WINDOWS FUNDAMENTALS REPORT

Introduction

This report offers an in-depth exploration of the core principles underpinning Windows operating systems, essential for any cybersecurity professional. It underscores the significance of comprehending Windows alongside Linux, given their pervasive presence across diverse IT landscapes, spanning on-premise setups to cloud environments.

Key Concepts Explored

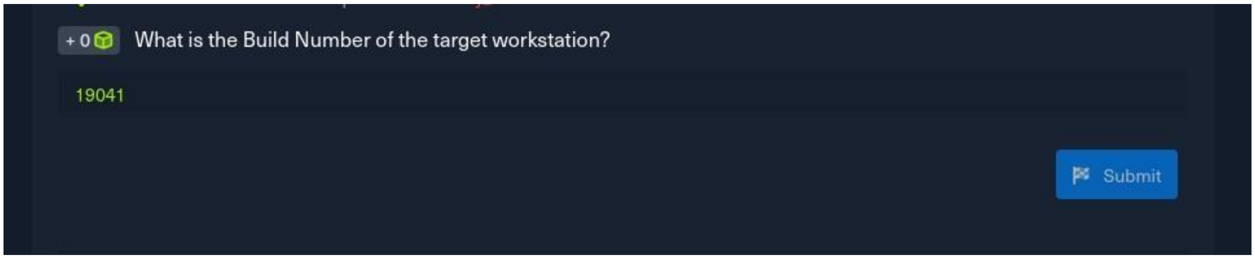
By tracing Windows' evolution from its inception in 1985 to its current iteration, Windows 10, this report highlights pivotal milestones such as the integration of Active Directory within Windows Server. Emphasis is placed on understanding version discrepancies and inherent vulnerabilities across different Windows releases.

Practical Application

Practical tasks featured in this report involve the hands-on utilization of tools like the GetWmiObject cmdlet. Through these exercises, users gain tangible insights into Windows operations and learn to address security concerns effectively.

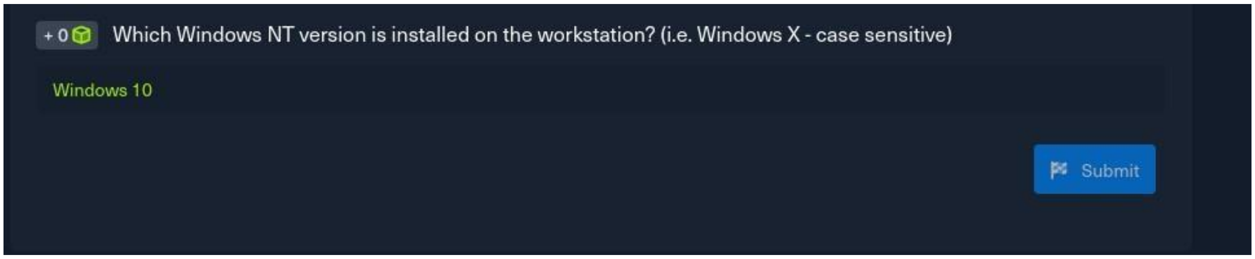
Reflections

Completing this module has not only deepened my comprehension of Windows operating systems but has also enhanced my practical skill set as a security analyst. From exploring Windows' historical trajectory to mastering tools like Active Directory, this journey equips me to navigate Windows environments proficiently.



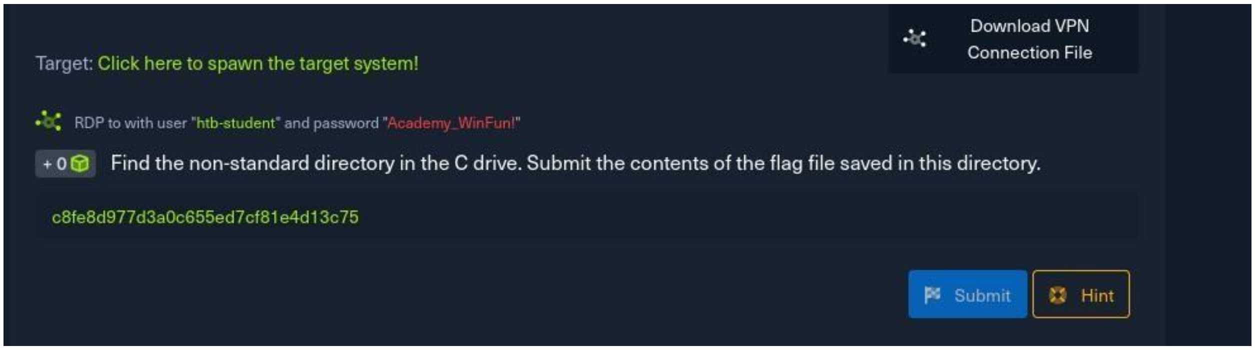
What is the Build Number of the target workstation?

19041



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

Windows 10

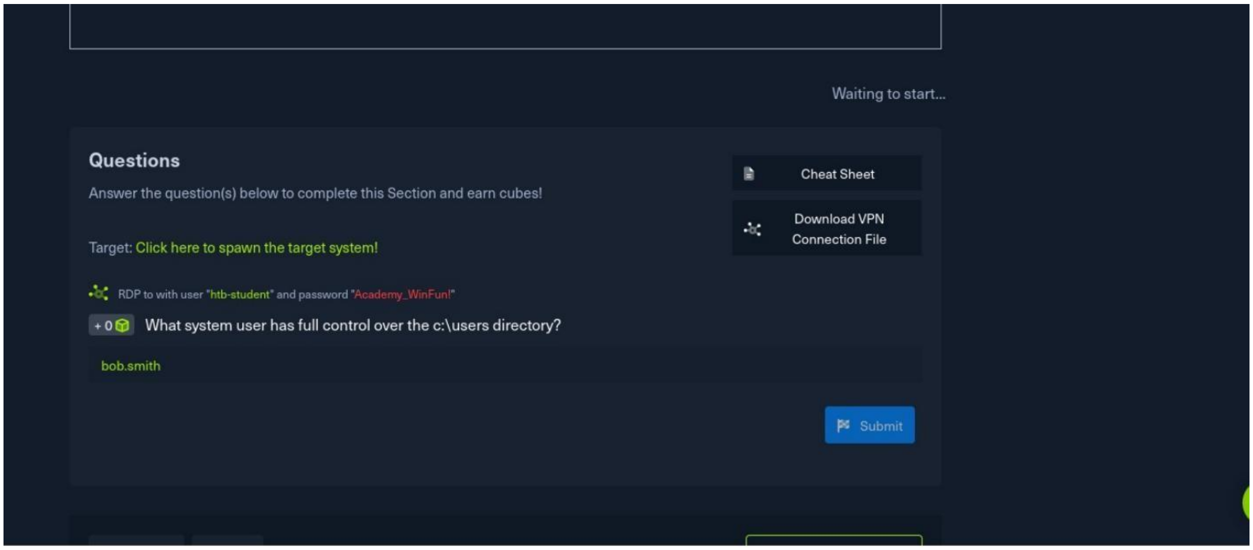


Target: Click here to spawn the target system!

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

+ 0 Find the non-standard directory in the C drive. Submit the contents of the flag file saved in this directory.

c8fe8d977d3a0c655ed7cf81e4d13c75



Waiting to start...

Questions

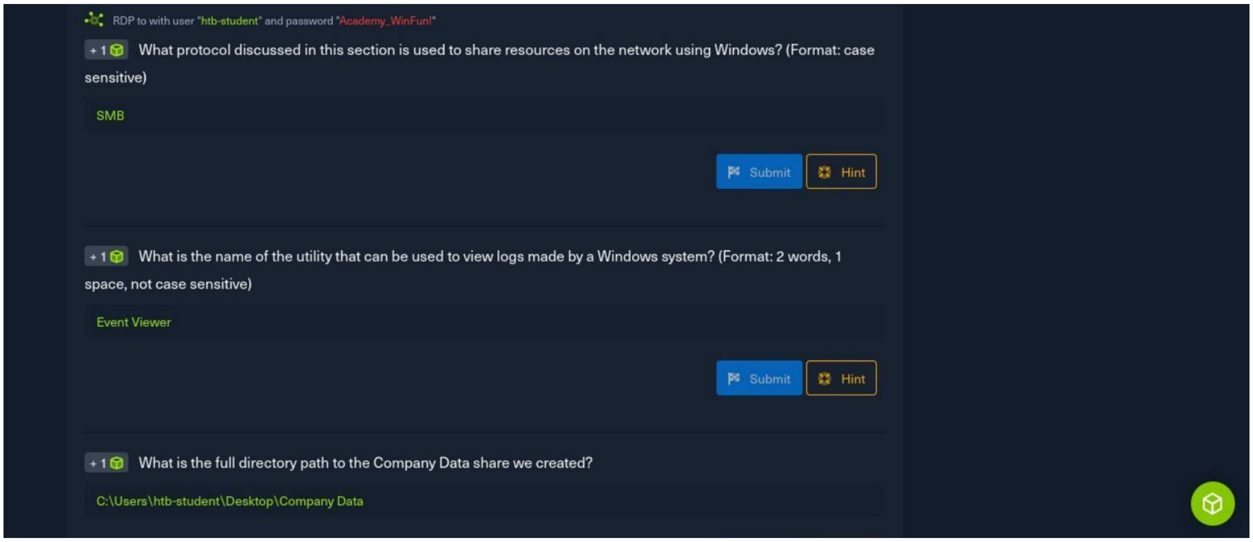
Answer the question(s) below to complete this Section and earn cubes!

Target: Click here to spawn the target system!

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

+ 0 What system user has full control over the c:\users directory?

bob.smith



RDP to 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)

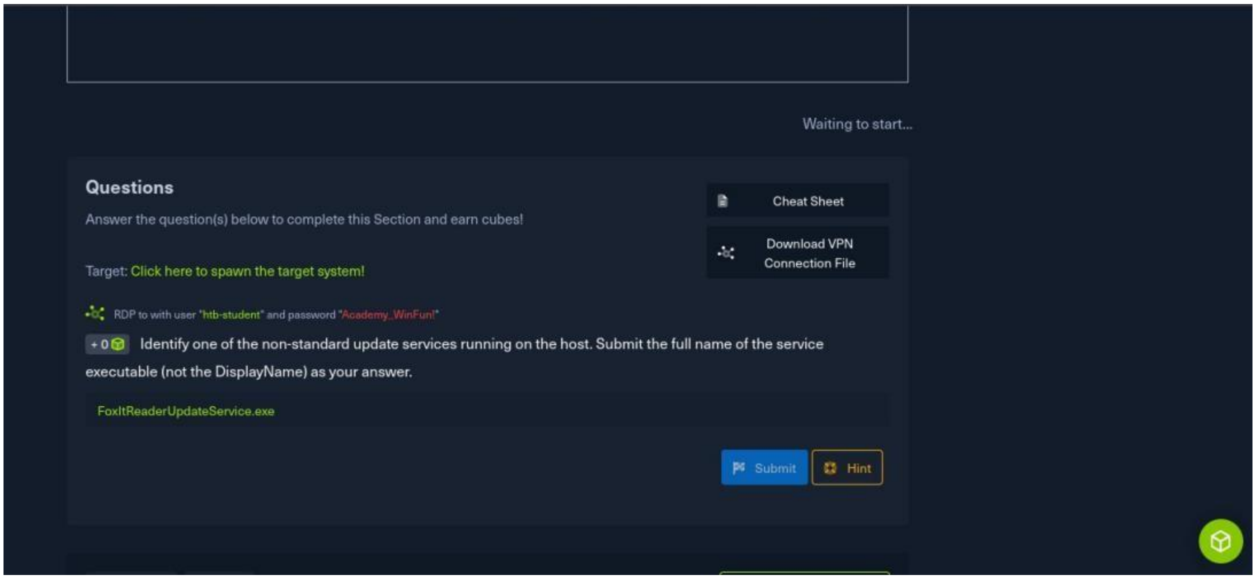
SMB

+ 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

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

C:\Users\htb-student\Desktop\Company Data



Questions

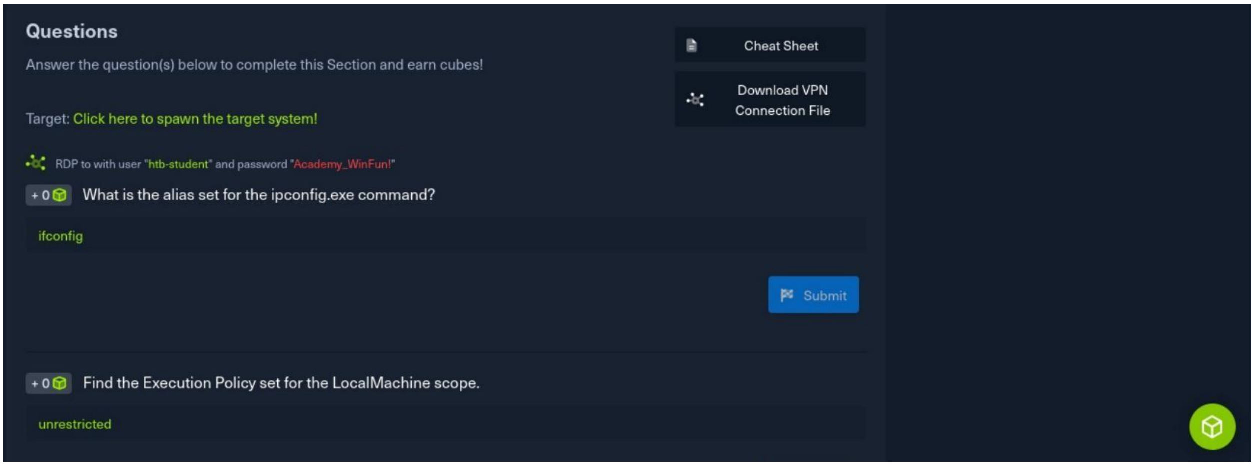
Answer the question(s) below to complete this Section and earn cubes!

Target: 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.

FoxitReaderUpdateService.exe



Questions

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

Target: Click here to spawn the target system!

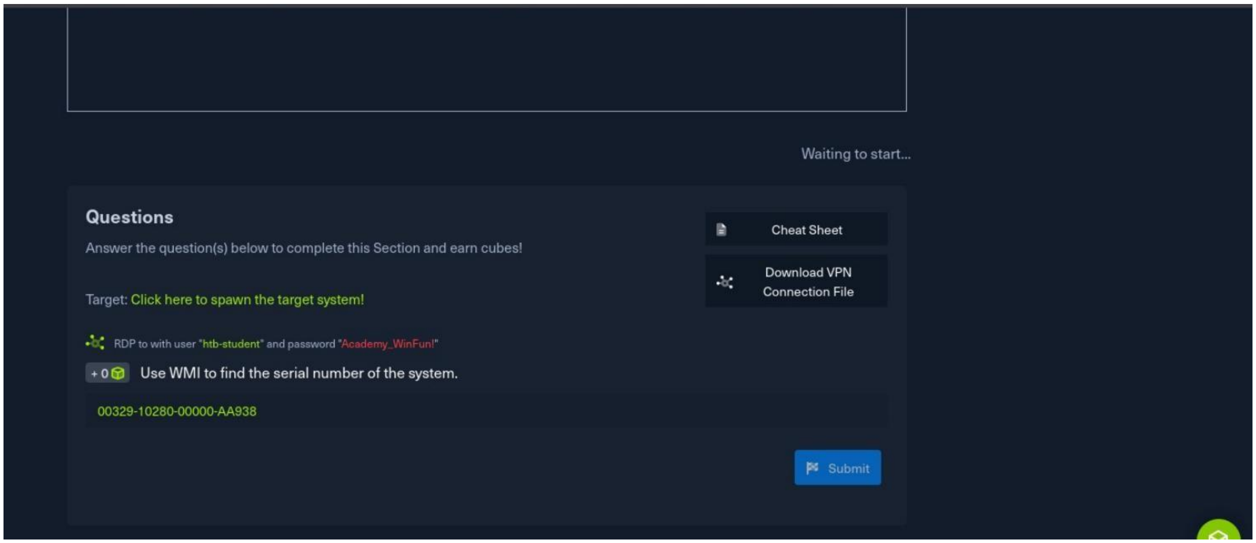
RDP to with user "htb-student" and password "Academy_WinFun!"

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

ifconfig

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

unrestricted



Questions

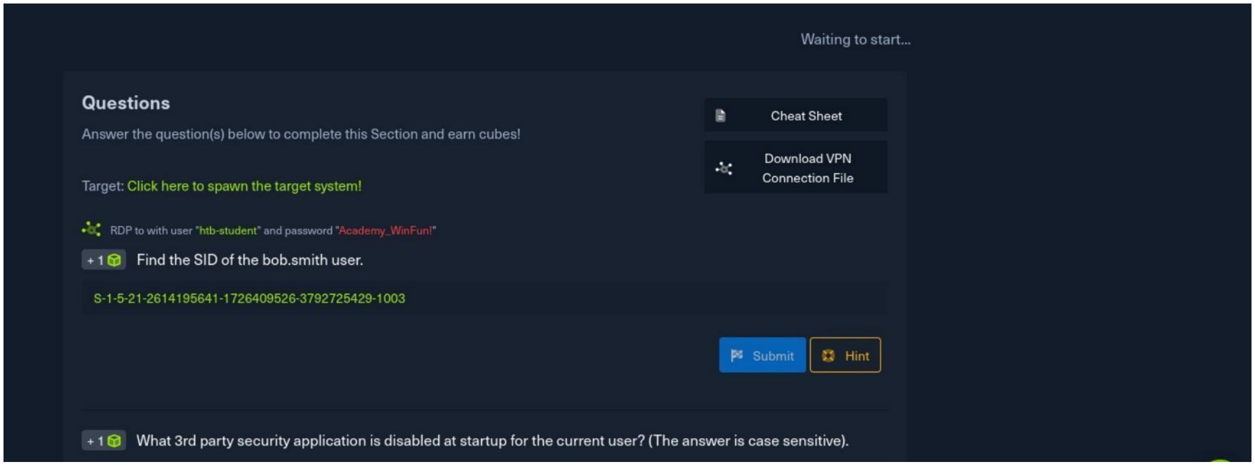
Answer the question(s) below to complete this Section and earn cubes!

Target: Click here to spawn the target system!

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

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

00329-10280-00000-AA938



Questions

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

Target: Click here to spawn the target system!

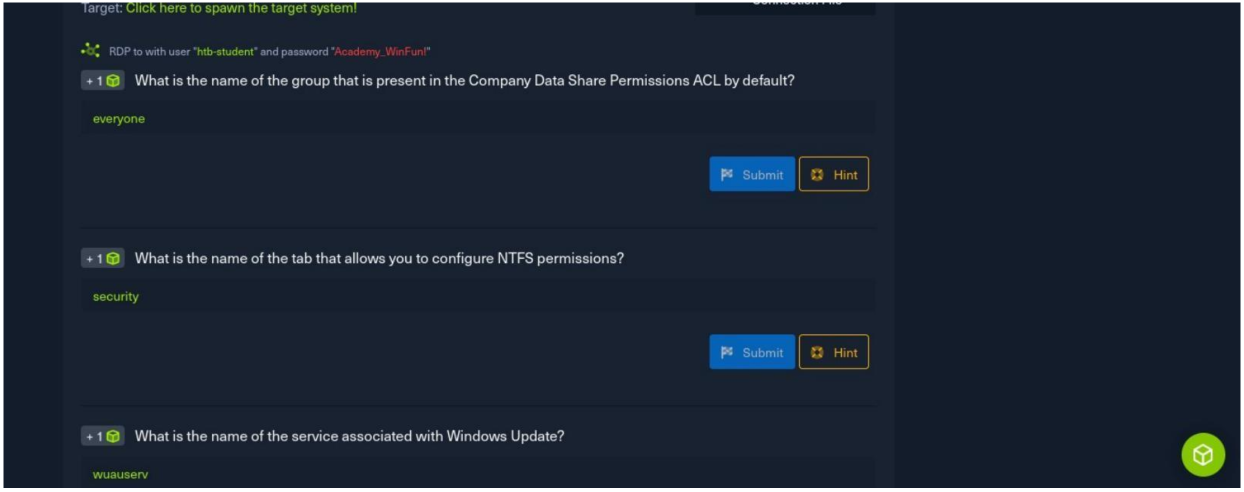
RDP to with user "htb-student" and password "Academy_WinFun!"

+1 Find the SID of the bob.smith user.

S-1-5-21-2614195641-1726409526-3792725429-1003

+1 What 3rd party security application is disabled at startup for the current user? (The answer is case sensitive).

Shareable link: https://academy.hackthebox.com/achievement/1294688/49



Target: Click here to spawn the target system!

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

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

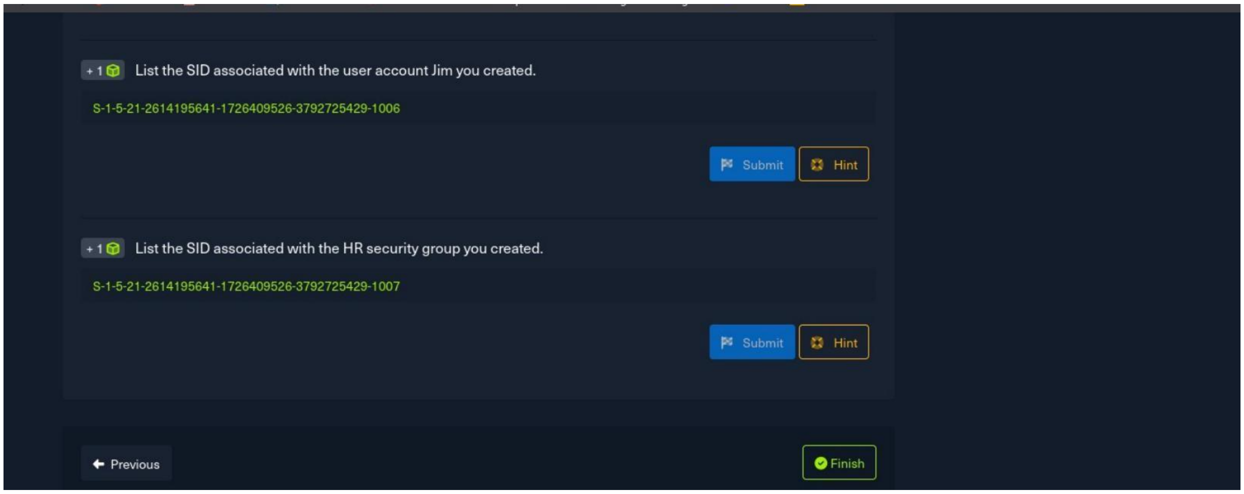
everyone

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

security

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

wuauserv



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

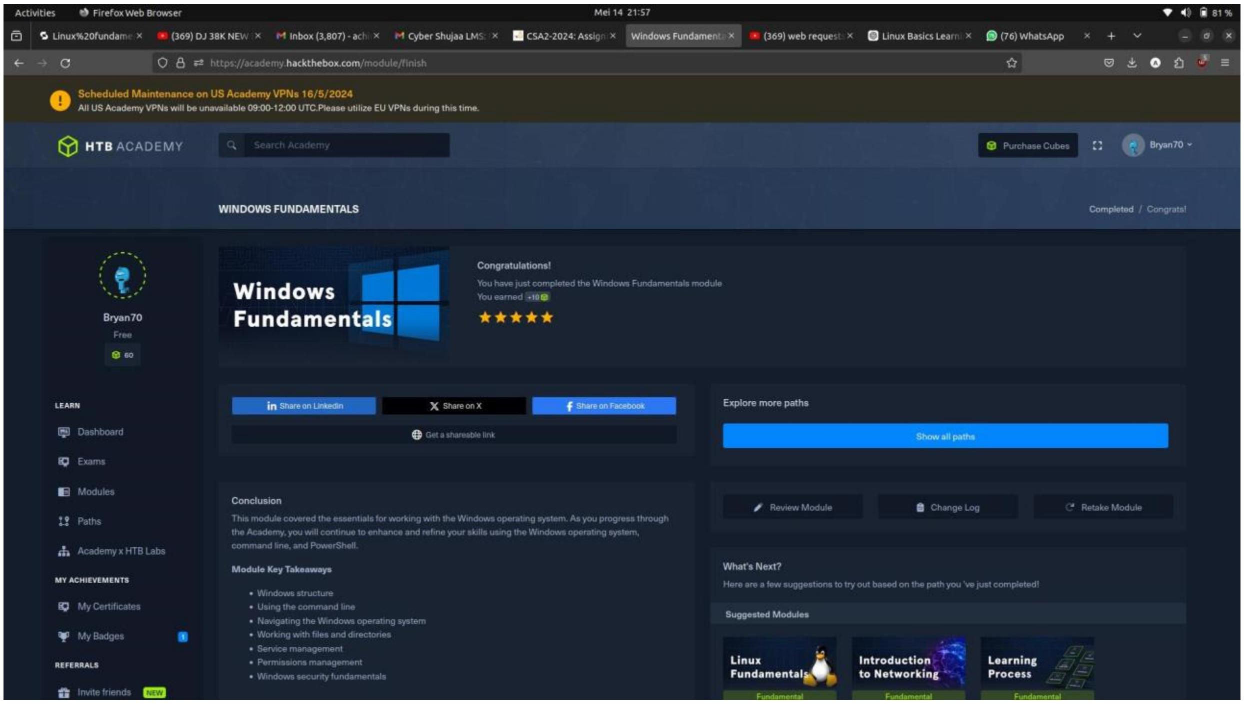
S-1-5-21-2614195641-1726409526-3792725429-1006

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

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

2. Provide a shareable link and final screenshot showing module completion. Post your module completion on social media to build your brand.

Shareable link : https://academy.hackthebox.com/achievement/1296187/49



Scheduled Maintenance on US Academy VPNs 16/5/2024

All US Academy VPNs will be unavailable 09:00-12:00 UTC.Please utilize EU VPNs during this time.

WINDOWS FUNDAMENTALS

Congratulations!

You have just completed the Windows Fundamentals module

You earned +10

Explore more paths

Conclusion

This module covered the essentials for working with the Windows operating system. As you progress through the Academy, you will continue to enhance and refine your skills using the Windows operating system, command line, and PowerShell.

Module Key Takeaways

- Windows structure
- Using the command line
- Navigating the Windows operating system
- Working with files and directories
- Service management
- Permissions management
- Windows security fundamentals

What's Next?

Here are a few suggestions to try out based on the path you 've just completed!

Suggested Modules