

Paths completed: 1  
Targets compromised: 68  
Ranking: Top 5%

PATHS COMPLETED



### Operating System Fundamentals

3 Modules **Easy**

To succeed in information security, we must have a deep understanding of the Windows and Linux operating systems and be comfortable navigating the command line on both as a "power user." Much of our time in any role, but especially penetration testing, is spent in a Linux shell, Windows cmd or PowerShell console, so we must have the skills to navigate both types of operating systems with ease, manage system services, install applications, manage permissions, and harden the systems we work from in accordance with security best practices.

PROGRESS

100% Completed



MODULE



### Intro to Academy

8 Sections **Fundamental** **General**

Your first step in Hack The Box Academy to become acquainted with the platform, its features, and its learning process.

PROGRESS

100% Completed



### Learning Process

20 Sections **Fundamental** **General**

The learning process is one of the essential and most important components that is often overlooked. This module does not teach you techniques to learn but describes the process of learning adapted to the field of information security. You will learn to understand how and when we learn best and increase and improve your learning efficiency greatly.

100% Completed

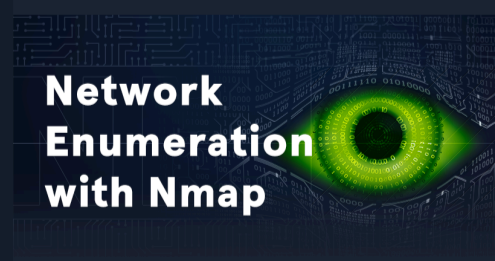


### Linux Fundamentals

30 Sections **Fundamental** **General**

This module covers the fundamentals required to work comfortably with the Linux operating system and shell.

100% Completed



### Network Enumeration with Nmap

12 Sections **Easy** **Offensive**

Nmap is one of the most used networking mapping and discovery tools because of its accurate results and efficiency. The tool is widely used by both offensive and defensive security practitioners. This module covers fundamentals that will be needed to use the Nmap tool for performing effective network enumeration.

100% Completed



### Introduction to Bash Scripting

10 Sections **Easy** **General**

This module covers the basics needed for working with Bash scripts to automate tasks on Linux systems. A strong grasp of Bash is a fundamental skill for anyone working in a technical information security role. Through the power of automation, we can unlock the Linux operating system's full potential and efficiently perform habitual tasks.

100% Completed



## Web Requests



### Web Requests

8 Sections **Fundamental** **General**

This module introduces the topic of HTTP web requests and how different web applications utilize them to communicate with their backends.

100% Completed



## Introduction to Networking



### Introduction to Networking

21 Sections **Fundamental** **General**

As an information security professional, a firm grasp of networking fundamentals and the required components is necessary. Without a strong foundation in networking, it will be tough to progress in any area of information security. Understanding how a network is structured and how the communication between the individual hosts and servers takes place using the various protocols allows us to understand the entire network structure and its network traffic in detail and how different communication standards are handled. This knowledge is essential to create our tools and to interact with the protocols.

100% Completed



## Windows Fundamentals



### Windows Fundamentals

14 Sections **Fundamental** **General**

This module covers the fundamentals required to work comfortably with the Windows operating system.

100% Completed



## Introduction to Active Directory



### Introduction to Active Directory

16 Sections **Fundamental** **General**

Active Directory (AD) is present in the majority of corporate environments. Due to its many features and complexity, it presents a vast attack surface. To be successful as penetration testers and information security professionals, we must have a firm understanding of Active Directory fundamentals, AD structures, functionality, common AD flaws, misconfigurations, and defensive measures.

100% Completed



## Introduction to Web Applications



### Introduction to Web Applications

17 Sections **Fundamental** **General**

In the Introduction to Web Applications module, you will learn all of the basics of how web applications work and begin to look at them from an information security perspective.

100% Completed



## Getting Started



### Getting Started

23 Sections **Fundamental** **Offensive**

This module covers the fundamentals of penetration testing and an introduction to Hack The Box.

100% Completed



## Intro to Assembly Language

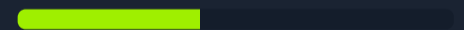


### Intro to Assembly Language

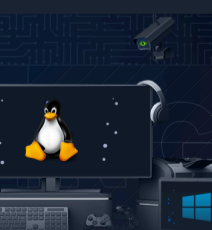
24 Sections **Medium** **General**

This module builds the core foundation for Binary Exploitation by teaching Computer Architecture and Assembly language basics.

41.67% Completed



## Setting Up



### Setting Up

9 Sections **Fundamental** **General**

This module covers topics that will help us be better prepared before conducting penetration tests. Preparations before a penetration test can often take a lot of time and effort, and this module shows how to prepare efficiently.

100% Completed



## Penetration Testing Process



### Penetration Testing Process

15 Sections **Fundamental** **General**

This module teaches the penetration testing process broken down into each stage and discussed in detail. We will cover many aspects of the role of a penetration tester during a penetration test, explained and illustrated with detailed examples. The module also covers pre-engagement steps like the criteria for establishing a contract with a client for a penetration testing engagement.

100% Completed



## Incident Handling Process



### Incident Handling Process

9 Sections **Fundamental** **General**

Security Incident handling has become a vital part of each organization's defensive strategy, as attacks constantly evolve and successful compromises are becoming a daily occurrence. In this module, we will review the process of handling an incident from the very early stage of detecting a suspicious event, to confirming a compromise and responding to it.

100% Completed



## MacOS Fundamentals



### MacOS Fundamentals

11 Sections **Fundamental** **General**

This module covers the fundamentals required to work comfortably within the macOS operating system and shell.

100% Completed



## Introduction to Windows Command Line



### Introduction to Windows Command Line

23 Sections **Easy** **General**

As administrators and Pentesters, we may not always be able to utilize a graphical user interface for the actions we need to perform. Introduction to Windows Command Line aims to introduce students to the wide range of uses for Command Prompt and PowerShell within a Windows environment. We will cover basic usage of both key executables for administration, useful PowerShell cmdlets and modules, and different ways to leverage these tools to our benefit.

100% Completed

