C=GB, o=CyberChef, ou=The Box, ou-Systems, cn=Web Client Authentication Authority
2024-09-18 09:06:35 VERIFY OK: depth=0, C=GB, o=CyberChef, ou=The Box, ou-Systems, cn=Web Server Authentication Authority
2024-09-18 09:06:35 VERIFY OK: CN
2024-09-18 09:06:35 Validating certificate extended key usage
++ Certificate has EKU (str) TLS Web Client Authentication, expects TLS Web Server Authentication
++ Certificate has EKU (oid) 2.5.29.32.2, expects TLS Web Server Authentication
2024-09-18 09:06:35 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2024-09-18 09:06:35 VERIFY OK
2024-09-18 09:06:35 VERIFY OK: depth=0, C=GB, o=CyberChef, ou=The Box, ou-Systems, cn=Web-academy-3
2024-09-18 09:06:37 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 256 bits ECDHE559, signature: ECDHE559, peer temporary key: 253 bits ECDHE559
[academy-3] Peer Connection: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 256 bits ECDHE559, signature: ECDHE559, peer temporary key: 253 bits ECDHE559
2024-09-18 09:06:37 New session: den=ACTIVE user=NINITIA, result=sent
2024-09-18 09:06:37 TLS multi-process: initial handshake session promoted to trusted
2024-09-18 09:06:38 SENT CONNECT [academy-3]: "PQOSSL:MIMT" status=1
2024-09-18 09:06:38 PQOSSL accepted control message: [AF_INET] route 10.10.10.2,255.255.255.0,route 10.129.8.0,255.255.255.0,route-ipsec deadbeat:/4,explicit-est-notify,tun-ipsec,routegateway 10.10.10.1,topology subnet,ping 10.ping-v
start 120,ifconfig ipsec deadbeat:/100764/deadbeat:/1a/config 10.10.10.17,225.225.224.0,peer-id 0,cipher AES-256-GCM
2024-09-18 09:06:38 OPTIONS EXPORT -- Ifconfig options modified
2024-09-18 09:06:38 OPTIONS IMPORT -- route options modified
2024-09-18 09:06:38 OPTIONS IMPORT -- route-related options modified
2024-09-18 09:06:38 net_route_want_ipsec query: ok 0.0.0.0
2024-09-18 09:06:38 net_route_want_ipsec result: via 10.10.2.2 dev eth0
2024-09-18 09:06:38 ROUTE_GATEWAY 10.10.2.2/255.255.255.0 dev eth0 MMADDR=00:0C:0B:0F:17:08:abdc
2024-09-18 09:06:38 CONN_ROUTE_WANT_IPSEC/N/A
2024-09-18 09:06:38 net_route_want_ipsec query: ok 1
2024-09-18 09:06:38 tunnel send: still generic error (-12): Network is unreachable
2024-09-18 09:06:38 ROUTES: default_gateway=NONE
2024-09-18 09:06:38 TUN/TAP device link opened
2024-09-18 09:06:38 net_iface_mtu_set: mtu 1500 for tun0
2024-09-18 09:06:38 net_iface_up: net down
2024-09-18 09:06:38 net_addr_wt_add: 10.10.10.17/23 dev tun0
2024-09-18 09:06:38 net_iface_state: net up for tun0
2024-09-18 09:06:38 net_iface_wt_add: deadbeat:/100764/dev tun0
2024-09-18 09:06:38 net_iface_wt_add: 10.10.10.8/23 via 10.10.10.1 dev [NULL] table 0 metric -1
2024-09-18 09:06:38 net_iface_wt_add: 10.129.8.0/24 via 10.10.10.1 dev [NULL] table 0 metric -1
2024-09-18 09:06:38 net_iface_wt_add: deadbeat:/4 via deadbeat:/4 metric -1 dev tun0
2024-09-18 09:06:38 net_route_wt_add: deadbeat:/4 via : dev tun0 table 0 metric -1
2024-09-18 09:06:38 Initialization Sequence Completed
```

```

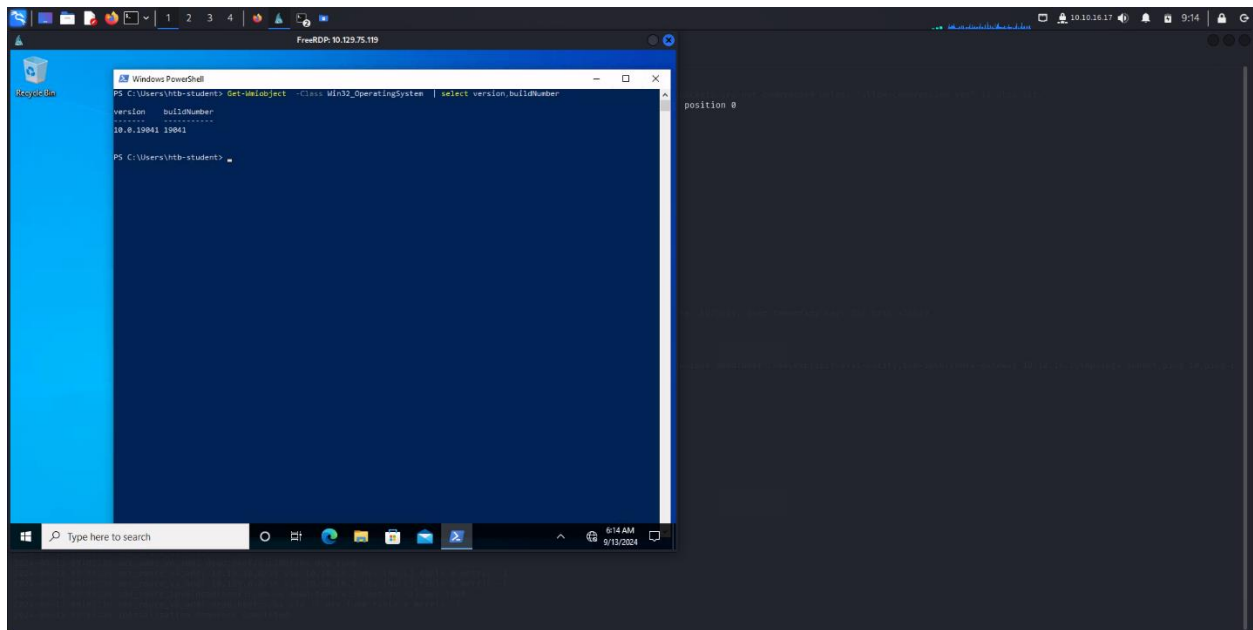
File Actions Edit View Help
[deathstroke@kali:~]$ ./freerdp /u:10.129.75.119 /u:htb-student /p:Academy_WinFun!
[09:08:43:094] [3868:3869] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (10)' at stack position 0
[09:08:43:094] [3868:3869] [WARN][com.freerdp.crypto] - CN = WSO1
[09:08:43:109] [3868:3869] [ERROR][com.freerdp.crypto] - ~~~~~
[09:08:43:109] [3868:3869] [ERROR][com.freerdp.crypto] - @ WARNING: CERTIFICATE NAME MISMATCH! @
[09:08:43:109] [3868:3869] [ERROR][com.freerdp.crypto] - ~~~~~
[09:08:43:109] [3868:3869] [ERROR][com.freerdp.crypto] - The hostname used for this connection (10.129.75.119:3389)
[09:08:43:109] [3868:3869] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[09:08:43:109] [3868:3869] [ERROR][com.freerdp.crypto] - Common Name (CN):
[09:08:43:109] [3868:3869] [ERROR][com.freerdp.crypto] - WSO1
[09:08:43:109] [3868:3869] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 10.129.75.119:3389 (RDP-Server):
    Common Name: WSO1
    Subject: CN = WSO1
    Issuer: CN = WSO1
    Thumbprint: 76:e7:90:d9:78:9d:eb:81:c8:e6:5e:c7:b7:93:22:0b:3c:37:09:aa:9b:ce:2a:4e:23:13:3b:89:17:b8:5f:33
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N)

```

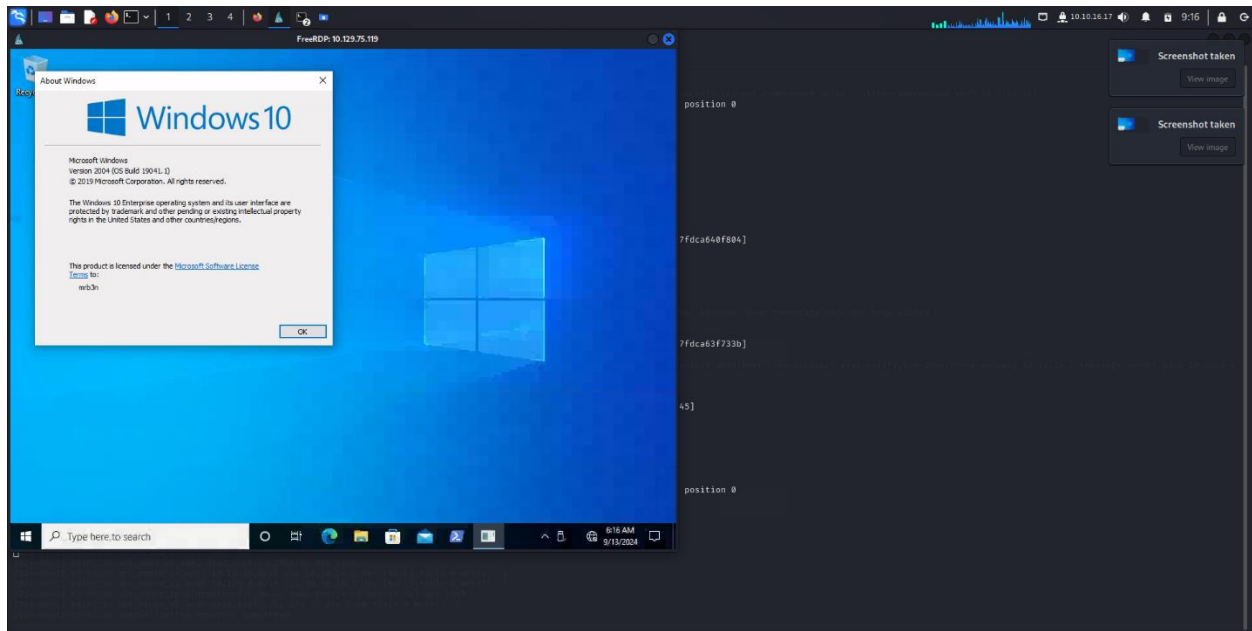
Questions I tackled



Using the PowerShell, I used the command *Get-WmiObject -Class win32_operatingsystem* to get Build Number of the machine



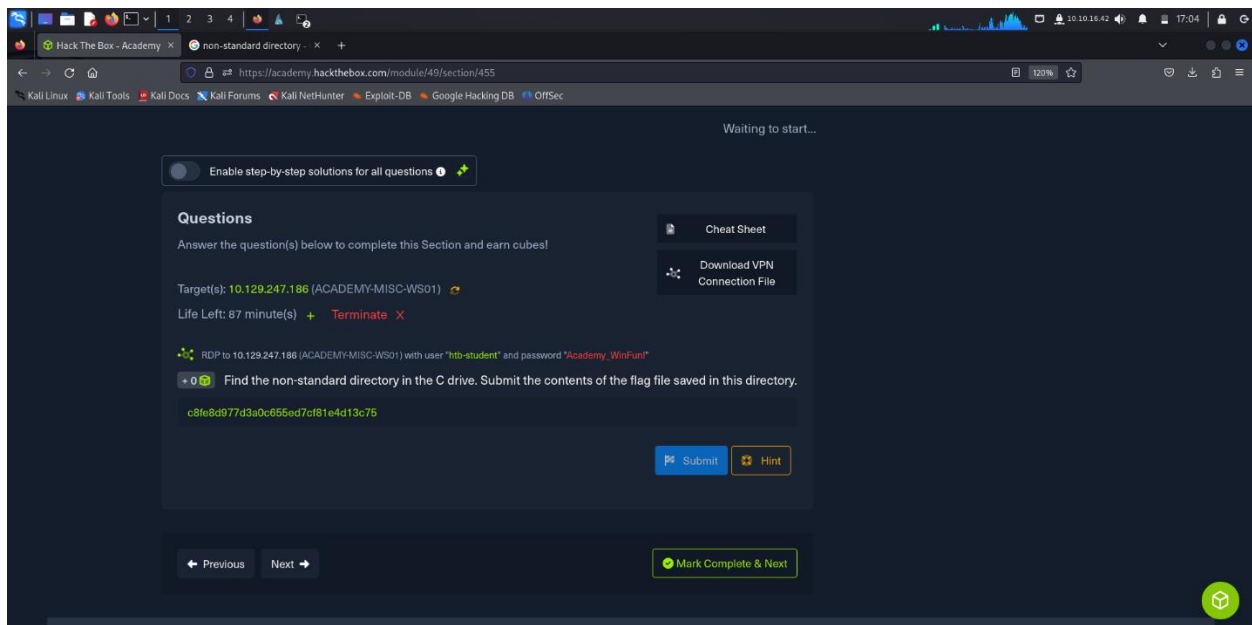
Using the *Windows Run* and *Winver* (Windows version) I found the windows version running on the machine



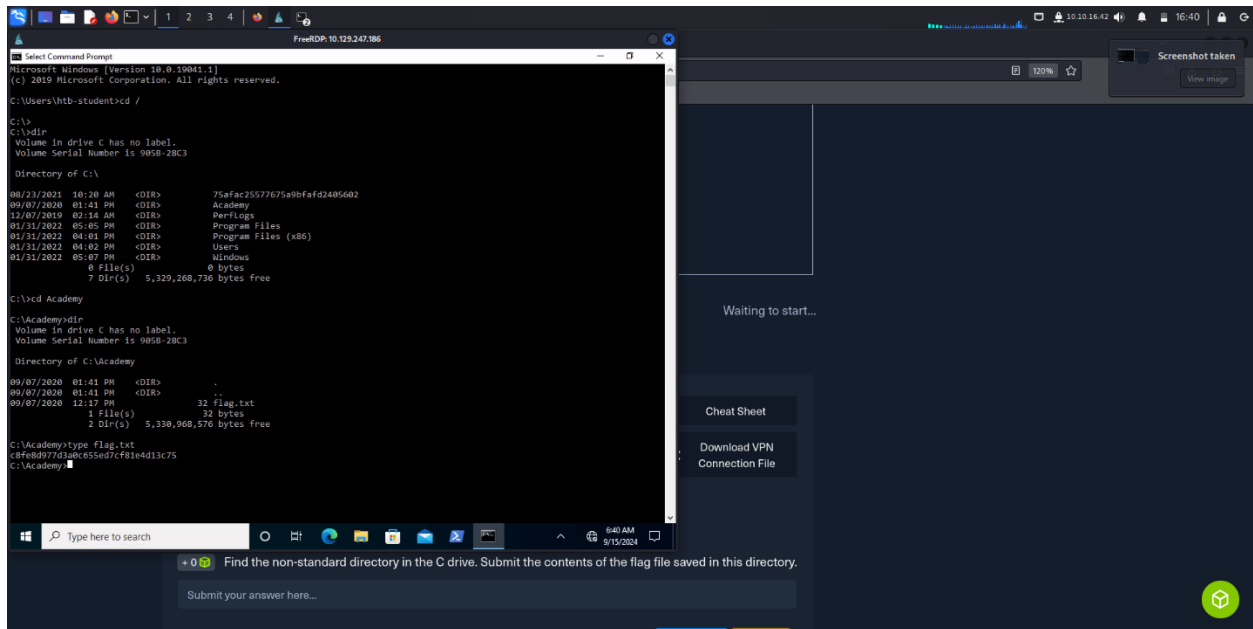
1.2 Operating system structure

Is a structure of how the Windows OS arranges its file system that is accessible to its users. That is the root directory where the OS is installed. Plus, it holds directories that are essential for windows OS to run.

Question



Using the command Dir, it shows files in a directory, and type command to show the contents of the flag file.



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

C:\Users\Htb-student>cd /

C:\>
C:\>dir
Volume in drive C has no label.
Volume Serial Number is 9958-28C3

Directory of C:\

08/23/2021 10:20 AM <DIR>          75afac25577675a8bfaf2405602
09/07/2020 01:41 PM <DIR>          Academy
12/07/2019 02:14 AM <DIR>          PerfLogs
01/31/2022 05:45 PM <DIR>          Program Files
01/31/2022 04:01 PM <DIR>          Program Files (x86)
01/31/2022 04:02 PM <DIR>          Users
01/31/2022 05:07 PM <DIR>          Windows
               0 File(s)            0 bytes
               7 Dir(s)    5,329,268,736 bytes free

C:\>cd Academy
C:\>dir
Volume in drive C has no label.
Volume Serial Number is 9958-28C3

Directory of C:\Academy

09/07/2020 01:41 PM <DIR>          .
09/07/2020 01:41 PM <DIR>          ..
09/07/2020 12:17 PM             32 flag.txt
               1 File(s)            32 bytes
               2 Dir(s)    5,330,968,576 bytes free

C:\Academy>type flag.txt
c8f68d977d1abc855ed7cf81e4d13c75
C:\Academy>
```

Waiting to start...

Cheat Sheet

Download VPN Connection File

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

Submit your answer here...

1.3 File system

NTFS is a default Windows file system being used that allows use to set granular permissions on both files and folders compared to FAT32. These permissions allow users to either, read, write, modify, execute, delete a file, folder or program.

Thus provide Access control security to important files and folders. In this file system, file, folders inherit permissions from the parent folder/ directory.

Question

The screenshot shows the Hack The Box Academy web interface. At the top, there's a navigation bar with tabs for 'Hack The Box - Academy' and 'non-standard directory'. The main content area is titled 'Questions' and contains the following information:

- Target(s): 10.129.247.186 (ACADEMY-MISC-WS01)
- Life Left: 86 minute(s) + Terminate X
- RDP to 10.129.247.186 (ACADEMY-MISC-WS01) with user "htb-student" and password "Academy_WinFun!"
- Question: What system user has full control over the c:\users directory?
- Answer input field: bob.smith
- Buttons: Submit, Previous, Next, Mark Complete & Next

At the bottom right, it says 'Powered by HACKTHEBOX'.

Using this command `icacls C:/Users` I identified the user that has full control over user directory

The screenshot shows a Windows Command Prompt window with the following output:

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

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

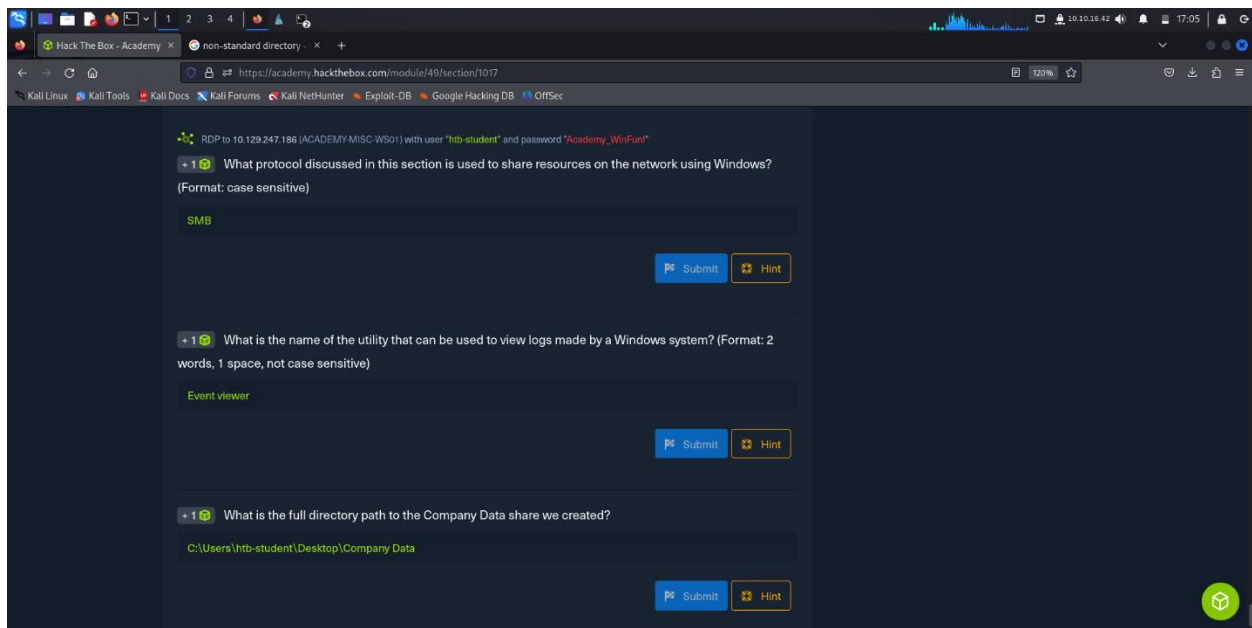
The output shows that the user 'bob.smith' has full control (F) over the C:/Users directory. The Command Prompt window is titled 'Select Command Prompt' and is open on a desktop with a taskbar showing the time as 8:01 AM on 9/15/2024.

1.4 NTFS & Share permissions

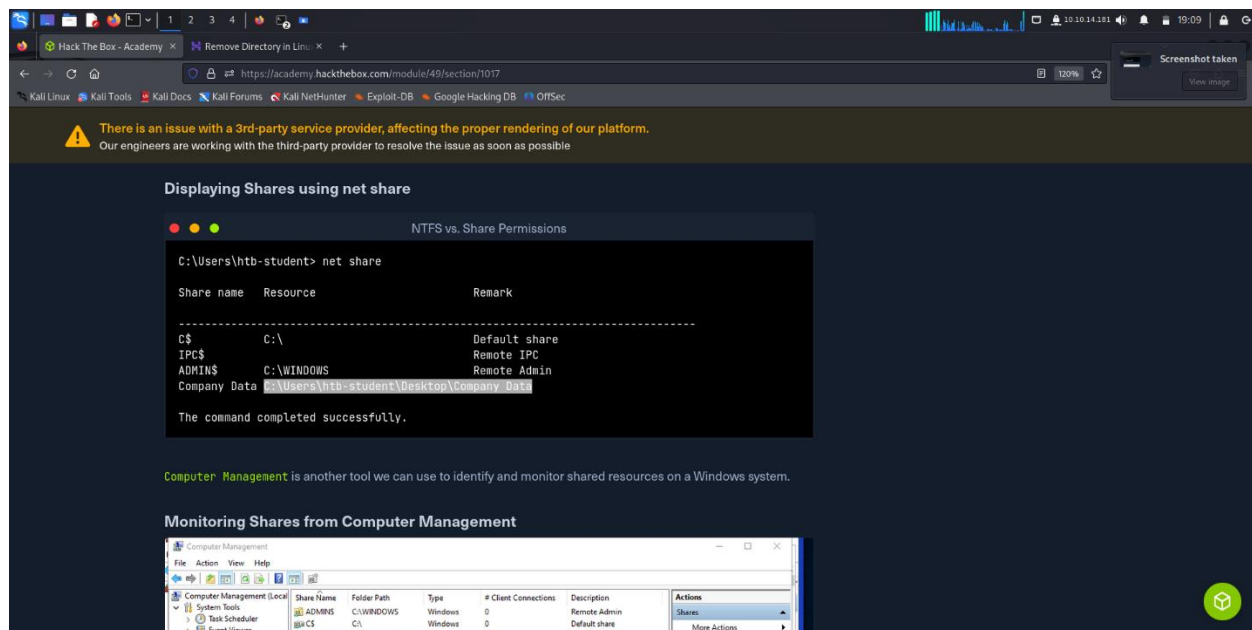
Permissions are crucial to computer as they give users either sysadmin or normal user privileges on what should be done on the computer, either Install Applications, run scripts, read or modify a file or a folder. In share permission it's a client-server situation, thus those resources being accessed must have share permissions on what should be done if one has access of them through the Server Message Block protocol (SMB).

SMB is the protocol being used to share resources on a network.

Event view is tool used to investigate actions completed on Windows, to view the logs.



The path company data was created on this topic



Using the command `smbclient` we can be able to view the available shares that are in the same network, and other tools such as NetShare, computer management and event viewer can be also used to view the shared resources.

1.5 Window services & processes

Services are crucial to Windows OS to running smoothly that is (Local, Network, System). These services are responsible for many functions within the Windows operating system, such as networking functions, performing system diagnostics, managing user credentials, controlling Windows updates, and more.

Processes run in the background, and they cannot be stopped or restarted those associated with installed applications can often be terminated without causing a severe impact on the operating system. Certain processes are critical and, if terminated, will stop certain components of the operating system from running properly.

In spite of using the `Get-Service` module, some other tools can be used to view the processes and services running and even to stop them, such Task manager and resource monitor.

Question

There is an issue with a 3rd-party service provider, affecting the proper rendering of our platform. Our engineers are working with the third-party provider to resolve the issue as soon as possible.

Questions

Answer the question(s) below to complete this Section and earn cubes!

Target(s): [Click here to spawn the target system!](#)

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

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.

`FontReaderUpdateService.exe`

[Submit](#) [Hint](#)

[Previous](#) [Next](#) [Mark Complete & Next](#)

Powered by HACKTHEBOX

Using the Get-Service module I found the service name.

```
File Action
FreeRDP: 10.129.239.141
deathtroike@kali: ~
Windows PowerShell
[deaths] Windows PowerShell
PS C:\Users\htb-student> Get-Service | Where-Object {$_.Name -like "reader*" } | fl
Name                : FontReaderUpdateService
DisplayName          : Font Reader Update Service
Status              : Running
DependentServices    : {}
ServicesDependedOn   : {}
CanPauseAndContinue : False
CanShutdown          : True
CanRestart          : True
ServiceType          : Win32OwnProcess, InteractiveProcess
Is                  :
Th
The above is the output of the Get-Service command.
PS C:\Users\htb-student>
```

1.6 Service Permission

Services being crucial to windows OS running smoothly, we should be mindful of permissions given to users or group of users, as they can be potential threat vector, used to load malicious programs, or scripts. The best option is to create service accounts apart from users accounts to manage this service.

1.7 Windows Sessions

These windows sessions can either be:

Interactive- initiated when user authenticates to a local/ domain system with existing credentials. Also initiated with logging directly into the system by requesting a secondary Logon session.

Non-interactive- they don't require login credentials. And are generally used by the Windows operating system to automatically start services and applications without requiring user interaction

1.8 interacting with windows OS

The Windows OS although of being a user-friendly platform, it can be interacted with in different ways using different tools, such using

Graphic user interface e.g., App, File, folder.

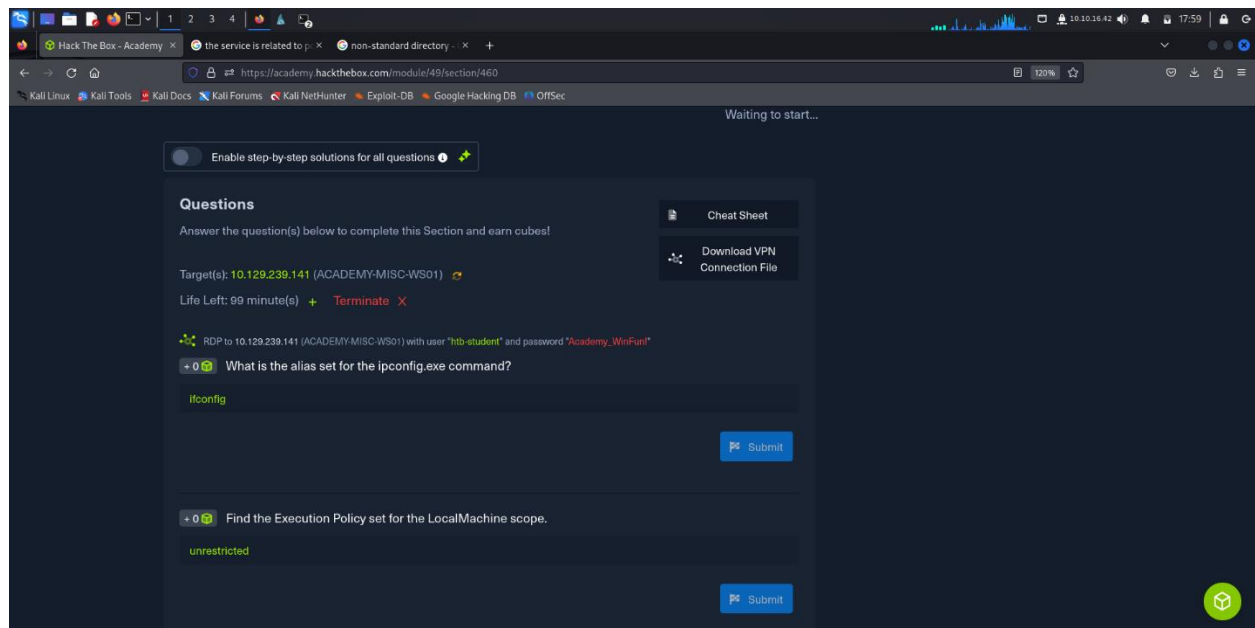
A command prompt but its no user friendly as you should know the commands that you want to run, as it allows you to interact directly with the computer.

PowerShell same as Command prompt but more powerful.

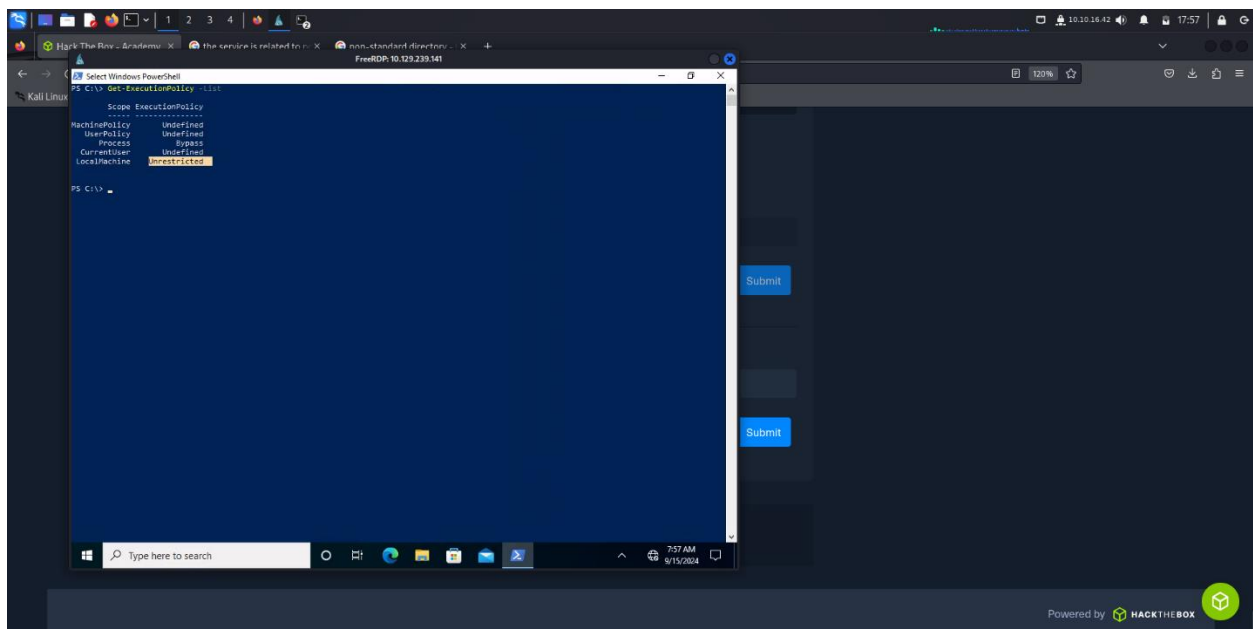
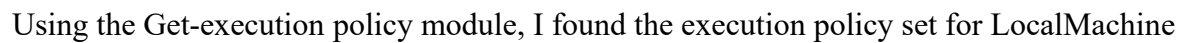
Remote Desktop you can access target OS and interact with.

Tho PowerShell allows you to run script, you can be unable to the run scripts on a system due to a security feature, execution policy, that attempts to prevent the execution of malicious scripts.

Question



Using the Get-Alias module, was able to alias of ipconfig



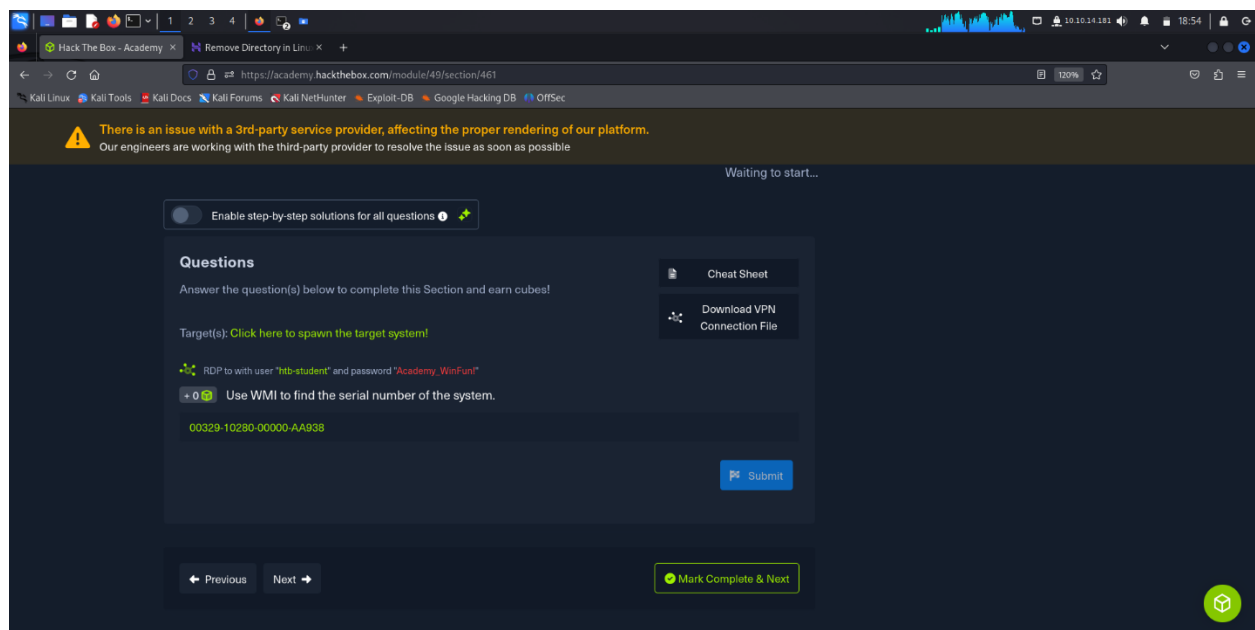
1.9 Windows Management Instrumentation (WMI)

It's a subsystem that provides sysadmin with tools to monitor systems. Plus is a core part of the Windows operating system. It's used to check the status of a local system or remote system, execute a command or even set or change user and group permissions, and many more, to make this possible it should be combined with PowerShell.

Combining with PowerShell we use Module like Get-WmiObject that can be use to list the information about a class.

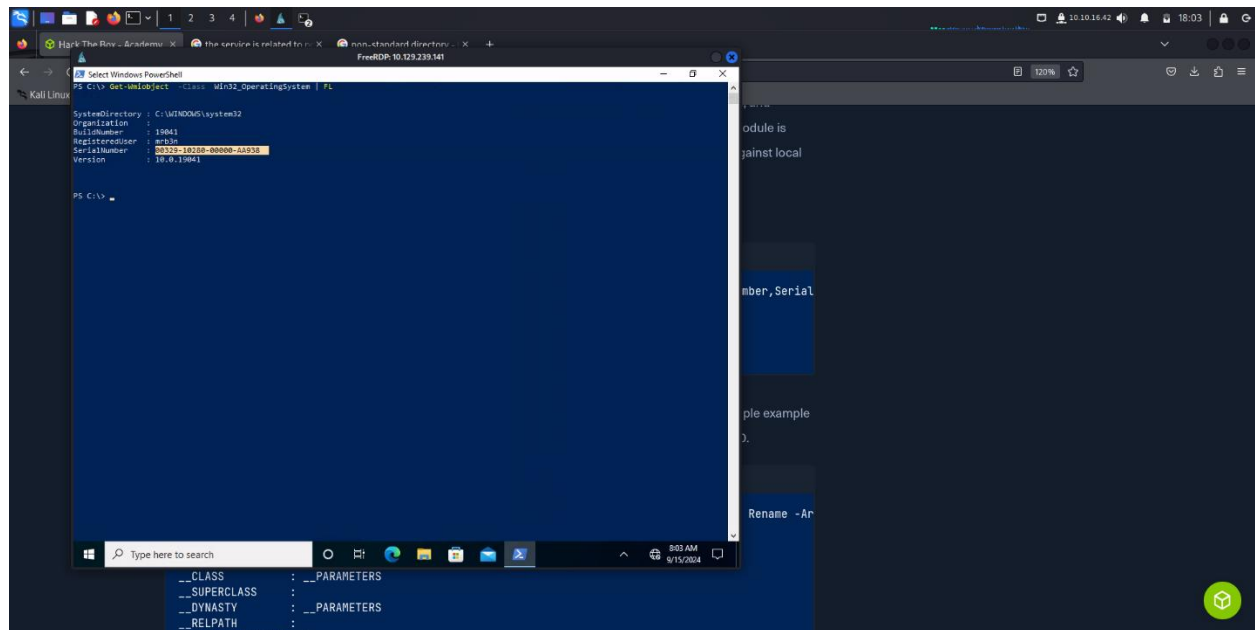
Also, it can be used with command prompt by using a command such as wmic os list brief to get the information of the OS.

Question



The screenshot shows a web browser window displaying a Hack The Box Academy question page. The browser's address bar shows the URL `https://academy.hackthebox.com/module/49/section/461`. A notification banner at the top states: "There is an issue with a 3rd-party service provider, affecting the proper rendering of our platform. Our engineers are working with the third-party provider to resolve the issue as soon as possible." Below this, a toggle switch for "Enable step-by-step solutions for all questions" is visible. The main content area is titled "Questions" and includes the instruction: "Answer the question(s) below to complete this Section and earn cubes!". The question text is: "Target(s): Click here to spawn the target system! RDP to with user 'htb-student' and password 'Academy_WinFun!' Use WMI to find the serial number of the system." A text input field contains the serial number "00329-10280-00000-AA938". To the right of the question, there are links for "Cheat Sheet" and "Download VPN Connection File". A "Submit" button is located at the bottom right of the question area. At the bottom of the page, there are "Previous" and "Next" navigation buttons, a "Mark Complete & Next" button, and a green cube icon in the bottom right corner.

I used Get-Wmiobject to the serial number of the system.



1.10 Microsoft Management Console (MMC)

It's a tool that used to group snap-ins, or administrative tools, to manage hardware, software, and network components within a Windows host.

On windows using the mmc tool we can create and distribute tools to users, it utilizes the concept of snap-ins.

1.11 Windows Subsystem for Linux (WSL)

Its feature of the Windows OS that enables you to run a Linux file system, along with Linux command-line tools and GUI apps, natively on Windows. This allows to run the Linux in a bash shell with a distro of choice.

1.12 Desktop Experience vs. Server Core

In this topic learnt about Server core using the PowerShell and command-line for its management and configuration and in spite of lacking a GUI, some graphical programs are still supported, such as Registry Editor, Notepad.

And interaction on command-line it has lower management requirements, a smaller attack surface, and uses less disk space and memory than its Desktop Experience (GUI).

1.13 Windows Security

Security is crucial aspect in computer, a network, system or even at personal level, thus ensuring the security in computer it improves reliability, integrity and confidentiality. On windows as a product of Microsoft, there are patches of security released to improve the overall computer security.

Also, computer has a set identifier that's a unique number that each registered user has, and they are added to user's access token to identify all actions that the user is authorized to take. And in user account control there is an admin that oversees what should be done on the computer thus prevents malicious activities.

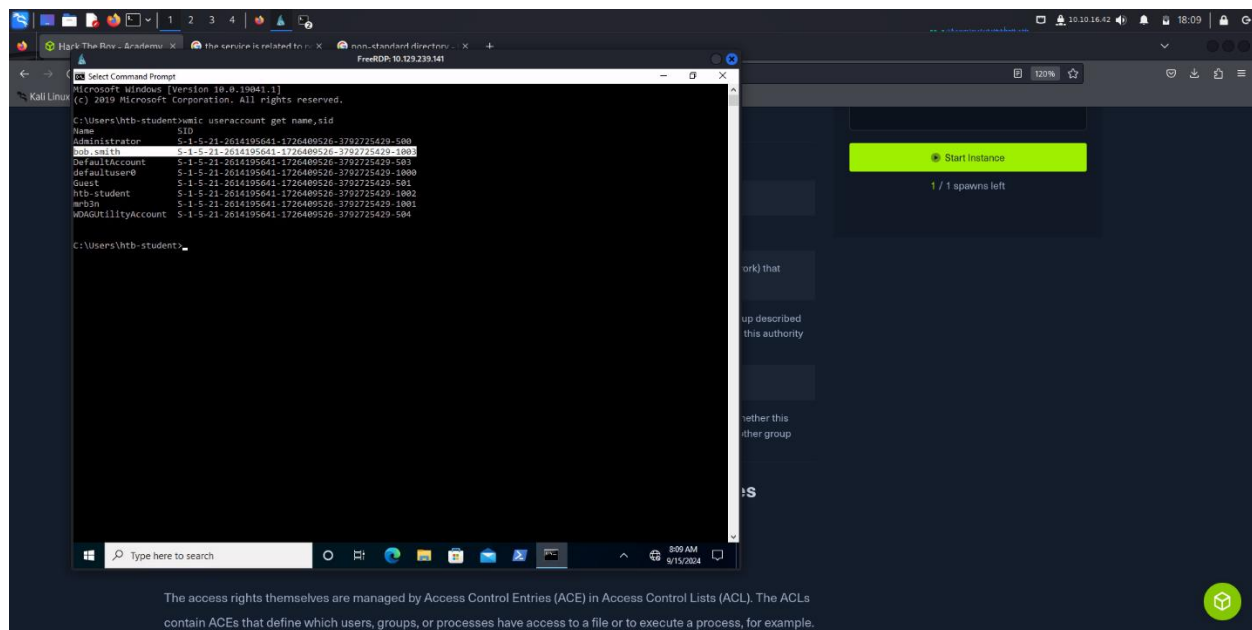
Windows also has a window defender that has a built-in antivirus. It has several features such as real-time protection, which protects the device from known threats in real-time and cloud-delivered protection, which works in conjunction with automatic sample submission to upload suspicious files for analysis. Another feature is Tamper Protection, which prevents security settings from being changed through the Registry, PowerShell.

Question

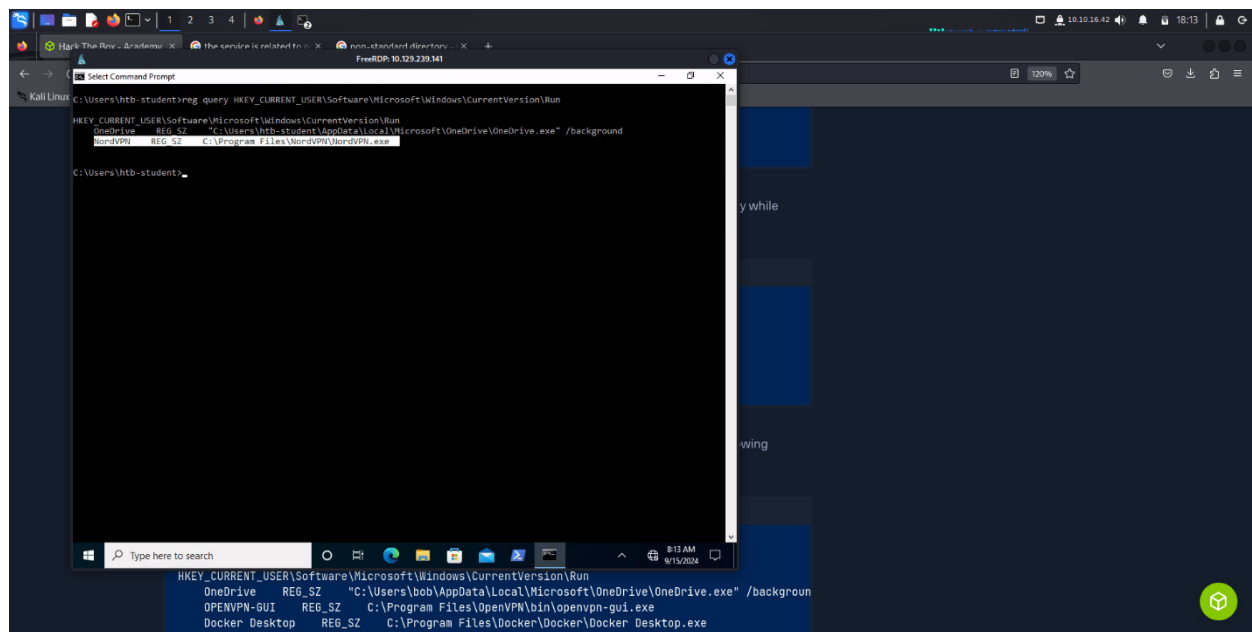
The screenshot shows a web browser window with the URL <https://academy.hackthebox.com/module/49/section/462>. The page displays a security quiz with the following content:

- A warning banner at the top: "There is an issue with a 3rd-party service provider, affecting the proper rendering of our platform. Our engineers are working with the third-party provider to resolve the issue as soon as possible." Below this, it says "Answer the question(s) below to complete this section and earn codes!".
- A button labeled "Download VPN Connection File".
- A target instruction: "Target(s): Click here to spawn the target system!".
- A hint: "RDP to with user 'htb-student' and password 'Academy_WinFun!'".
- A question: "+ 1 Find the SID of the bob.smith user." Below the question, the answer "S-1-5-21-2614195641-1726409526-3792725429-1003" is displayed.
- A "Submit" button for the first question and a "Hint" button.
- A second question: "+ 1 What 3rd party security application is disabled at startup for the current user? (The answer is case sensitive)." Below the question, the answer "NordVPN" is displayed.
- A "Submit" button for the second question.
- Navigation buttons at the bottom: "Previous", "Next", and "Mark Complete & Next".

Using this command wmic useraccount get name,sid



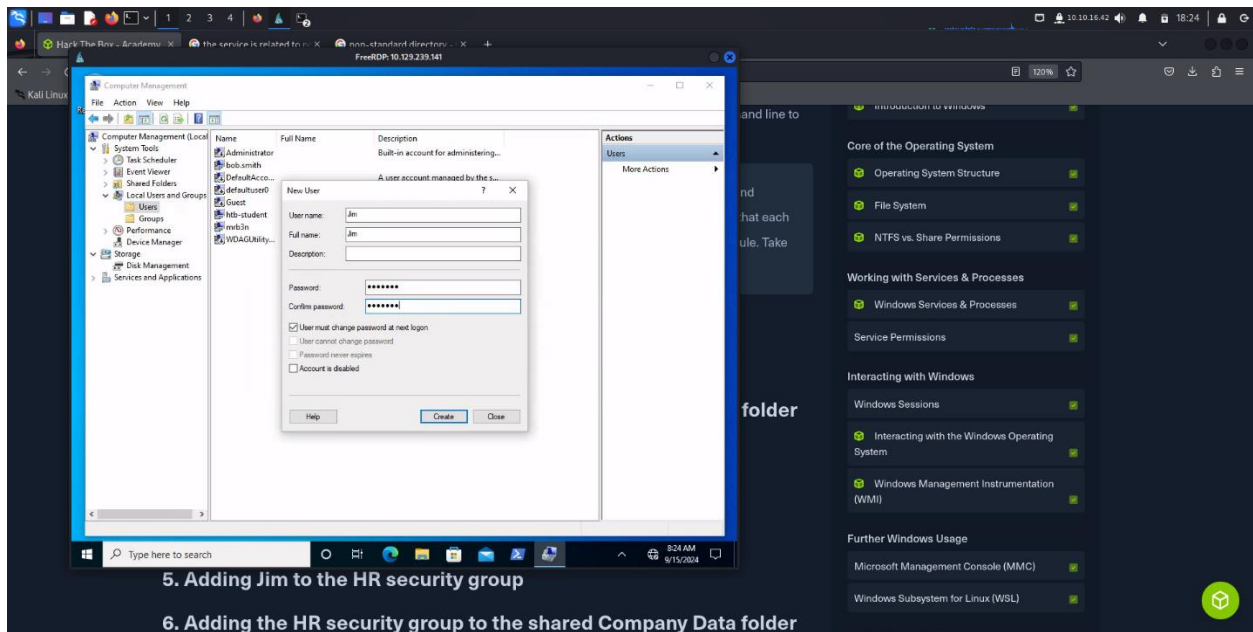
Using Registry (Reg) command I queried the registry hive to list all programs that are scheduled to run automatically when the current user logs in



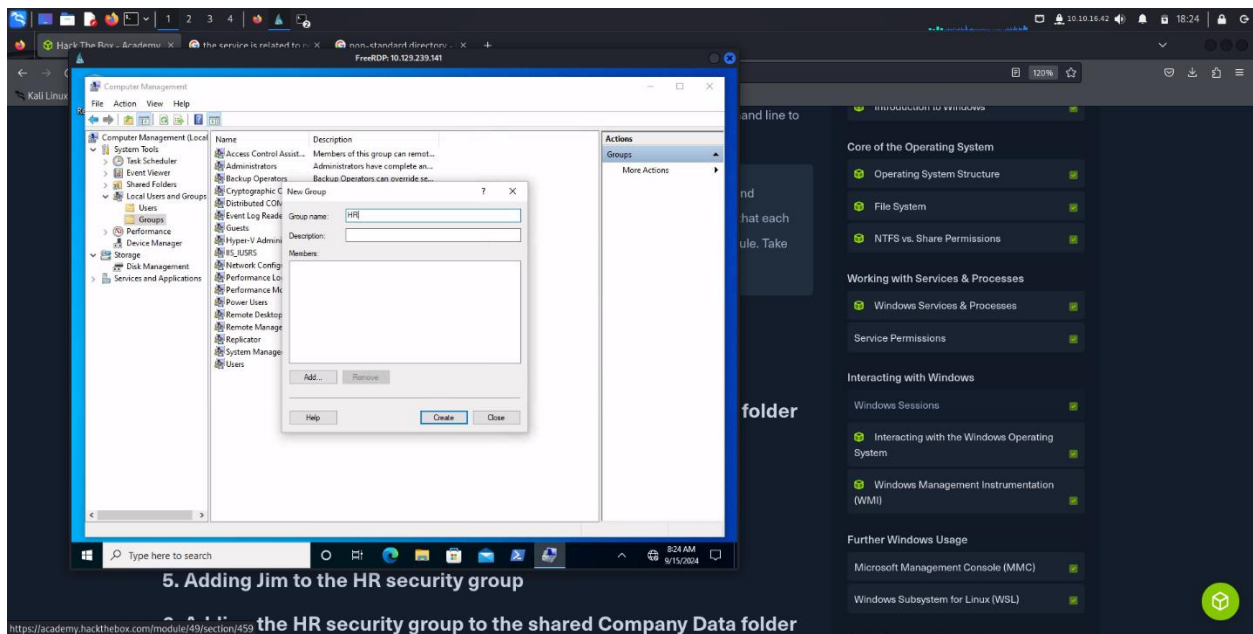
1.14 Skills Assessment

This was testing the skills learnt through the module, such I had to incorporate some of the commands I learnt about, as I was tasked to

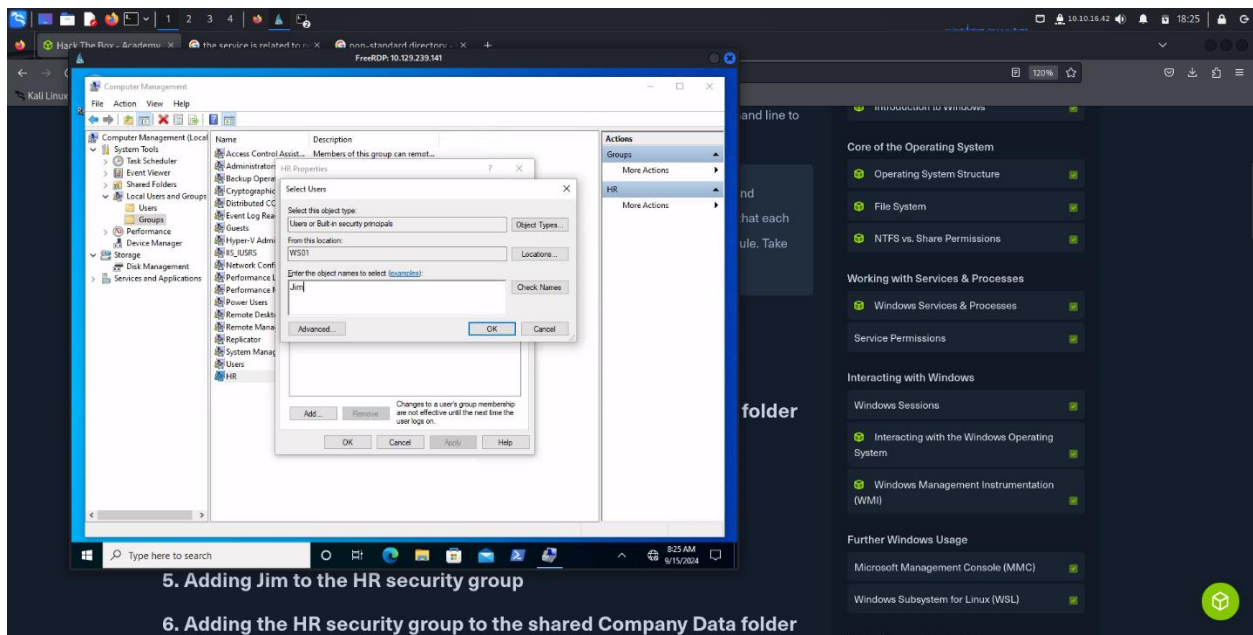
1. Creating a shared folder called Company Data
2. Creating a subfolder called HR inside of the Company Data folder
3. Creating a user called Jim
 - Uncheck: User must change password at logon



4. Creating a security group called HR

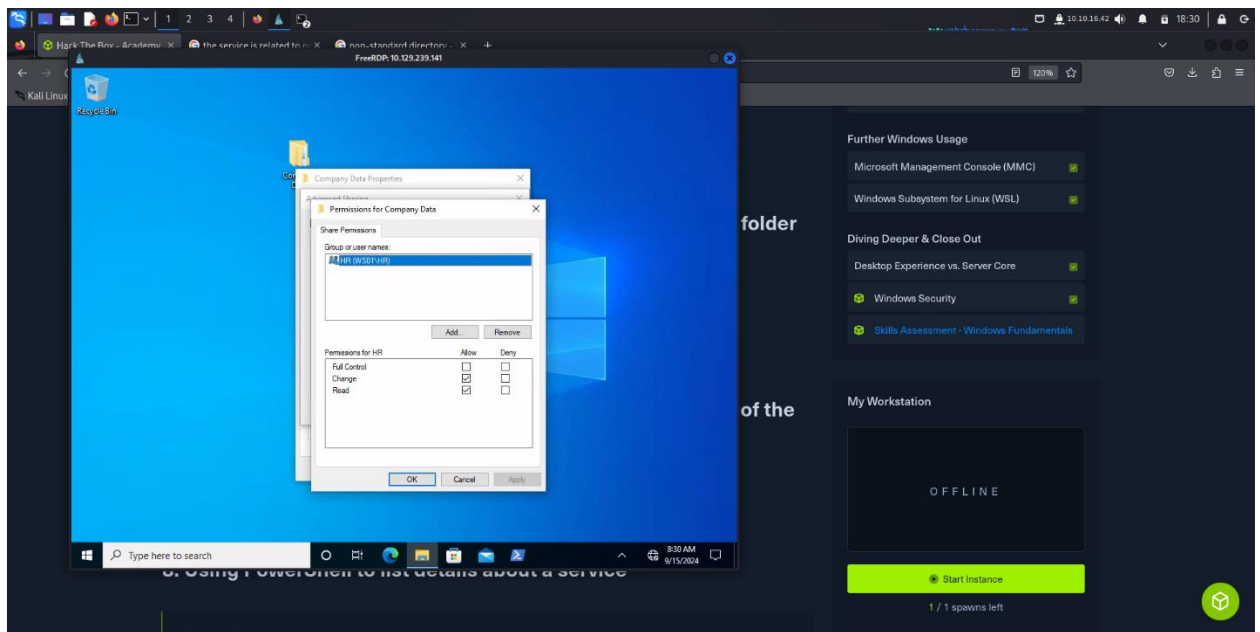


5. Adding Jim to the HR security group

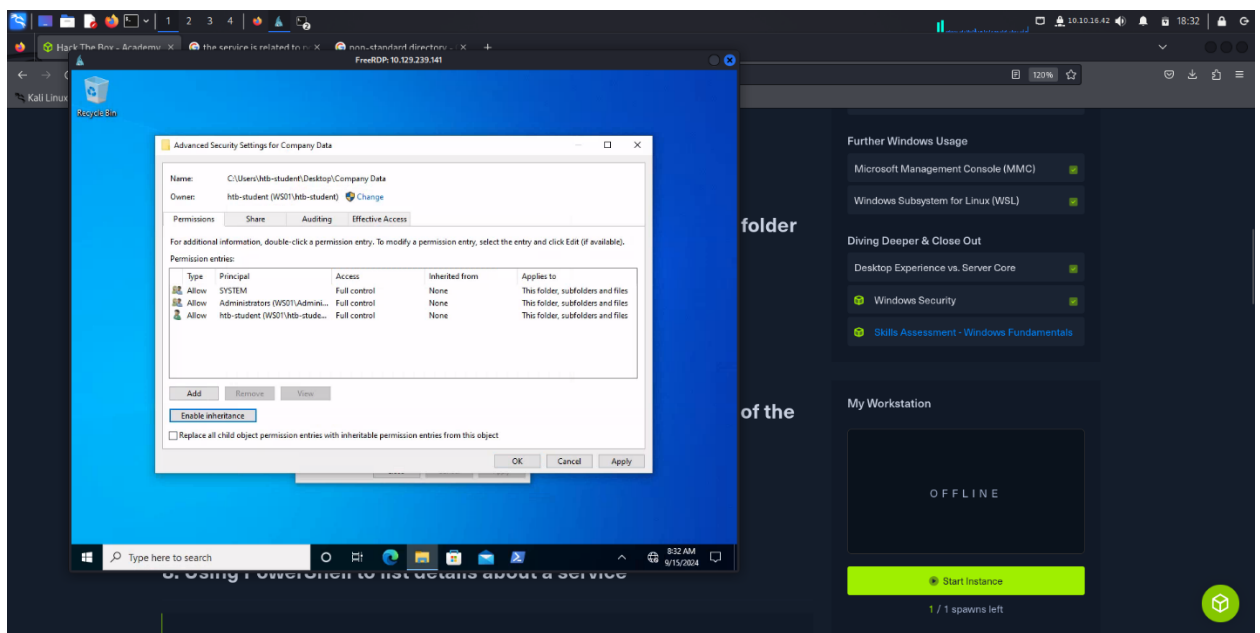


6. Adding the HR security group to the shared Company Data folder and NTFS permissions list

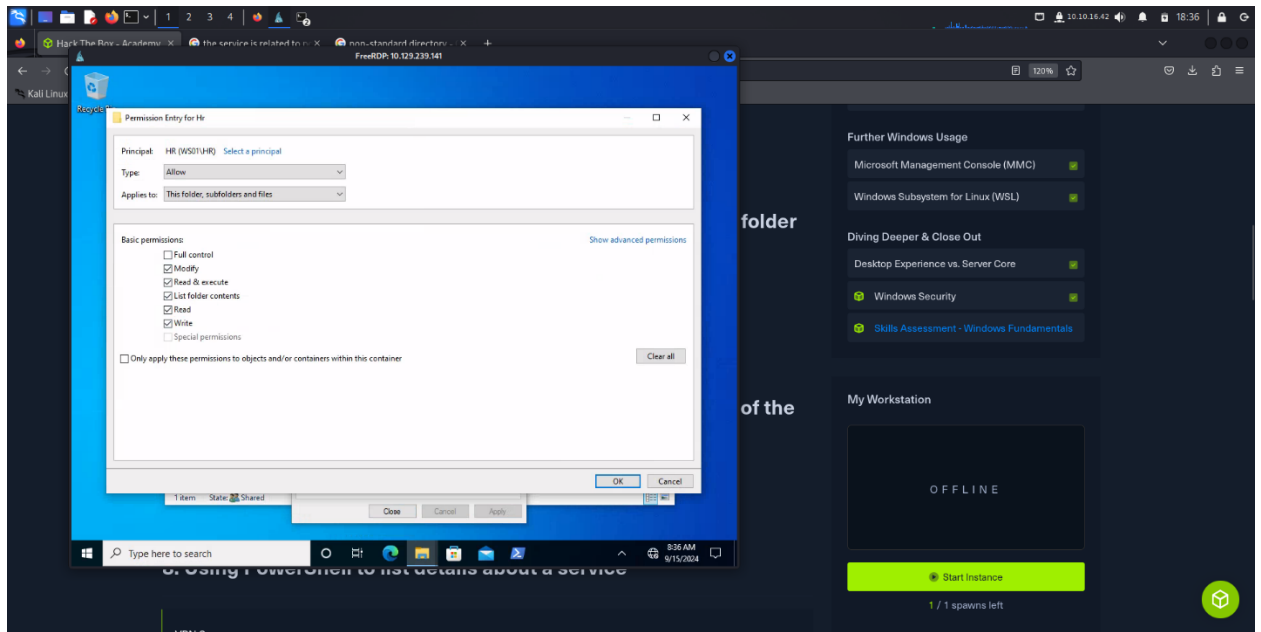
- Remove the default group that is present
- Share Permissions: Allow Change & Read



- Disable Inheritance before issuing specific NTFS permissions

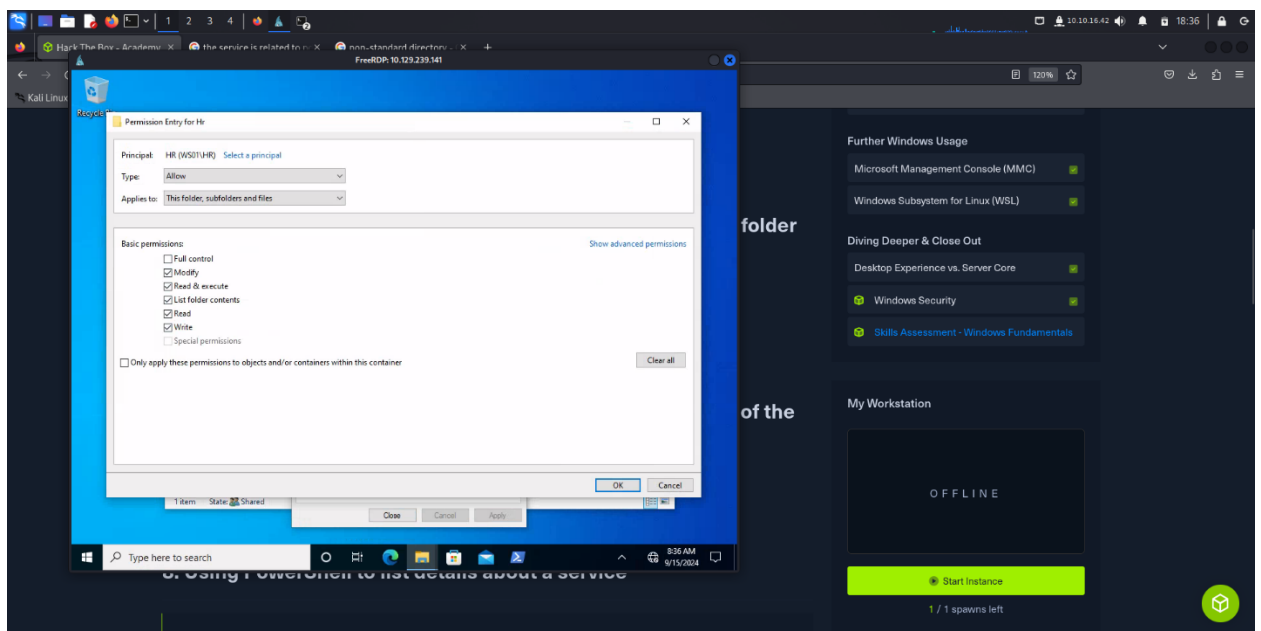


- NTFS permissions: Modify, Read & Execute, List folder contents, Read, Write



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



8. Using PowerShell to list details about a service

Questions

The screenshot displays the Hack The Box Academy interface, which is a web-based platform for learning and practicing penetration testing. The interface is dark-themed and features a sidebar on the left with navigation links for various tools and resources. The main content area is titled "Questions" and contains a series of questions and answers related to Windows permissions and services.

Questions

Answer the question(s) below to complete this Section and earn cubes!

Target(s): 10.129.239.141 (ACADEMY-MISC-WS01) 🚩

Life Left: 46 minute(s) + **Terminate** ✕

🔗 RDP to 10.129.239.141 (ACADEMY-MISC-WS01) with user "htb-student" and password "Academy_WinFull"

+ 1 📄 What is the name of the group that is present in the Company Data Share Permissions ACL by default?

Everyone

Submit **Hint**

+ 1 📄 What is the name of the tab that allows you to configure NTFS permissions?

Security

Submit **Hint**

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

wuauclt

Submit

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

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

Submit **Hint**

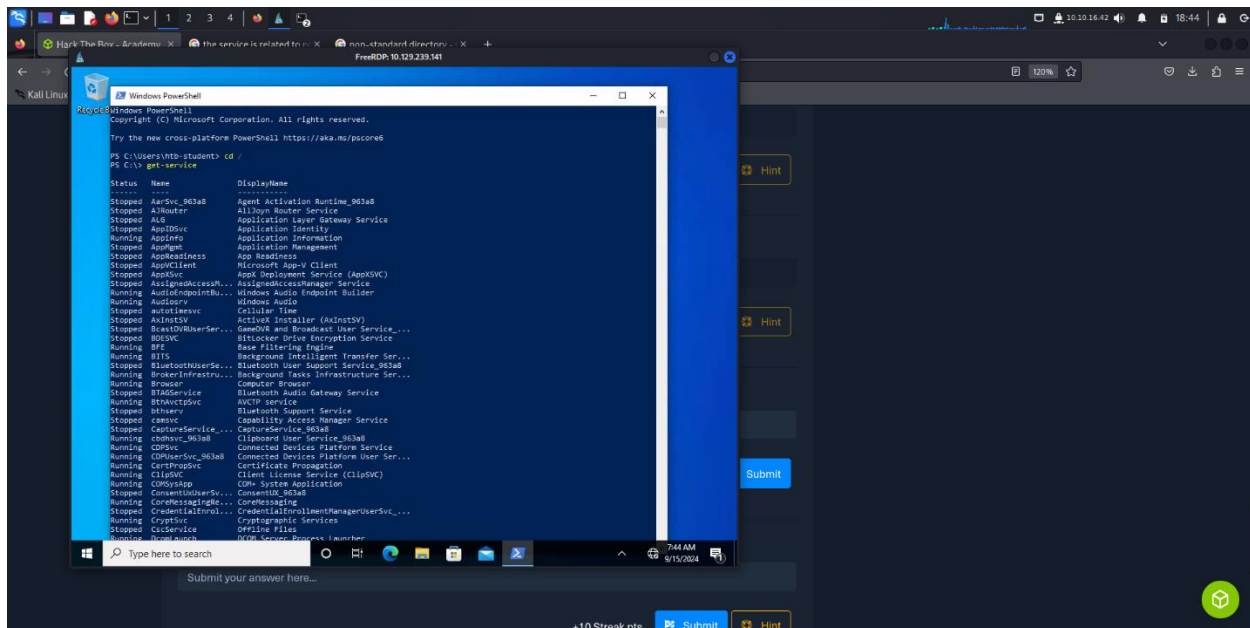
+ 1 📄 List the SID associated with the HR security group you created.

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

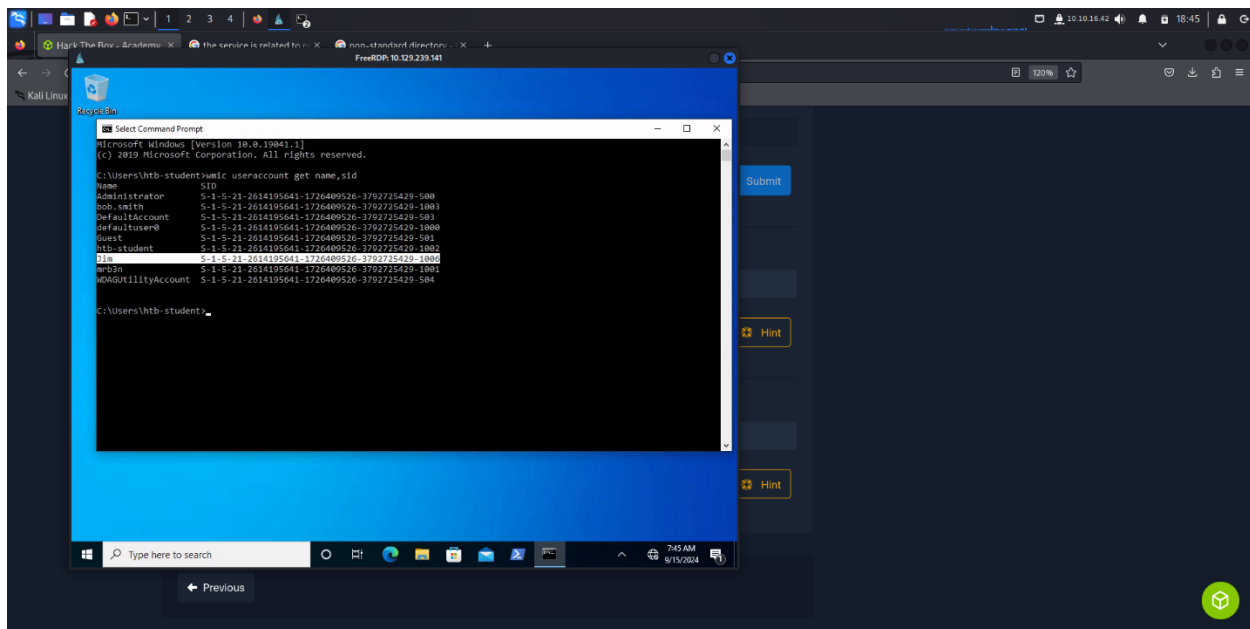
Submit **Hint**

Previous **Finish**

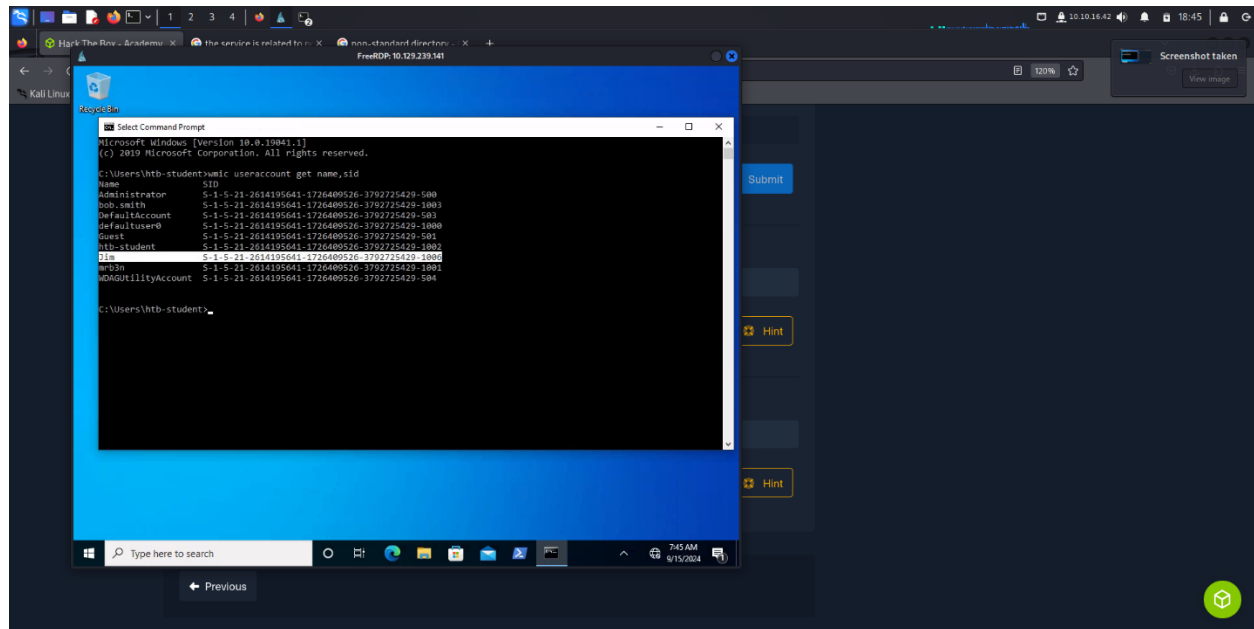
Used the get-service module to find service associated with windows update to wuauserv



Used the wmic to request user account to give out the name and SID of users registered as users in the computer, to get Jim SID



Used the wmic to request group account to give out the group-name and SID of group registered in the computer, to get HR group SID



2. In conclusion

This module gave me an understanding of the windows operation, and how permissions are configured, and its crucial in ensuring access level on user or group. To use build in windows tools such as registry, computer management, task manager, service and event viewer to monitor services and processes. Plus, to interact with OS, and the security aspects. Through this understanding to operations, I'm able to diagnose and troubleshoot a machine to know why it's not functioning properly, and to prevent exploits and vulnerabilities.