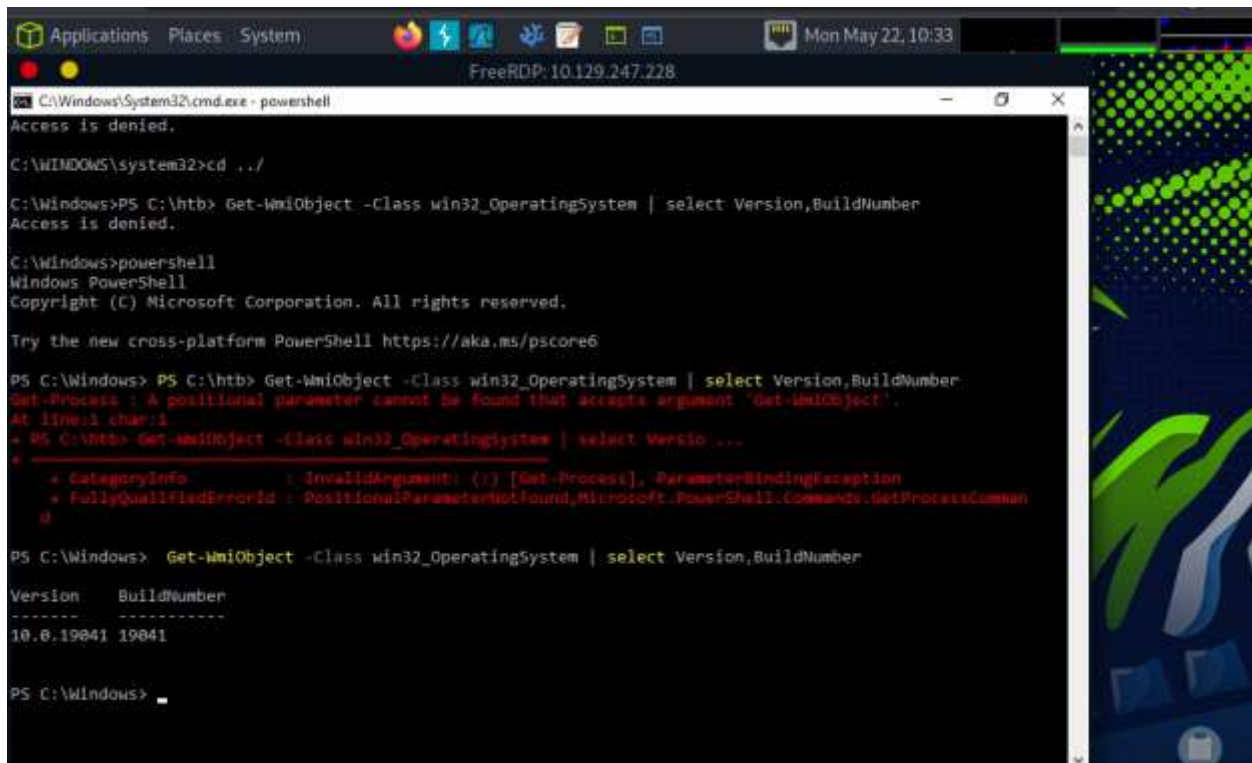


WINDOWS FUNDAMENTALS-HackTheBox

Introduction

This report provides an overview of key concepts in Windows Fundamentals, focusing on the assignment in the HackTheBox Academy. Windows Fundamentals encompasses essential aspects of Windows operating systems, including system architecture, user management, file systems, and security measures. Through hands-on challenges and practical scenarios, participants gain a comprehensive understanding of Windows operating systems and learn how to analyze and secure Windows-based systems effectively. This report will delve into these key concepts, with screenshots showing how to get answers to the provided tasks up to the completion level. The screenshots show commands used on PowerShell or cmd to get to the answers needed.

1.



```
C:\Windows\System32\cmd.exe - powershell
Access is denied.

C:\WINDOWS\system32>cd ../

C:\Windows>PS C:\htb> Get-WmiObject -Class win32_OperatingSystem | select Version,BuildNumber
Access is denied.

C:\Windows>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

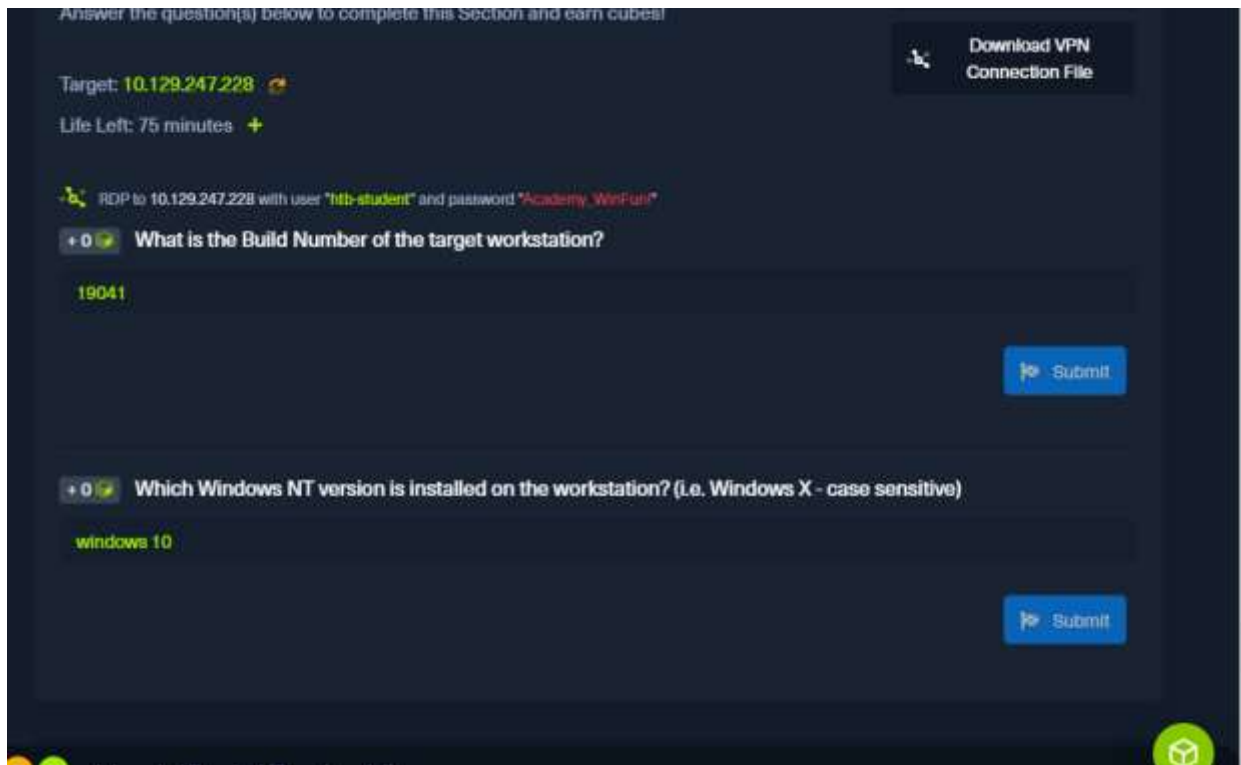
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows> PS C:\htb> Get-WmiObject -Class win32_OperatingSystem | select Version,BuildNumber
Get-Process : A positional parameter cannot be found that accepts argument 'Get-WmiObject'.
At line:1 char:1
+ PS C:\htb> Get-WmiObject -Class win32_OperatingSystem | select Versio ...
+ ~~~~~
+ CategoryInfo          : InvalidArgument: ([]) [Get-Process], ParameterBindingException
+ FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.GetProcessCommand

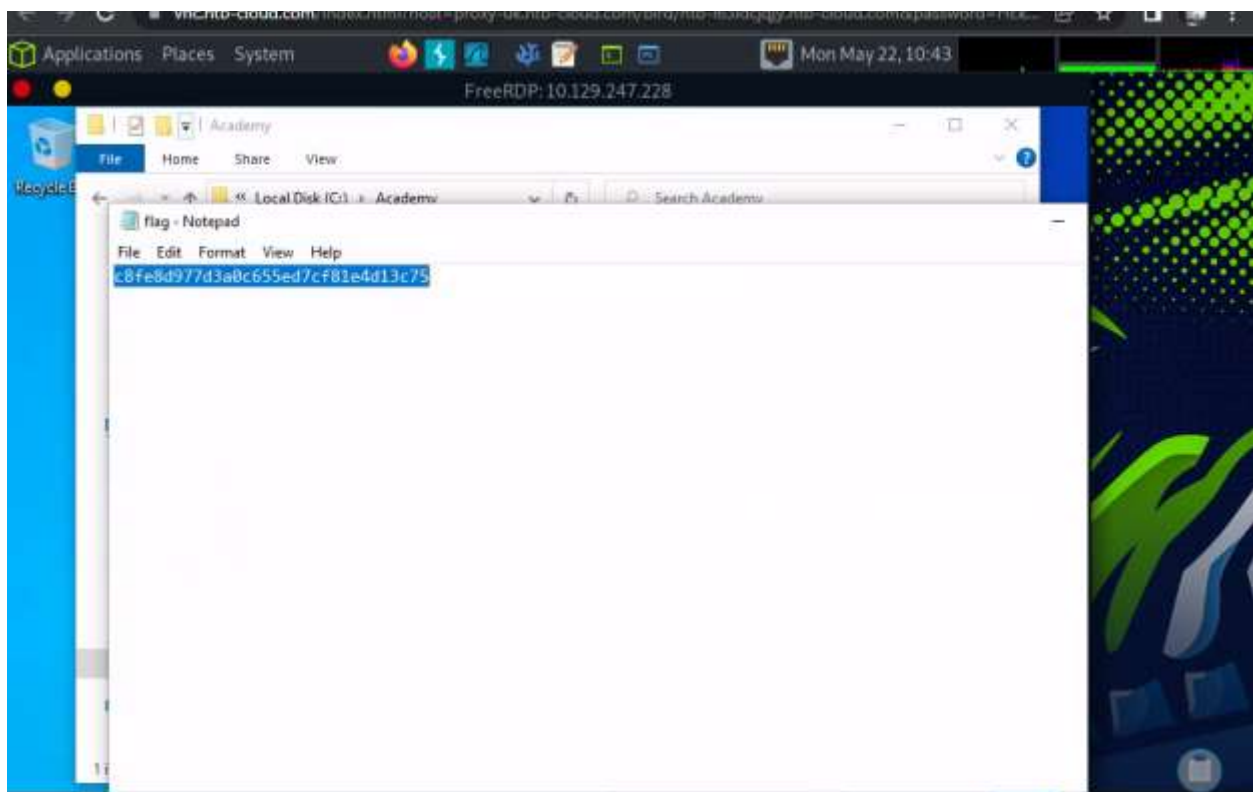
PS C:\Windows> Get-WmiObject -Class win32_OperatingSystem | select Version,BuildNumber

Version    BuildNumber
-----
10.0.19041 19041

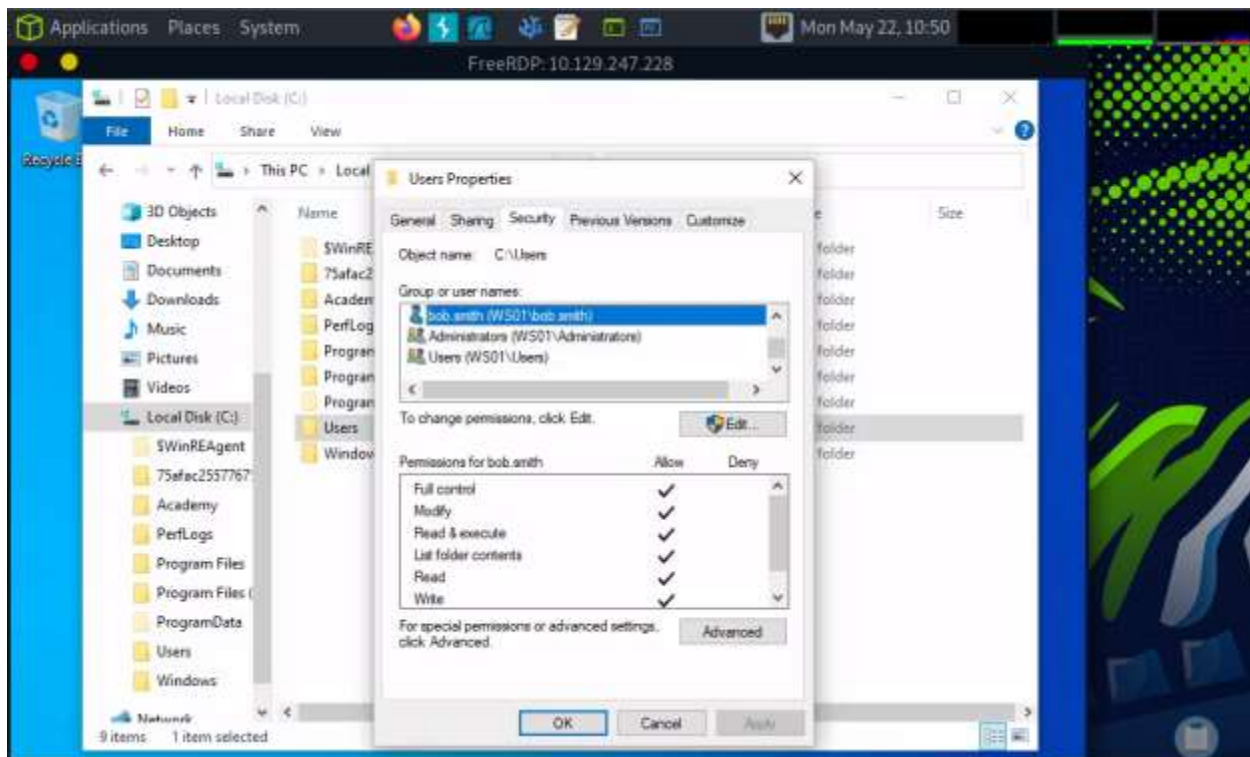
PS C:\Windows>
```



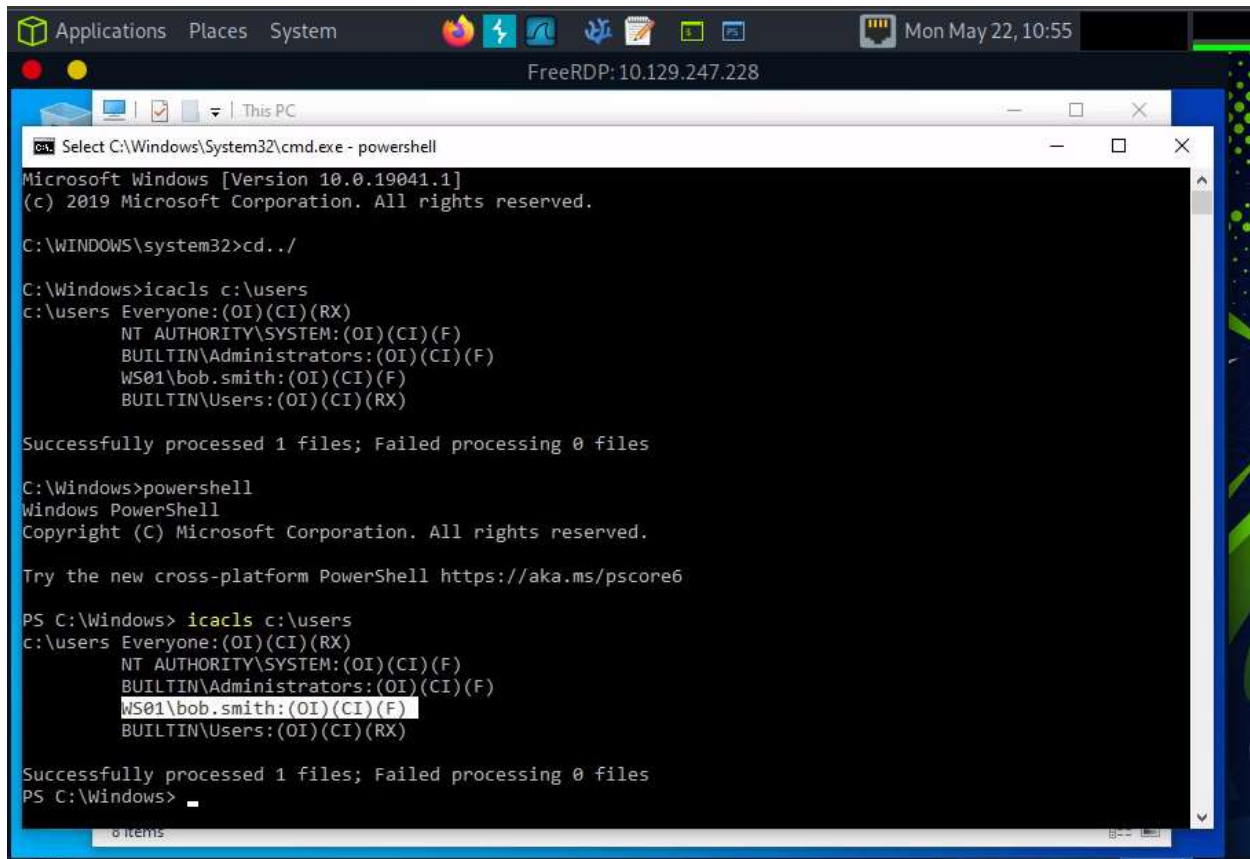
2.

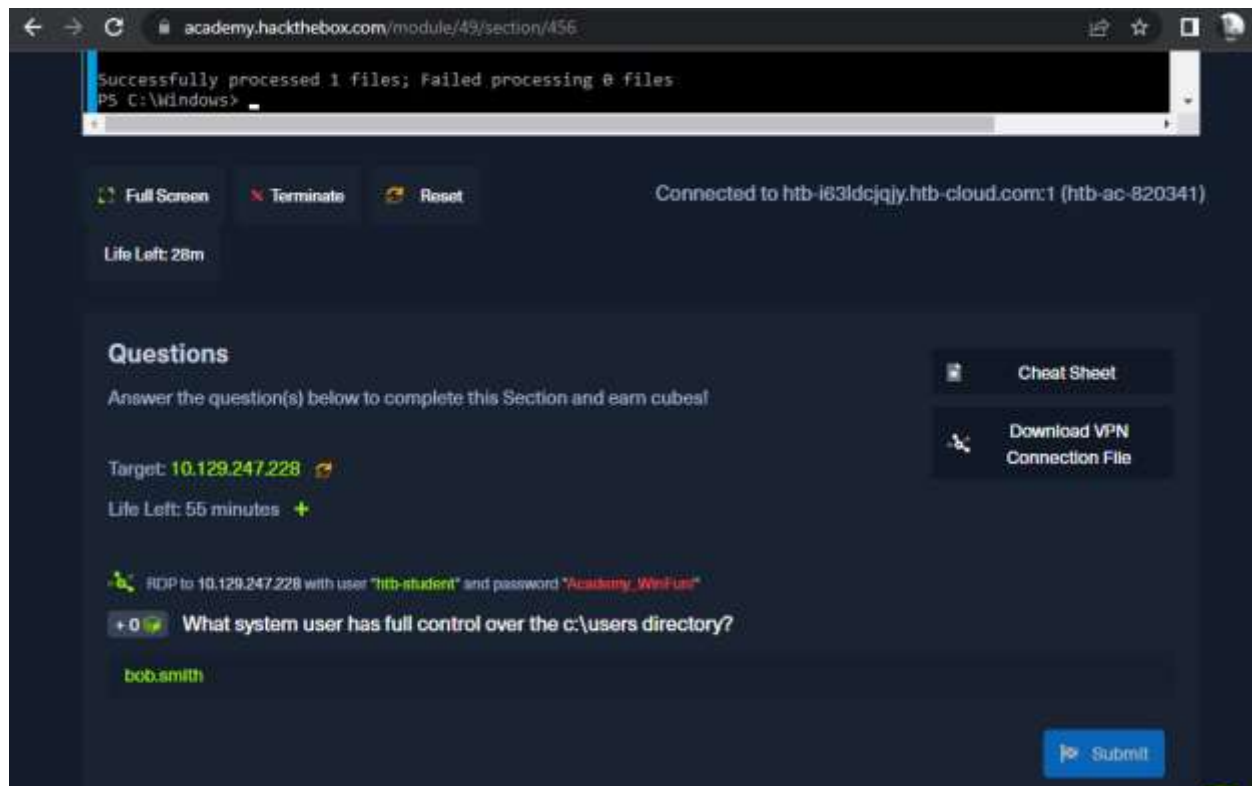


3.

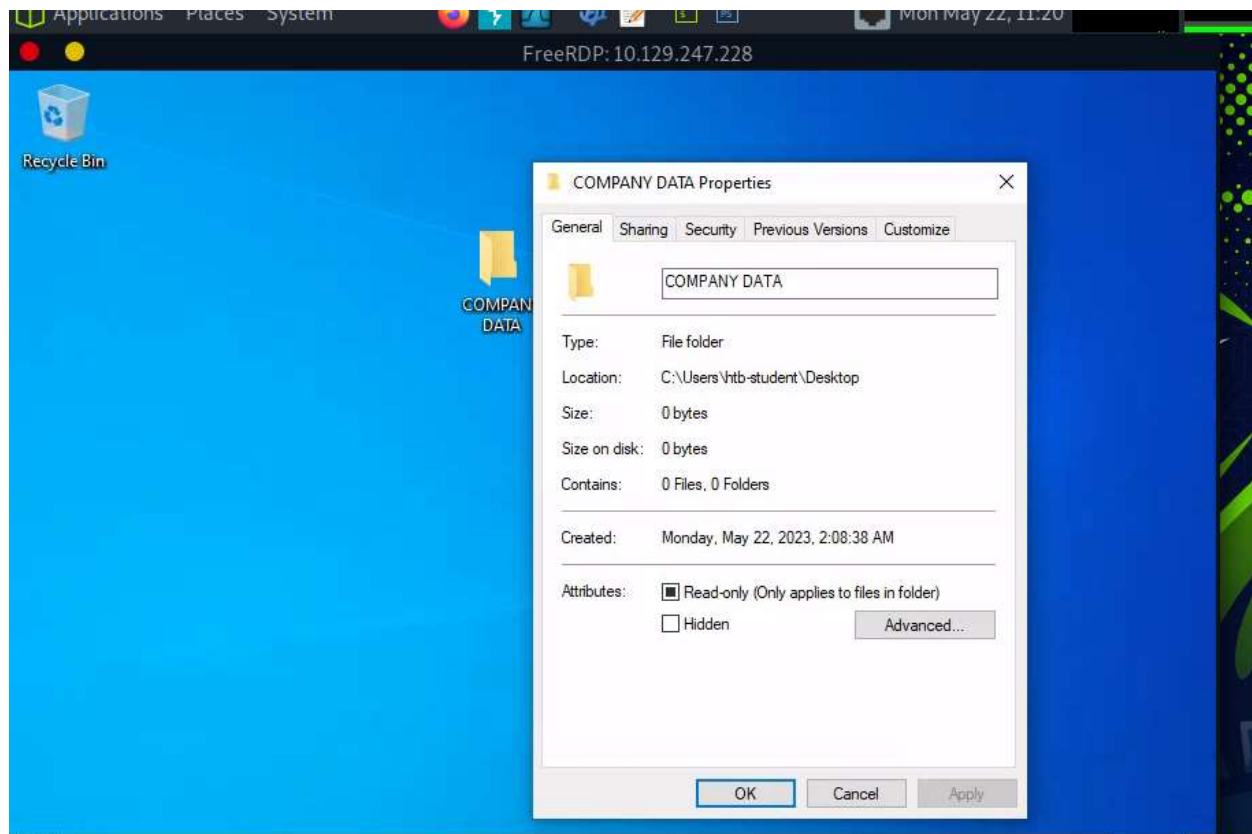


or





4.



RDP to 10.129.247.228 with user "htb-student" and password "Academy_WinFun!"

+1 What protocol discussed in this section is used to share resources on the network using Windows? (Format: case sensitive)

SMB

Submit Hint

+1 What is the name of the utility that can be used to view logs made by a Windows system? (Format: 2 words, 1 space, not case sensitive)

event viewer

Submit Hint

+1 What is the full directory path to the Company Data share we created?

C:\Users\htb-student\Desktop\COMPANY DATA

Submit Hint

Integrated Terminal (Experimental)

5.

Select Windows PowerShell				
svchost.exe	2124	Services	0	8,824 K
svchost.exe	2168	Services	0	8,088 K
svchost.exe	2176	Services	0	9,176 K
svchost.exe	2244	Services	0	8,136 K
svchost.exe	2252	Services	0	6,388 K
svchost.exe	2260	Services	0	9,432 K
svchost.exe	2372	Services	0	12,436 K
svchost.exe	2448	Services	0	9,292 K
svchost.exe	2520	Services	0	9,808 K
spoolsv.exe	2556	Services	0	15,204 K
svchost.exe	2604	Services	0	19,804 K
svchost.exe	2680	Services	0	7,256 K
svchost.exe	3028	Services	0	9,892 K
svchost.exe	3036	Services	0	29,404 K
svchost.exe	3048	Services	0	13,564 K
svchost.exe	3056	Services	0	18,532 K
FoxitReaderUpdateService.	1664	Services	0	7,140 K
svchost.exe	2844	Services	0	9,120 K
svchost.exe	3076	Services	0	5,608 K
VGAUTHService.exe	3084	Services	0	10,864 K
vm3dservice.exe	3096	Services	0	5,896 K
vmtoolsd.exe	3116	Services	0	20,832 K
MsMpEng.exe	3160	Services	0	211,428 K
svchost.exe	3196	Services	0	16,388 K
svchost.exe	3228	Services	0	10,536 K
svchost.exe	3320	Services	0	5,408 K
vm3dservice.exe	3340	RDP-Tcp#1	1	6,744 K
dllhost.exe	3880	Services	0	13,828 K
WmiPrvSE.exe	3172	Services	0	15,556 K

Questions

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

Target: 10.129.154.220

Life Left: 40 minutes

Cheat Sheet

Download VPN
Connection File

RDP to 10.129.154.220 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.

FoxitReaderUpdateService.exe

Submit

Hint

6.

```
Applications Places System Tue May 23, 07:53
FreeRDP: 10.129.186.143

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

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

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>
```

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

CommandType	Name	Version	Source
Alias	ifconfig -> ipconfig.exe		

Target: 10.129.154.220

Life Left: 51 minutes +

RDP to 10.129.154.220 with user "htb-student" and password "Academy_WinFun!"

+ 0 What is the alias set for the ipconfig.exe command?

ifconfig

Submit

+ 0 Find the Execution Policy set for the LocalMachine scope.

unrestricted

Submit

7.

Applications Places System Tue May 23, 07:58 FreeRDP: 10.129.186.143

```
Windows PowerShell
PS C:\Users\htb-student> Get-WmiObject -Class Win32_OperatingSystem | select SystemDirectory, BuildNumber, SerialNumber, Version | ft
SystemDirectory      BuildNumber  SerialNumber      Version
-----
C:\WINDOWS\system32  19041       00329-10280-00000-AA938  10.0.19041

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

Menu [VNC config] Parrot Terminal FreeRDP: 10.129.186.1... Disconnected

Full Screen Terminate Reset

Life Left: 95m

Questions

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

Target: 10.129.186.143

Life Left: 94 minutes

RDP to 10.129.186.143 with user "htb-student" and password "Academy_WinFun!"

+0 Use WMI to find the serial number of the system.

00329-10280-00000-AA938

Cheat Sheet

Download VPN Connection File

8.

```
vnc.htb-cloud.com/index.html?host=proxy-uk.htb-cloud.com/bird/htb-ogwhawbiku.htb-cloud.com&pa
```

Applications Places System Tue May 23, 08:14

FreeRDP: 10.129.186.143

Select Windows PowerShell

```
PS C:\Users\htb-student> Get-WmiObject -Class Win32_OperatingSystem | select SystemDirectory, BuildNumber, SerialNumber, Version | ft
```

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

```
PS C:\Users\htb-student> whoami /user
```

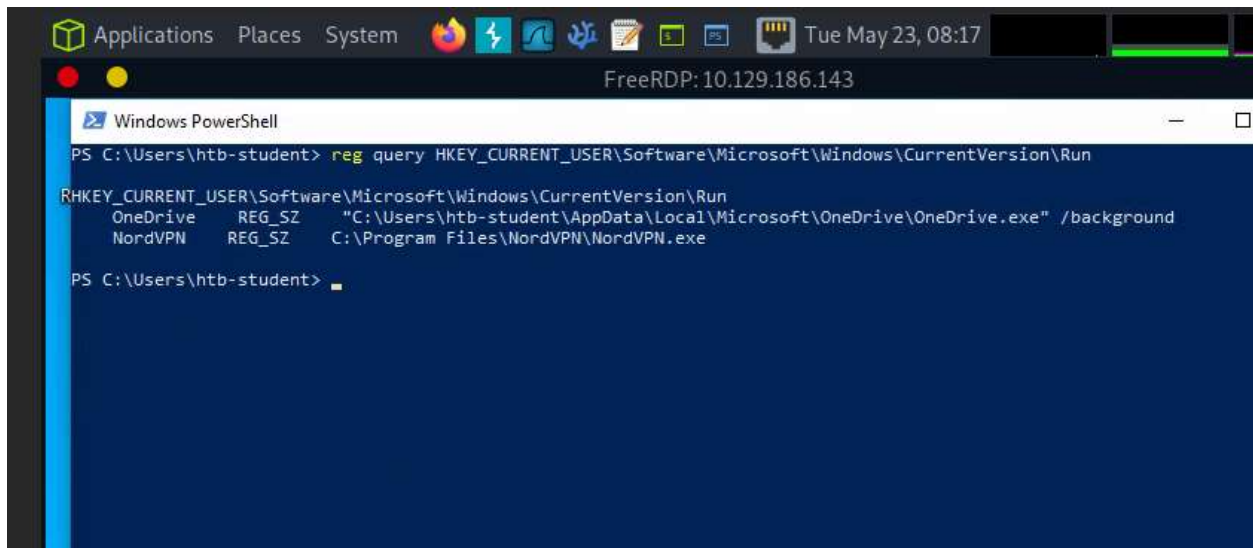
USER INFORMATION

User Name	SID
ws01\htb-student	S-1-5-21-2614195641-1726409526-3792725429-1002

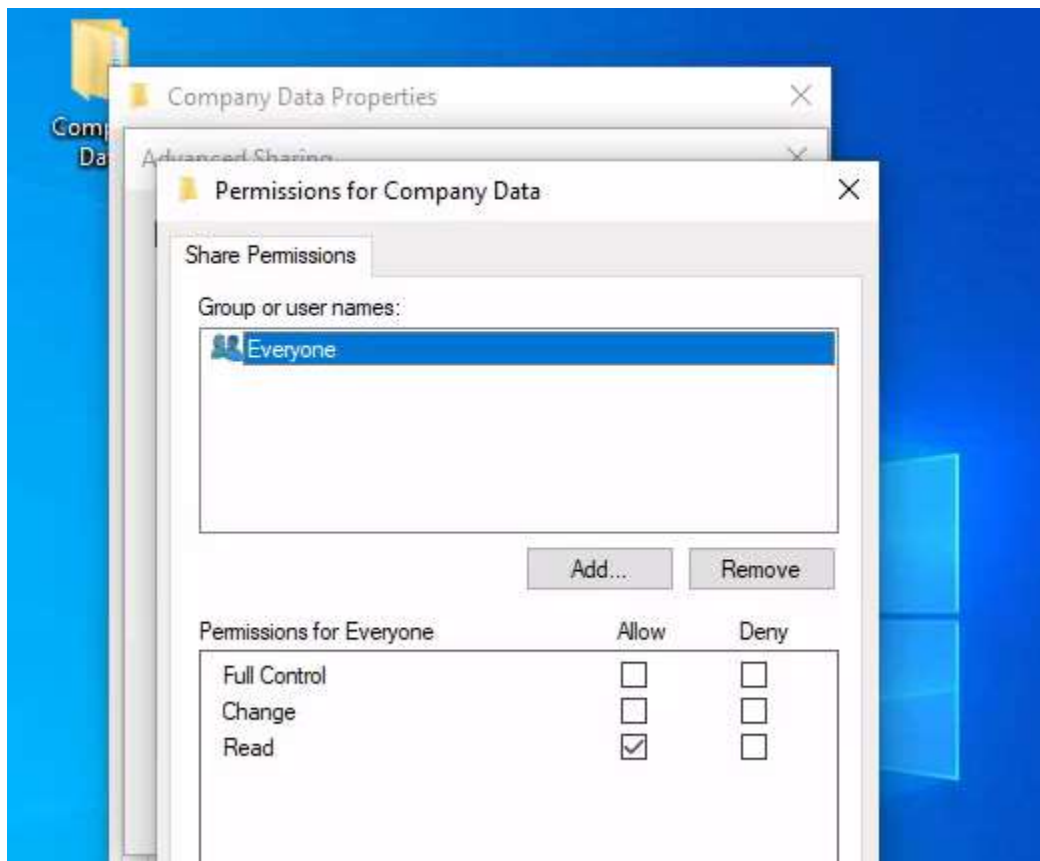
```
PS C:\Users\htb-student> Get-WmiObject -Class Win32_useraccount -Filter "name = 'bob.smith'"
```

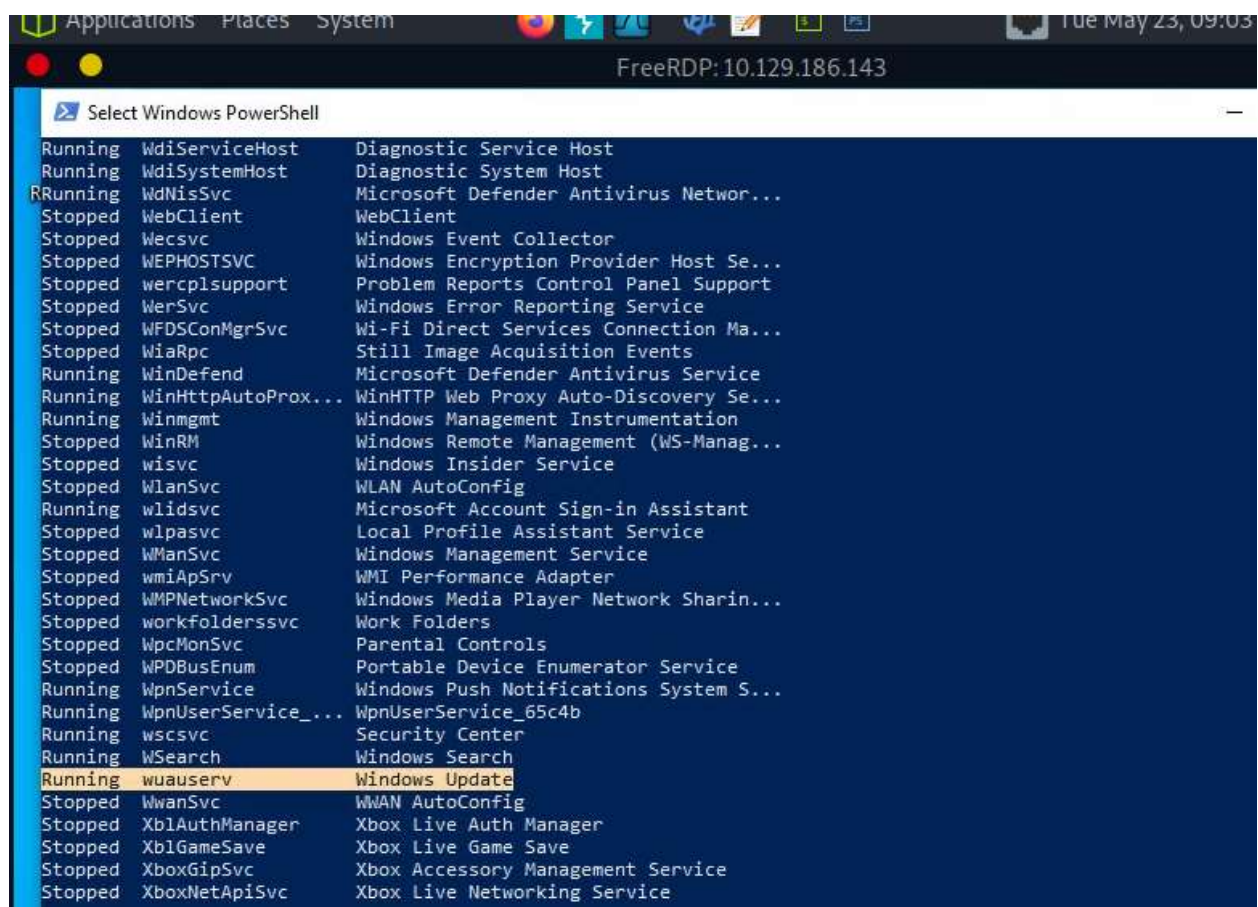
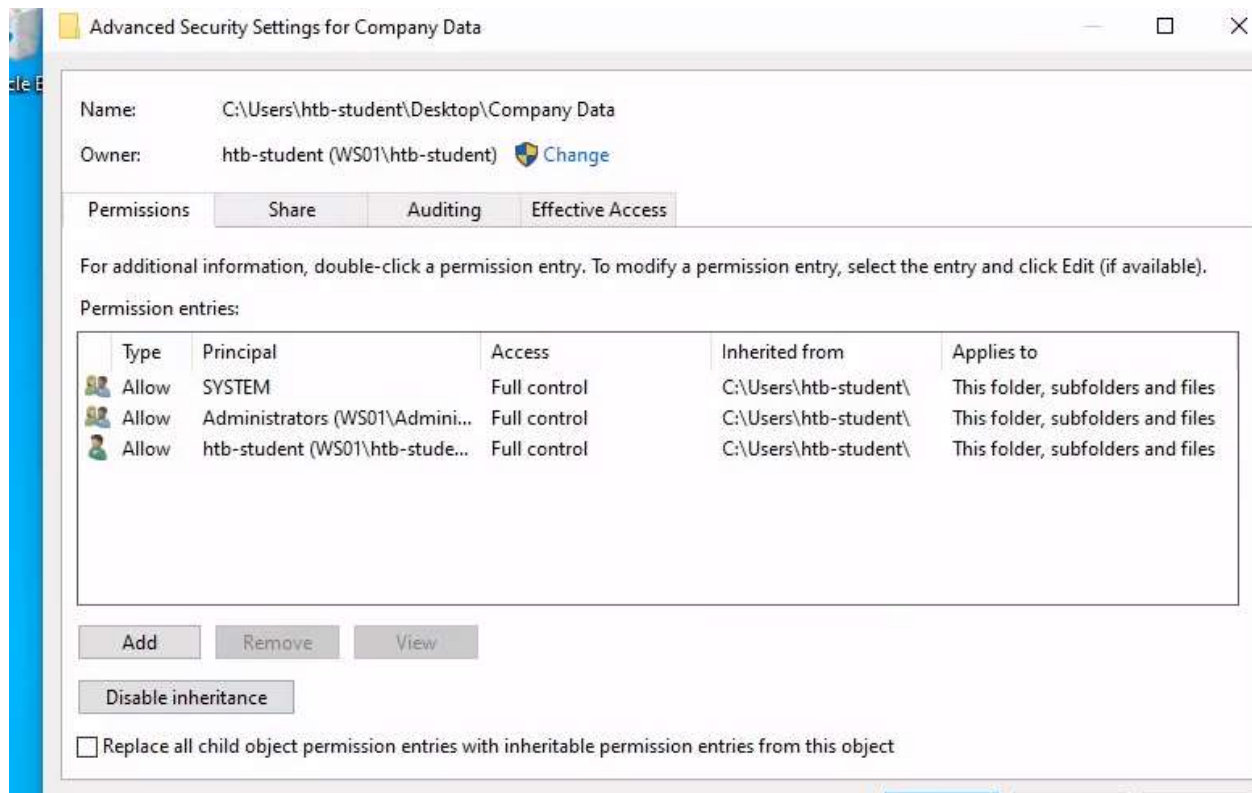
```
AccountType : 512
Caption      : WS01\bob.smith
Domain       : WS01
SID          : S-1-5-21-2614195641-1726409526-3792725429-1003
FullName     :
Name         : bob.smith
```

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

9. FINAL TEST





```
Select Windows PowerShell

PS 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
Jim S-1-5-21-2614195641-1726409526-3792725429-1006
mrb3n S-1-5-21-2614195641-1726409526-3792725429-1001
WDAGUtilityAccount S-1-5-21-2614195641-1726409526-3792725429-504

PS C:\Users\htb-student> wmic group get name,sid
Name SID
-----
Access Control Assistance Operators S-1-5-32-579
Administrators S-1-5-32-544
Backup Operators S-1-5-32-551
Cryptographic Operators S-1-5-32-569
Distributed COM Users S-1-5-32-562
Event Log Readers S-1-5-32-573
Guests S-1-5-32-546
Hyper-V Administrators S-1-5-32-578
IIS_IUSRS S-1-5-32-568
Network Configuration Operators S-1-5-32-556
Performance Log Users S-1-5-32-559
Performance Monitor Users S-1-5-32-558
Power Users S-1-5-32-547
Remote Desktop Users S-1-5-32-555
Remote Management Users S-1-5-32-580
Replicator S-1-5-32-552
System Managed Accounts Group S-1-5-32-581
Users S-1-5-32-545
HR S-1-5-21-2614195641-1726409526-3792725429-1007

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

+ 1

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

security

Hint

+ 1

What is the name of the service associated with Windows Update?

wuauclt

+ 1

List the SID associated with the user account Jim you created.

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

Hint

+ 1

List the SID associated with the HR security group you created.

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

Completed



Sharable link

<https://academy.hackthebox.com/achievement/820341/49>

Conclusion:

In conclusion, the assignment on Windows Fundamentals in the HackTheBox Academy has provided a valuable learning experience and enhanced my understanding of essential concepts in Windows operating systems. Through the hands-on challenges and practical scenarios, I have gained a deeper knowledge of system architecture, user management, file systems, and security measures within Windows environments.

One of the key takeaways from this assignment is the importance of a solid foundation in Windows Fundamentals for effective cybersecurity practices right from accessing Hackthebox machine to working with it to solve a range of simple to complex tasks. Understanding the inner workings of Windows operating systems allows for better analysis and identification of vulnerabilities, as well as the implementation of appropriate security measures to protect against potential threats.

Overall, the Windows Fundamentals assignment has not only deepened my understanding of Windows operating systems but also equipped me with practical skills and knowledge to analyze and secure Windows-based systems effectively ranging from creating users and setting permission to using the command prompt and PowerShell tools effectively. This experience has been invaluable in strengthening my cybersecurity expertise and preparedness for real-world scenarios. I look forward to applying the knowledge and skills gained from this assignment in future endeavors within the cybersecurity field.