Getting Started Module

Mastering tools like SSH, Netcat, Tmux, and Vim is essential for any information security professional. These tools, while not specific to penetration testing, play critical roles in the process. Here's a brief overview of each tool and its use in penetration testing.

Using SSH

Secure Shell (SSH) is a network protocol providing secure remote access to systems. Running on port 22 by default, SSH can be configured with password authentication or more securely with public-key authentication using an SSH key pair. It's useful for:

Remote Access: Connect to systems within the same network or over the internet.

Port Forwarding/Proxying: Facilitate connections to resources in other networks.

File Transfers: Upload and download files between local and remote systems.

SSH is typically more stable than reverse shell connections and can be used as a jump host to access and attack other network hosts. To connect via SSH, use the command:

Using Netcat

Netcat (nc) is a versatile network utility for interacting with TCP/UDP ports. Key uses in penetration testing include:

Connecting to Shells: Establish connections to remote shells.

Banner Grabbing: Identify services running on specific ports by connecting and reading their banners. For example:

File Transfers: Transfer files between machines.

Netcat comes pre-installed on most Linux distributions, with Windows versions also available. Socat, a similar utility, extends Netcat's functionality with features like port forwarding and connecting to serial devices.

Using Tmux

Tmux is a terminal multiplexer that enhances the capabilities of a standard terminal by allowing multiple windows and panes within a single terminal session. Key features include:

cs-sa07-24019
John Mutave

Multiple Windows: Open multiple terminal windows within one session.

Panes: Split windows into multiple panes for side-by-side task management.

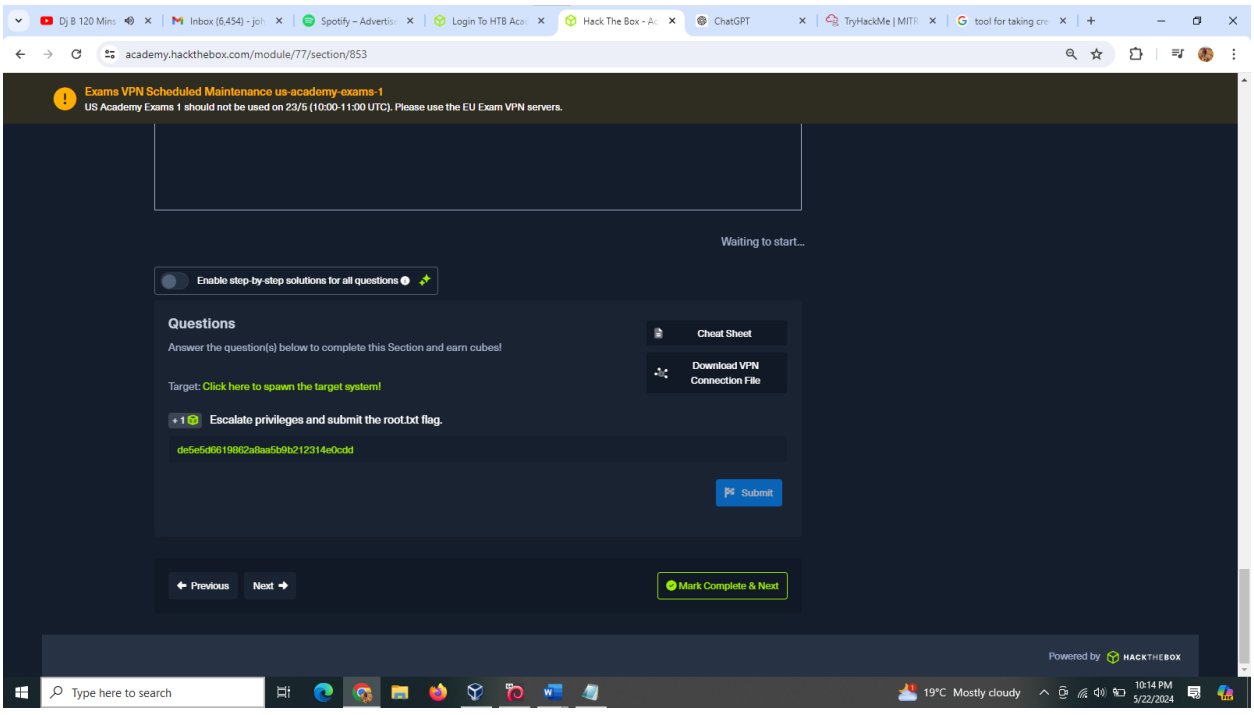
Navigation: Easily switch between windows and panes.

To install and start using Tmux:

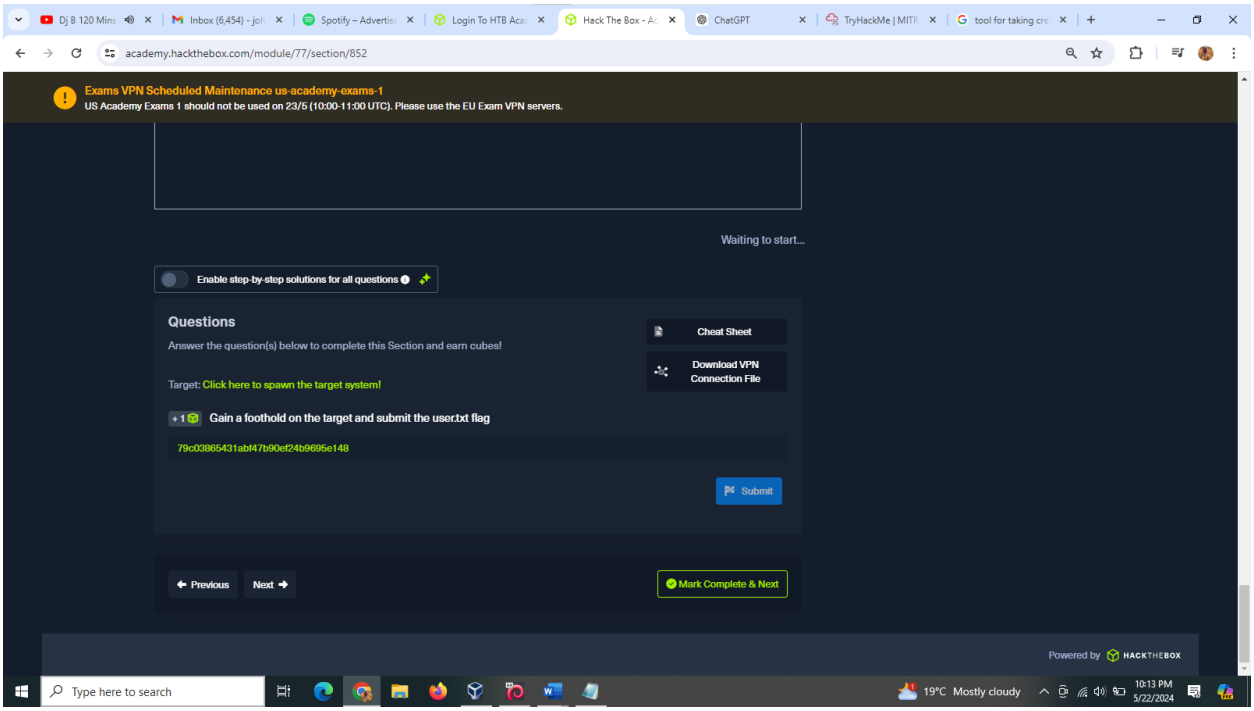
Using Vim

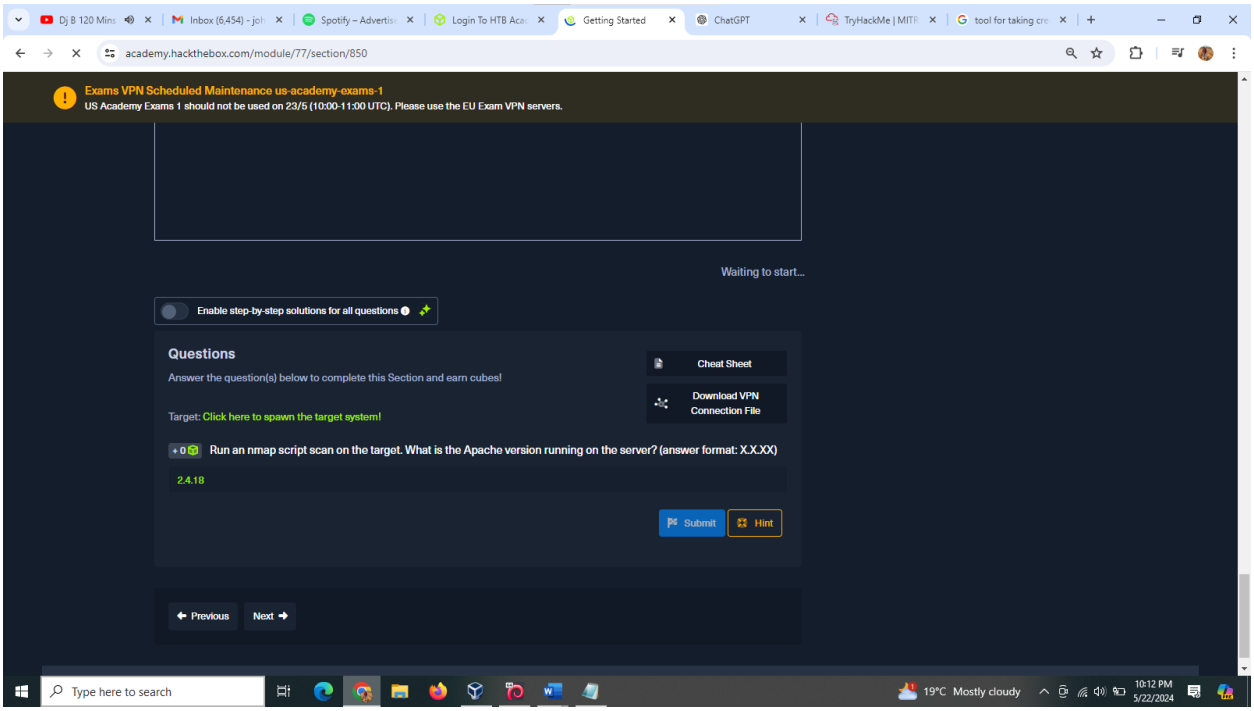
Vim is a powerful text editor that enhances productivity through keyboard-only navigation. Commonly found on Linux systems, Vim is crucial for editing files during penetration tests. Basic Vim commands include:

- Understanding and mastering these tools is crucial for effective penetration testing. SSH allows secure remote access and file transfers, Netcat provides versatile network interaction capabilities, Tmux enhances terminal management, and Vim offers powerful text editing features. These tools form the backbone of daily operations for penetration testers and system administrators alike.

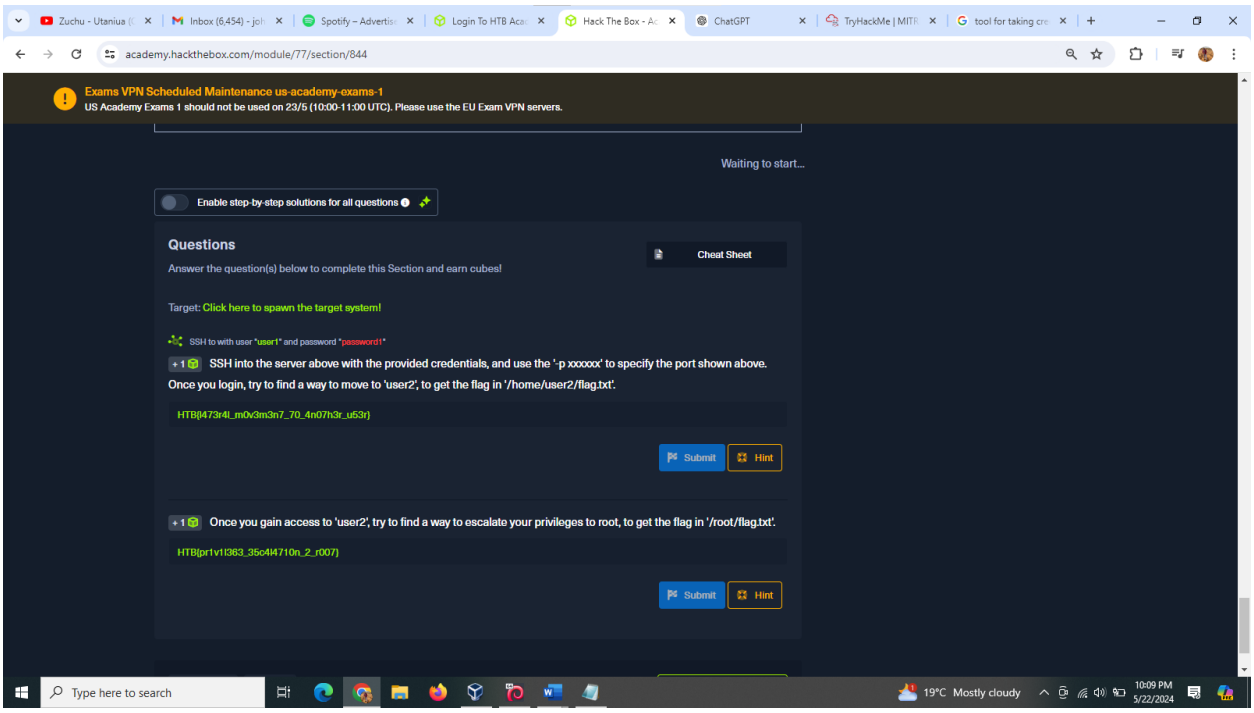


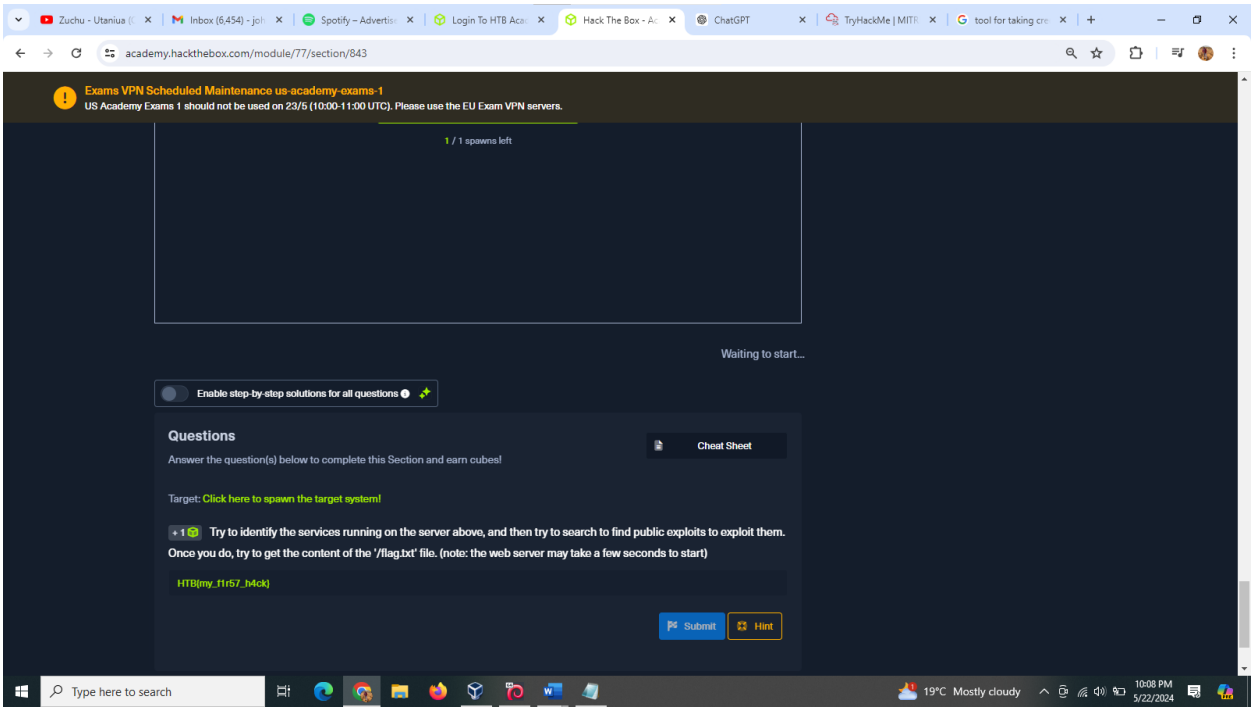
cs-sa07-24019
John Mutave



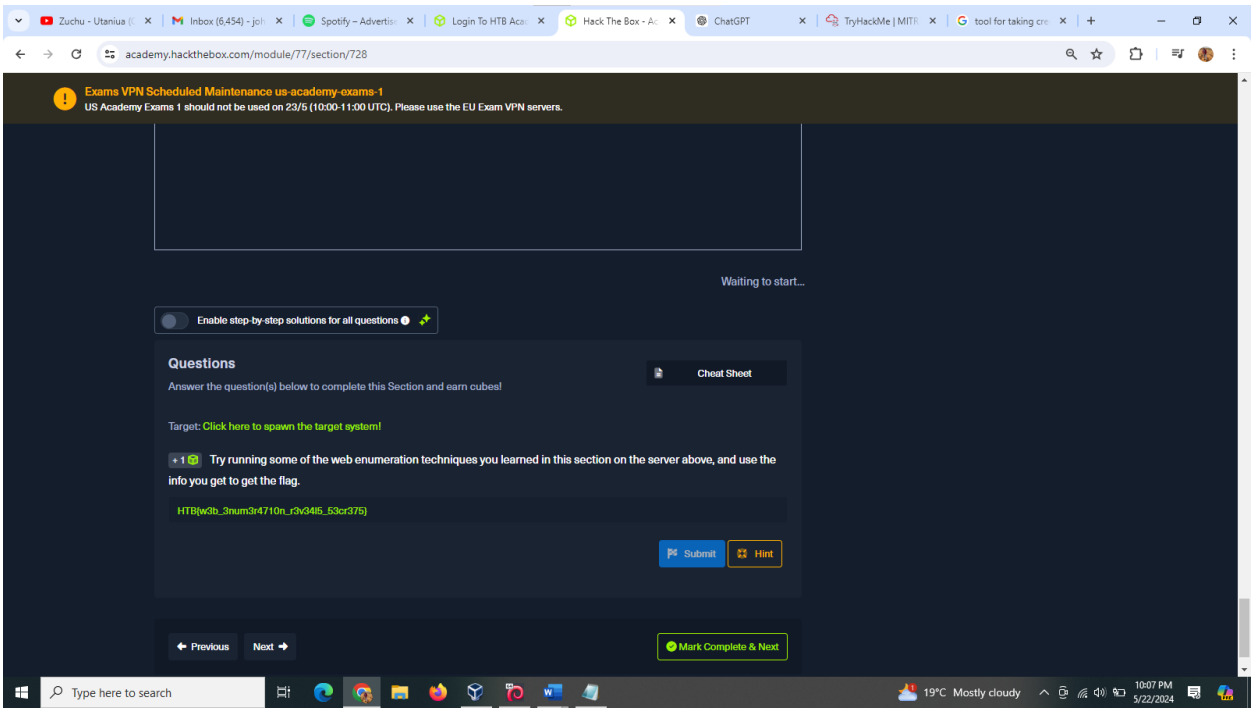


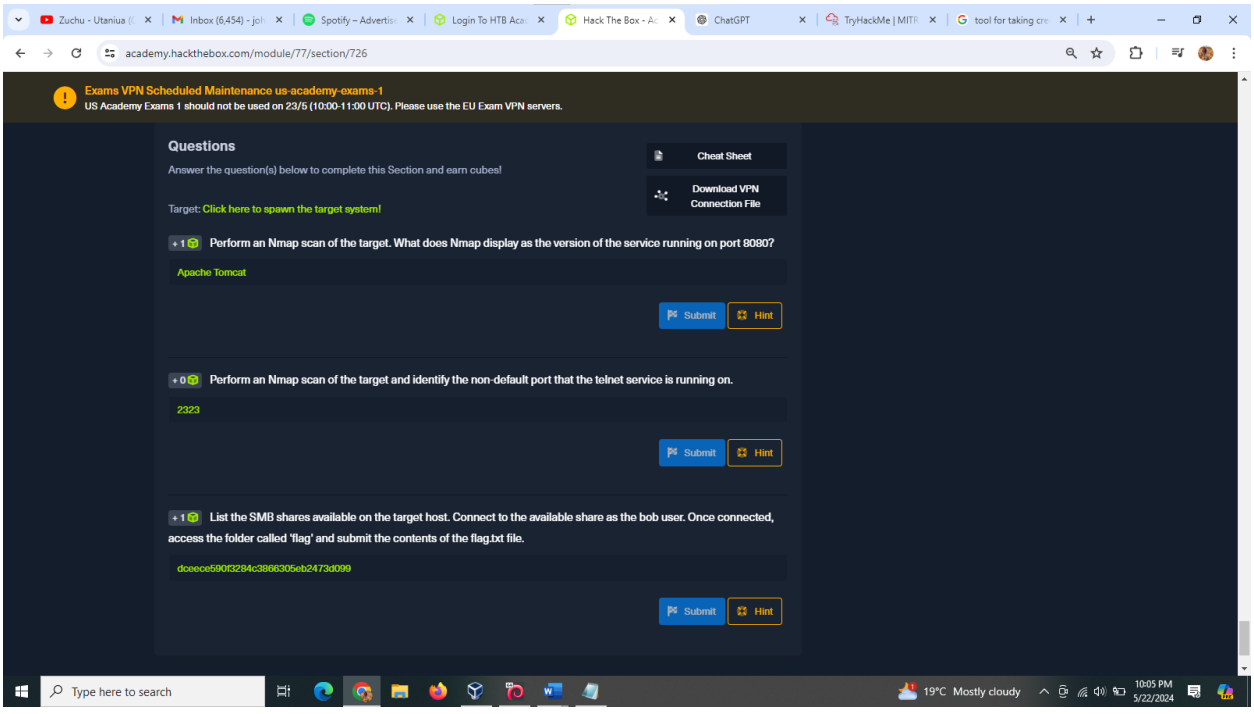
cs-sa07-24019
John Mutave





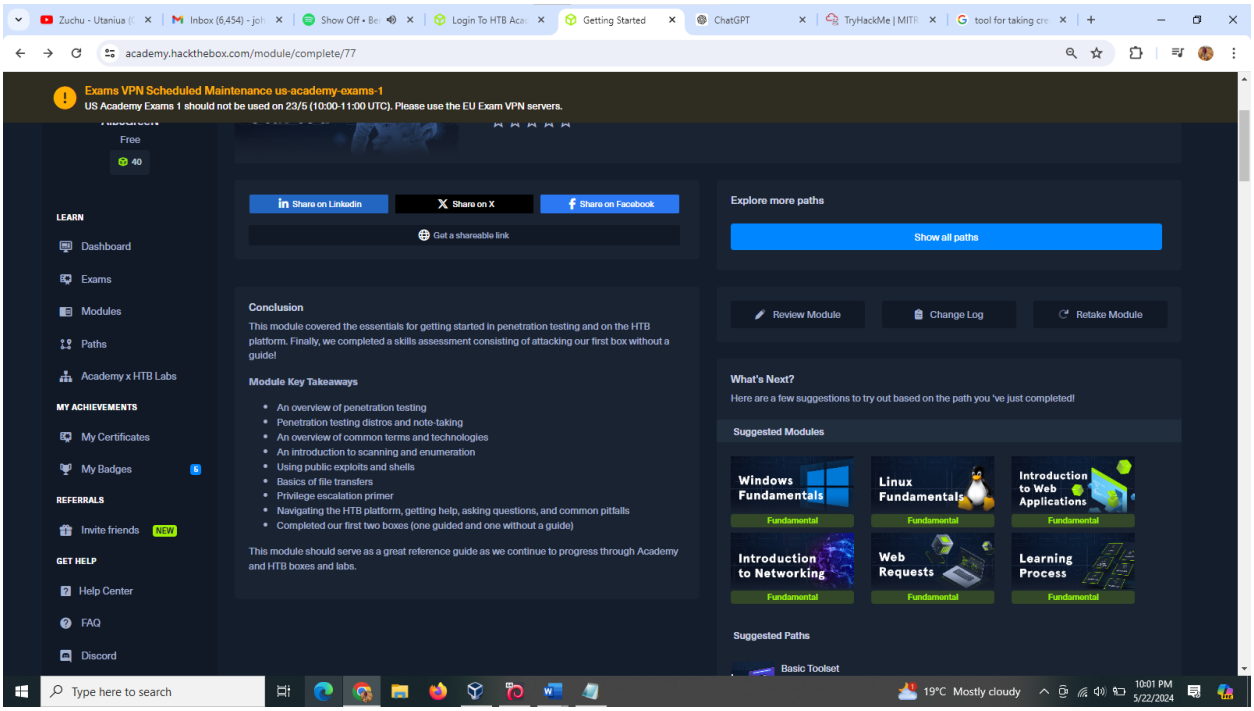
cs-sa07-24019
John Mutave





cs-sa07-24019
John Mutave

Shareable link- https://academy.hackthebox.com/achievement/1296187/77



Conclusion

This module covered the essentials for getting started in penetration testing and on the HTB platform. Finally, I completed a skills assessment consisting of attacking our first box without a guide!

Module Key Takeaways

An overview of penetration testing

Penetration testing distros and note-taking

An overview of common terms and technologies

An introduction to scanning and enumeration

Using public exploits and shells

Basics of file transfers

Privilege escalation primer