

WINDOWS FUNDAMENTALS

ASSIGNMENT REPORT



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

1. INTRODUCTION

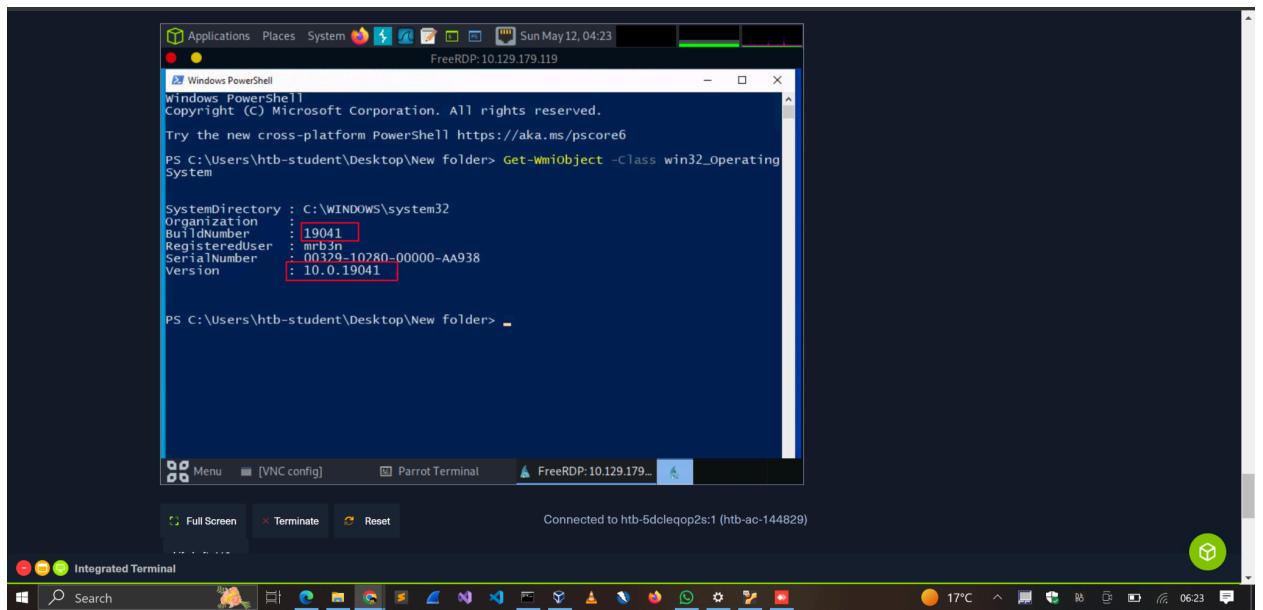
This report documents my completion of the **Windows Fundamentals** Module on the HacktheBox platform. The module covered the fundamentals required to work comfortably with the Windows operating system. It explains the Windows operating system structure and its file system, processes management, windows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



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\htb-student\Desktop\New folder> Get-WmiObject -Class win32_OperatingSystem

SystemDirectory : C:\WINDOWS\system32
Organization    :
BuildNumber    : 19041
RegisteredUser : mrb3n
SerialNumber   : 00329-10280-00000-AA938
Version        : 10.0.19041

PS C:\Users\htb-student\Desktop\New folder>
```

The screenshot shows a Windows PowerShell window running on a Windows 10 system. The command `Get-WmiObject -Class win32_OperatingSystem` is run, and the output shows various system properties. The `BuildNumber` property is explicitly highlighted with a red box. The output also includes the organization name, registered user, serial number, and version number.

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.

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\htb-student\Desktop>New folder> Get-WmiObject -Class win32_OperatingSystem

SystemDirectory : C:\WINDOWS\system32
Organization :
BuildNumber : 19041
RegisteredUser : mrb2n
SerialNumber : 00329-10280-00000-AA938
Version : 10.0.19041

PS C:\Users\htb-student\Desktop>New folder> (Get-WmiObject -Class win32_OperatingSystem).Caption
Microsoft Windows 10 Enterprise
PS C:\Users\htb-student\Desktop>New folder>

```

Core of the Operating System

- 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 a file named “flag”.

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\htb-student> cd C:\
PS C:\> dir

Directory: C:\

Mode LastWriteTime Length Name
---- -- -- -- --
d---- 8/23/2021 10:20 AM 75a#ac25572675a9bfed2405602
d---- 3/1/2022 1:14 AM PerfLogs
d---- 12/7/2022 4:05 PM Program Files
d---- 1/31/2022 3:01 PM Program Files (x86)
d---- 1/31/2022 3:02 PM Users
d---- 1/31/2022 3:02 PM Windows

PS C:\> dir Academy
Directory: C:\Academy

Mode LastWriteTime Length Name
---- -- -- -- --
-a--- 9/7/2020 12:17 PM 32 flag.txt

```

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

```

Windows PowerShell
PS C:\> cd Academy
PS C:\Academy> dir

Directory: C:\Academy

Mode                LastWriteTime     Length Name
----                -----        -----    -----
-a---       9/7/2020 12:17 PM          32 flag.txt

PS C:\Academy> type flag.txt
c8fe8d97d3a6e655ed7cf81e4d13c75
PS C:\Academy>

```

Flag

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.

```

Command Prompt
C:\Users\htb-student>icacls c:\users
c:\users Everyone:(OI)(CI)(RX)
          NT AUTHORITY\SYSTEM:(OI)(CI)(F)
          bob.smith:(OI)(CI)(F)
          BUILTIN\Administrators:(CI)(F)
          BUILTIN\Users:(OI)(CI)(RX)
Successfully processed 1 files; Failed processing 0 files
C:\Users\htb-student>

```

F => full access

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.

```
Applications Places System FreeRDP: 10.129.179.119 Sun May 12, 04:50
Command Prompt
C:\Users\htb-student>net share
Share name   Resource           Remark
-----       -----           -----
C$          C:\                 Default share
IPC$         IPC                Remote IPC
ADMIN$       C:\WINDOWS         Remote Admin
Company Data C:\Users\htb-student\Desktop\Company Data
The command completed successfully.

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

Shared folder

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**

```

Windows PowerShell
FreeRDP: 10.129.179.119
Sun May 12, 05:03

CanShutdown : False
CanStop : True
ServiceType : Win32OwnProcess, Win32ShareProcess
Name : FontCache
DisplayName : Windows Font Cache Service
Status : Running
DependentServices : {}
ServicesDependedOn : {}
CanPauseAndContinue : False
CanShutdown : True
CanStop : True
ServiceType : Win32OwnProcess, Win32ShareProcess
Name : FoxitReaderUpdateService
DisplayName : Foxit Reader Update Service
Status : Running
DependentServices : {}
ServicesDependedOn : {}
CanPauseAndContinue : False
CanShutdown : True
CanStop : True
ServiceType : Win32OwnProcess, InteractiveProcess
Name : EPPSVC
DisplayName : Group Policy Client
Status : Running
DependentServices : {}
ServicesDependedOn : {RPCSS, Mup}
CanPauseAndContinue : False
CanShutdown : False
CanStop : True
ServiceType : Win32OwnProcess, Win32ShareProcess
Name : Test11Service

```

Connected to htб-5dcleqop2s:1 (htб-ac-144829)

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.

```

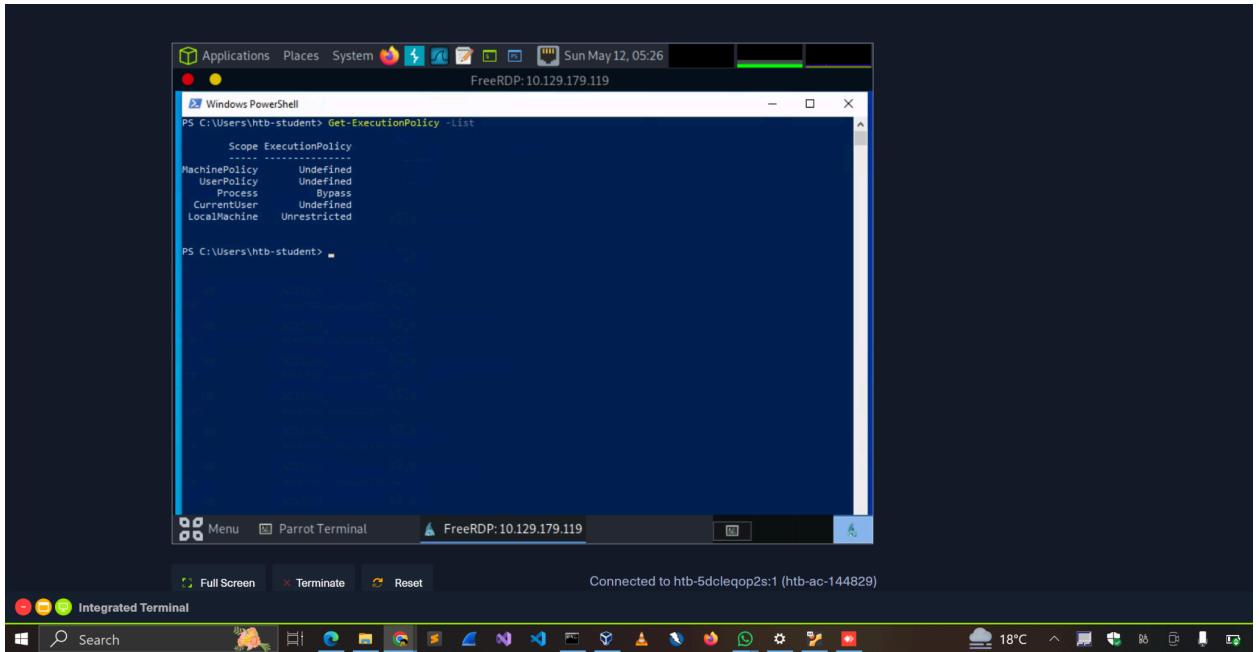
Windows PowerShell
FreeRDP: 10.129.179.119
Alias gmo -> Get-Module
Alias gp -> Get-Process
Alias gpr -> Get-Print
Alias gpv -> Get-ItemPropertyValue
Alias group -> Group-Object
Alias gsnp -> Get-PSSession
Alias gsnp -> Get-PSSnapin
Alias gv -> Get-Variable
Alias gv -> Get-Unique
Alias gv -> Get-Variable
Alias gwmi -> Get-WmiObject
Alias h -> Get-History
Alias history -> Get-History
Alias icm -> Invoke-Command
Alias iex -> Invoke-Expression
Alias ifconfig -> inconfig.exe
Alias ihy -> Invoke-History
Alias ii -> Invoke-Item
Alias ipal -> Import-Alias
Alias ipcsv -> Import-Csv
Alias ipm -> Import-Module
Alias iopen -> Import-PSSession
Alias irm -> Invoke-RestMethod
Alias ise -> powershell_ise.exe
Alias iwm -> Invoke-WMIMethod
Alias iwr -> Invoke-WebRequest
Alias iwr -> Invoke-WebRequest
Alias lpr -> Out-Printer
Alias ls -> Get-ChildItem
Alias man -> help
Alias md -> mkdir
Alias measure -> Measure-Object
Alias mi -> Move-Item
Alias mount -> New-PSDrive

```

Connected to htб-5dcleqop2s:1 (htб-ac-144829)

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

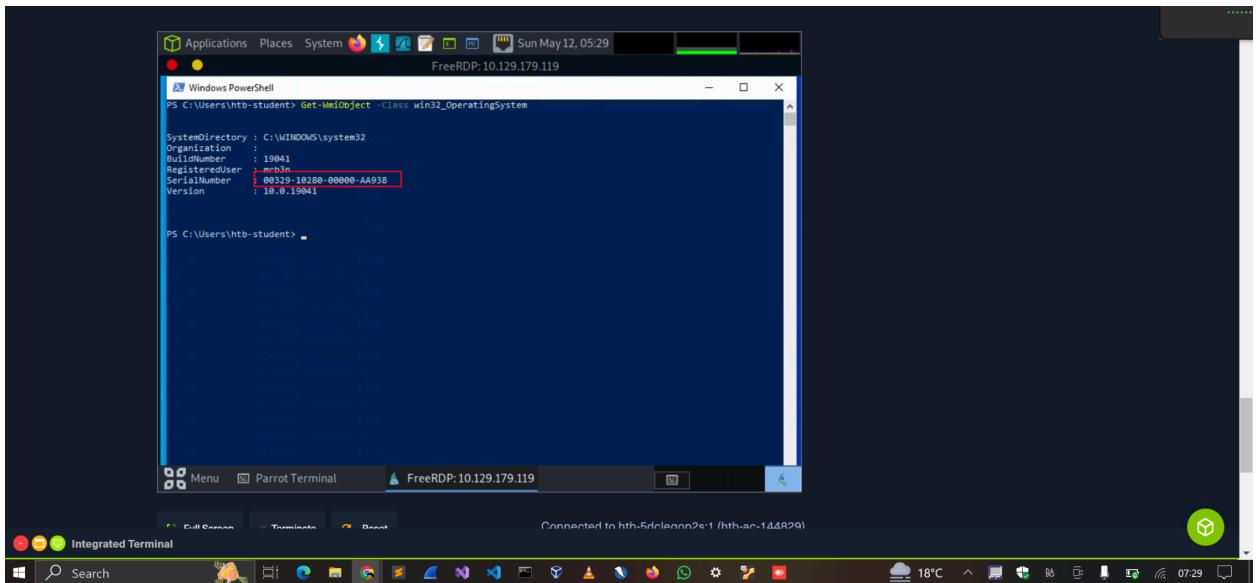
From the screenshot below, the execution policy of the LocalMachine is set to unrestricted.



```
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>
```

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



```
PS C:\Users\htb-student> Get-WmiObject -Class win32_OperatingSystem
SystemDirectory : C:\WINDOWS\system32
Organization :
DomainName : 192.168.1.11
RegisteredUser : bob.smith
SerialNumber : 00329-10280-00000-AA93B
Version : 10.0.19041

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

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.

```
Windows PowerShell
PS C:\Users> Get-WmiObject -Class win32_useraccount

AccountType : S12
Caption : WS01\Administrator
Domain : WS01
SID : S-1-5-21-2614195641-1726409526-3792725429-500
FullName :
Name : Administrator

AccountType : S12
Caption : bob.smith
Domain : WS01
SID : S-1-5-21-2614195641-1726409526-3792725429-1003
FullName :
Name : bob.smith

AccountType : S12
Caption : WS01\DefaultAccount
Domain : WS01
SID : S-1-5-21-2614195641-1726409526-3792725429-503
FullName :
Name : DefaultAccount

AccountType : S12
Caption : WS01\defaultuser0
Domain : WS01
SID : S-1-5-21-2614195641-1726409526-3792725429-1000
FullName :
Name : defaultuser0

AccountType : S12
Caption : WS01\Guest
Domain : WS01
```

Connected to htb-5dcleqop2s:1 (htb-ac-144829)

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

```
Windows PowerShell
PS C:\Users> reg query HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

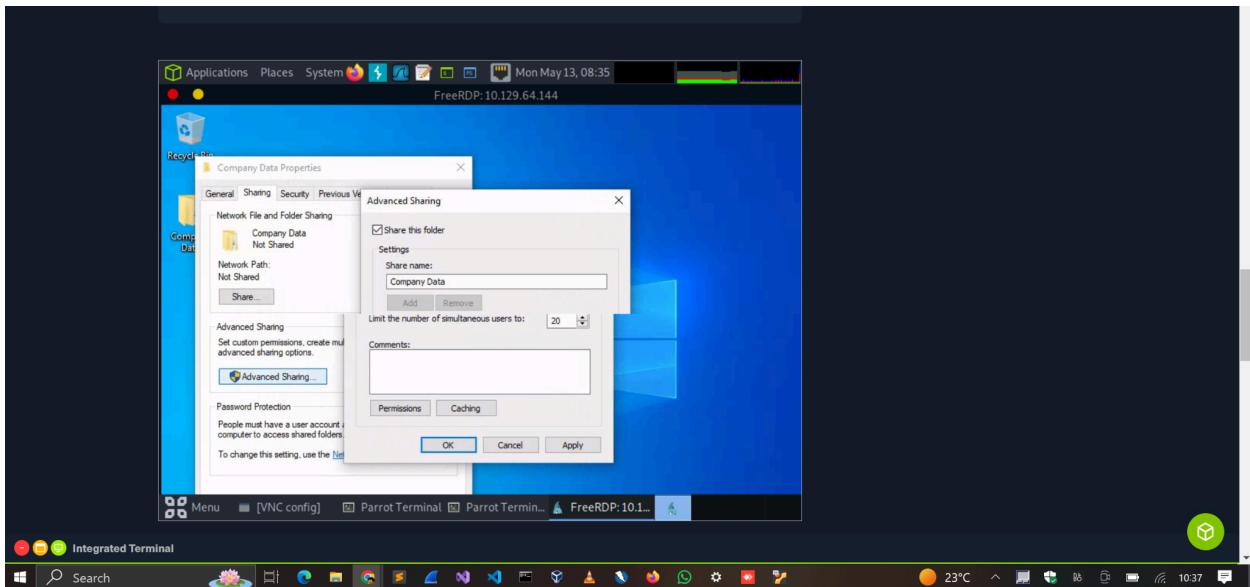
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
OneDrive REG_SZ "C:\Users\htb-student\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
NorVPN REG_SZ C:\Program Files\NorVPN\NorVPN.exe
```

NorVPN

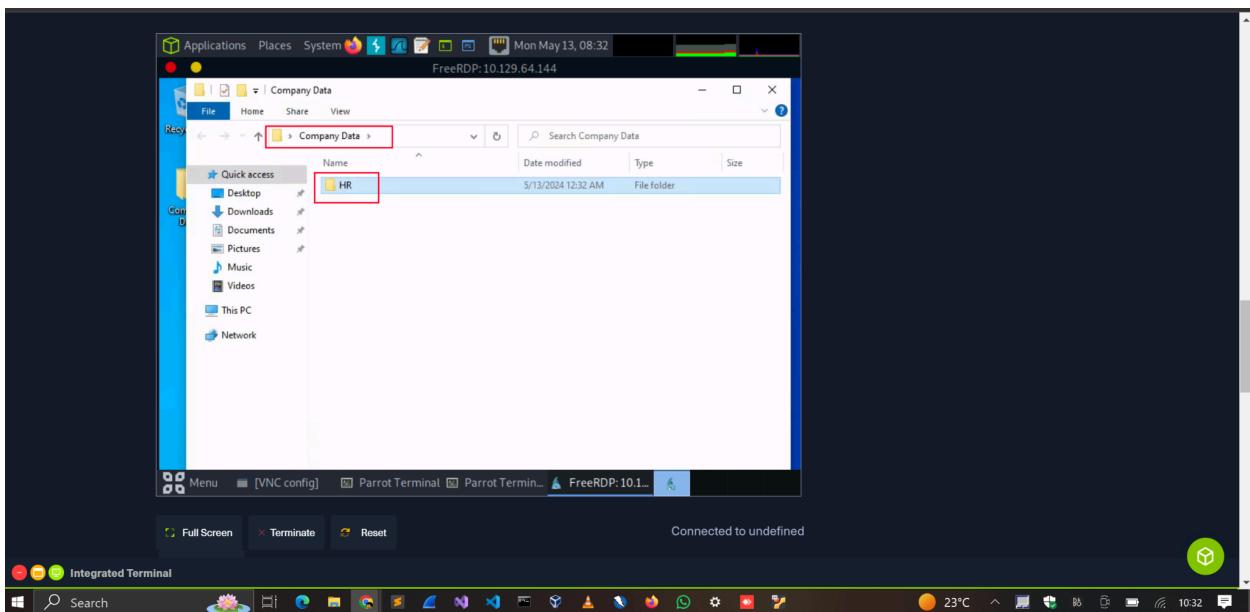
Connected to htb-5dcleqop2s:1 (htb-ac-144829)

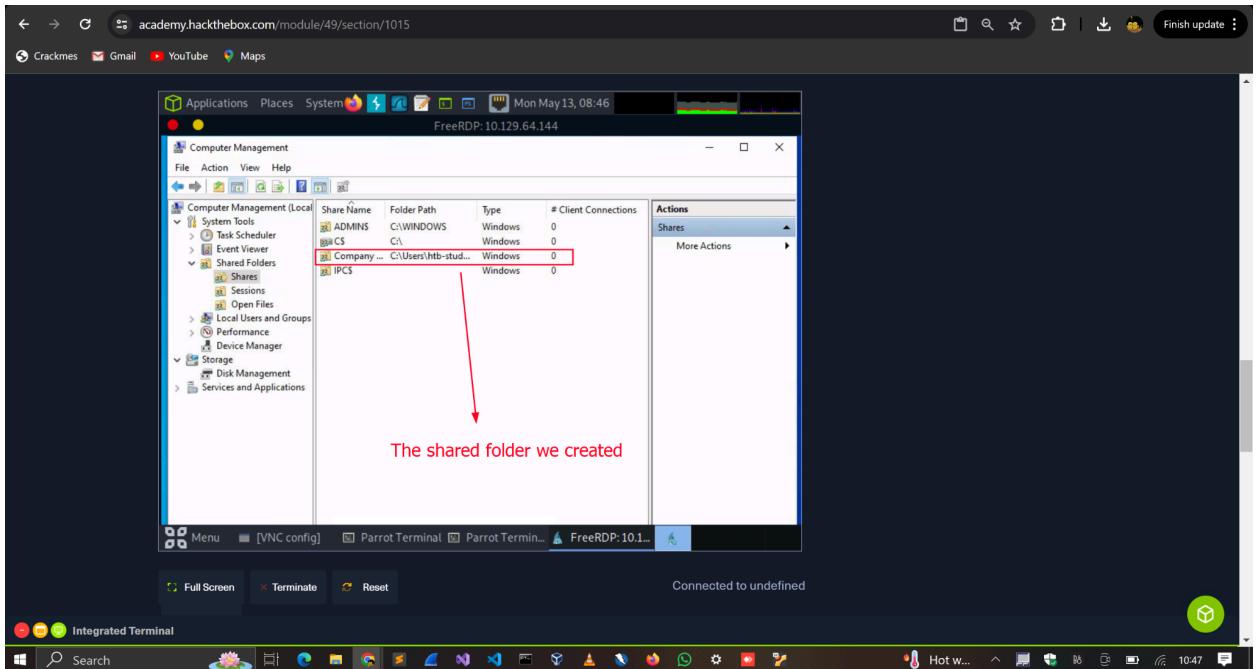
Skills Assessment

1. Creating a shared folder called Company Data

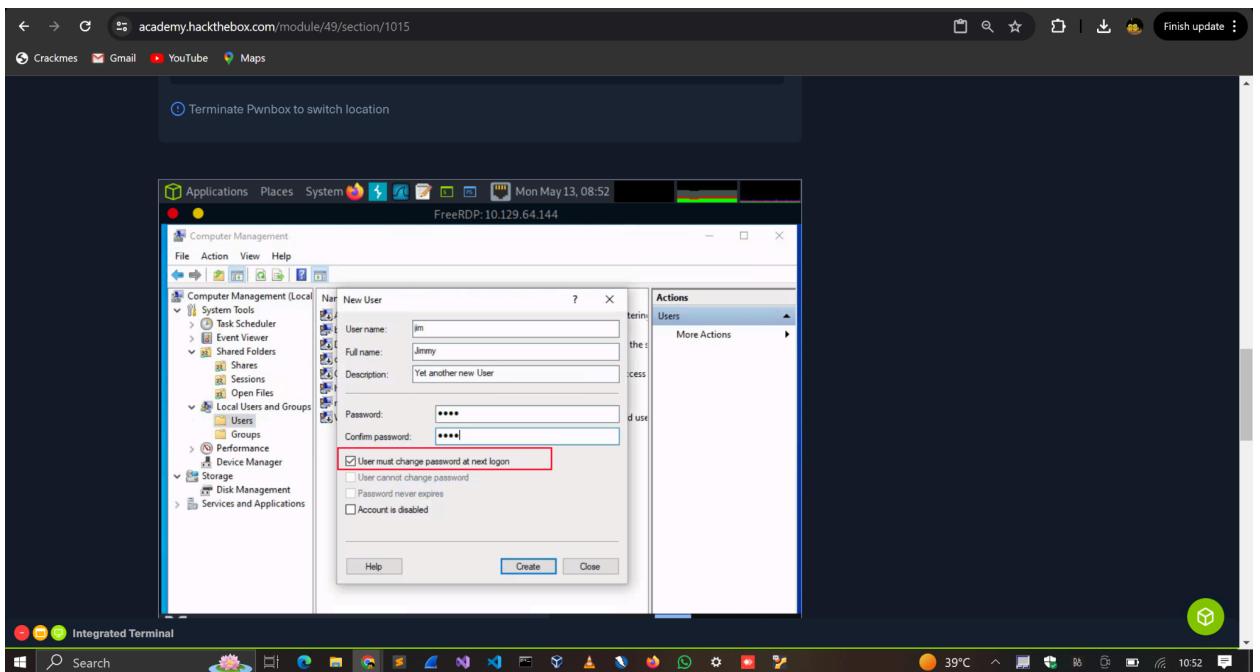


2. Creating a subfolder called HR inside of the Company Data folder



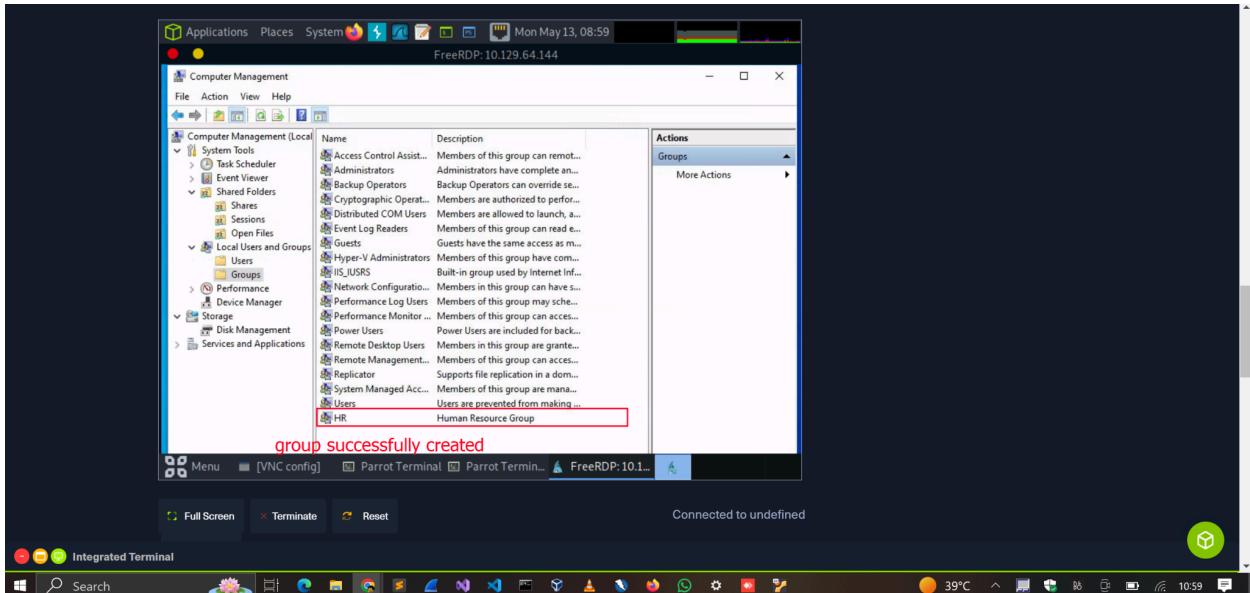


3. Creating a user called Jim Uncheck: User must change password at logon

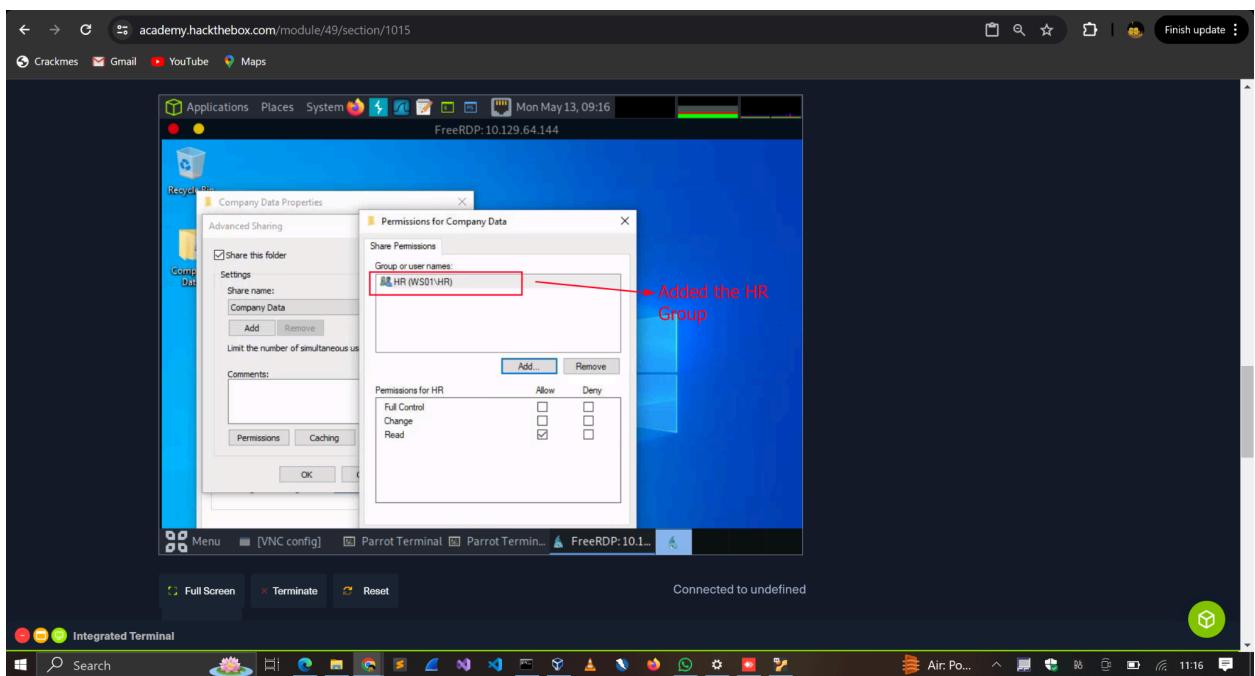
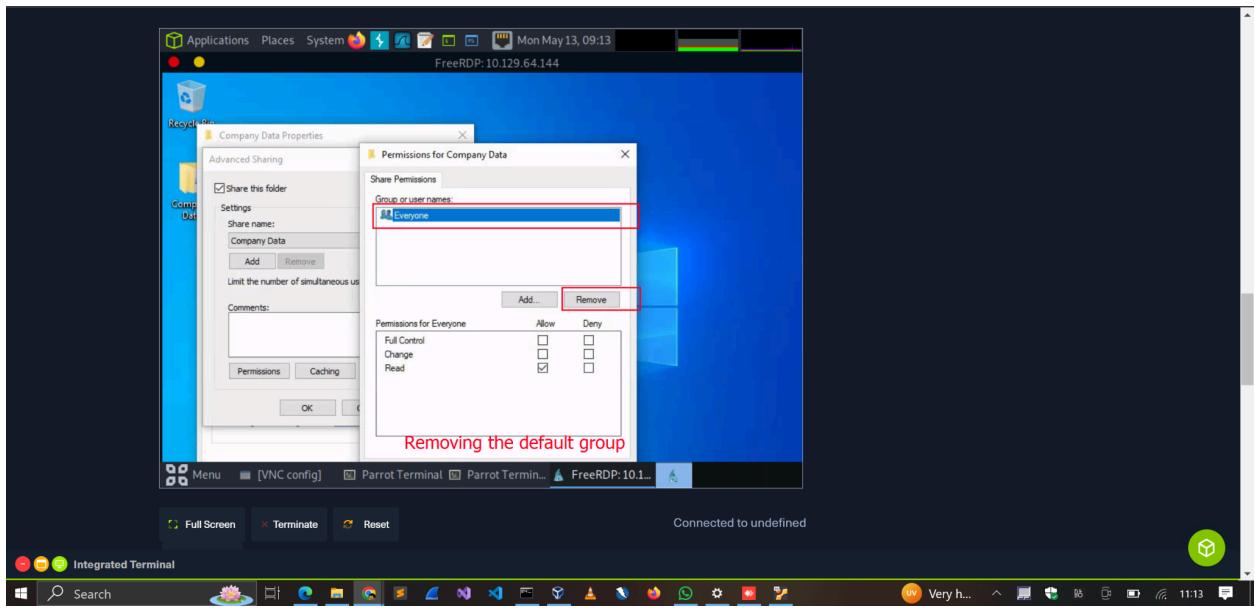


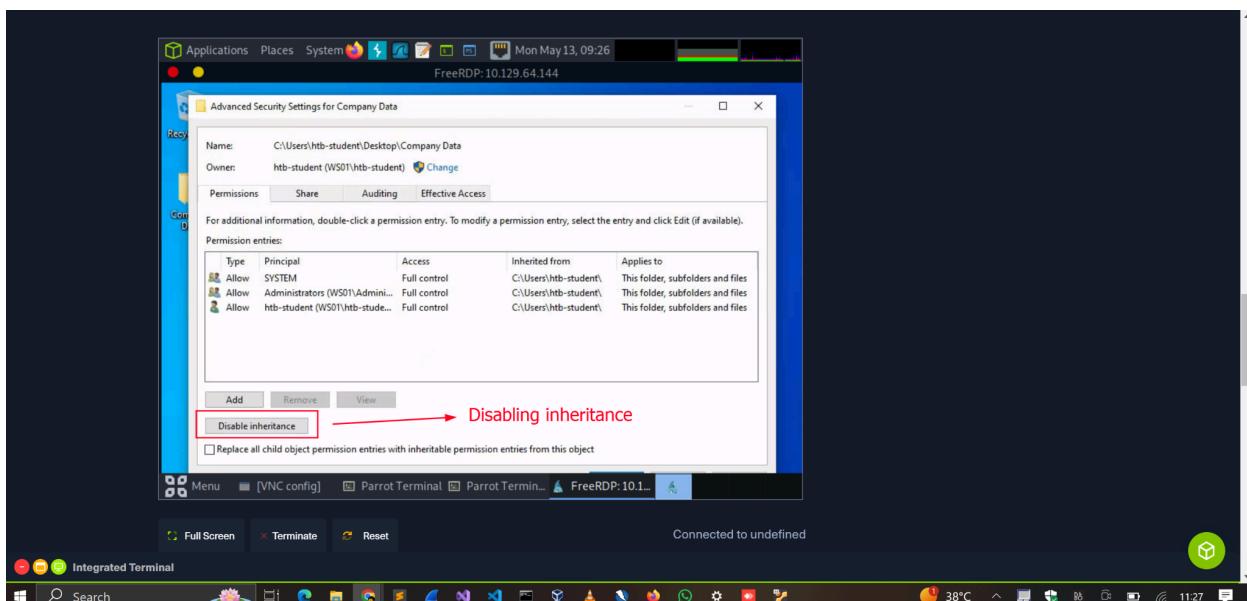
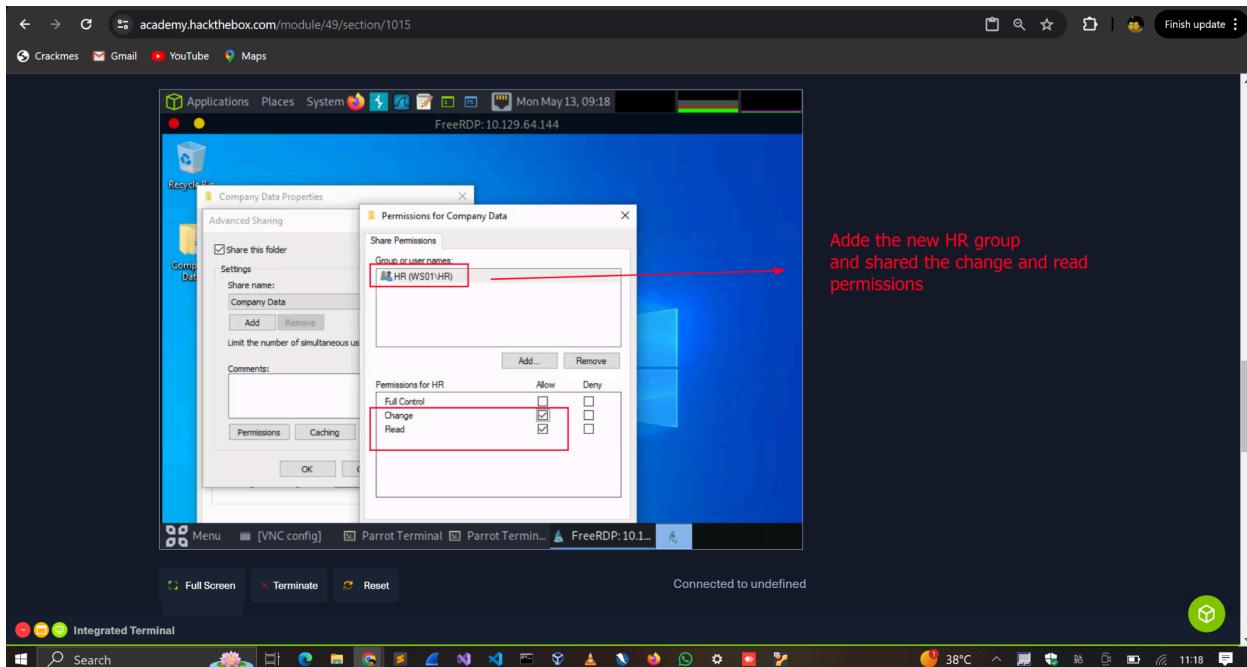
4. Creating a security group called HR

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





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.

+ 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

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.

FreeRDP: 10.129.95.201

```
Windows PowerShell
PS C:\Users\htb-student> Get-WmiObject -Class win32_useraccount | ? {$_ .Name -eq 'jim'}
AccountType : 512
Caption      : WS01\jim
Domain       : WS01
SID          : S-1-5-21-2614195641-1726409526-3792725429-1006
FullName     : Jimmy
Name         : jim

PS C:\Users\htb-student> Get-WmiObject -Class win32_Group | ? {$_ .Name -eq 'HR'}
Caption Domain Name SID
----- -----
WS01\HR WS01   HR   S-1-5-21-2614195641-1726409526-3792725429-1007

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

3. MODULE COMPLETION

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

A screenshot of the HTB Academy platform showing the completion of the Windows Fundamentals module. The main title 'Windows Fundamentals' is displayed prominently. A message says 'Great job c1ph3rbnuk!' and 'Completed / Congrats!'. Below this, it says 'Paths' and 'Show all paths'. On the left sidebar, there's a profile icon for 'c1ph3rbnuk' (Free, 63), and sections for 'LEARN' (Dashboard, Exams, Modules, Paths, Academy x HTB Labs) and 'MY ACHIEVEMENTS' (My Certificates, My Badges). In the center, there's a 'Conclusion' section with a summary of the module's content and a 'Module Key Takeaways' list: Windows structure, Using the command line, Navigating the Windows operating system. At the bottom, there are sharing options for LinkedIn, X, Facebook, and a 'Get a shareable link' button. To the right, there's a 'What's Next?' section with suggestions and a 'Suggested Modules' list.

<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.