


Paths completed: 2  
Targets compromised: 52  
Ranking: Top 5%

PATHS COMPLETED

PROGRESS




### Cracking into Hack the Box

3 Modules **Easy**

To be successful in any technical information security role, we must have a broad understanding of specialized tools, tactics, and terminology. This path introduces core concepts necessary for anyone interested in a hands-on technical infosec role. The modules also provide the essential prerequisite knowledge for joining the main Hack The Box platform, progressing through Starting Point through easy-rated retired machines, and solving "live" machines with no walkthrough. It also includes helpful information about staying organized, navigating the HTB platforms, common pitfalls, and selecting a penetration testing distribution. Students will complete their first box during this path with a guided walkthrough and be challenged to complete a box on their own by applying the knowledge learned in the Getting Started module.

100% 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.

100% Completed

MODULE

PROGRESS

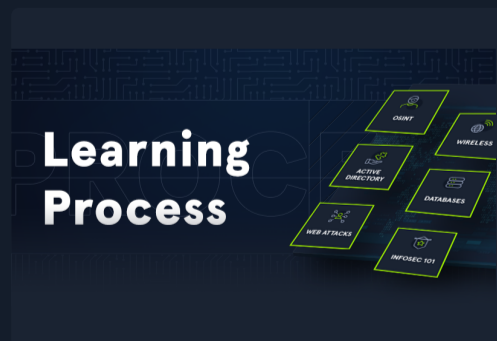


### Intro to Academy

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

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

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.

30% 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

## Introduction to Bash Scripting



### 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



## Using the Metasploit Framework



### Using the Metasploit Framework

15 Sections **Easy** **Offensive**

The Metasploit Framework is an open-source set of tools used for network enumeration, attacks, testing security vulnerabilities, evading detection, performing privilege escalation attacks, and performing post-exploitation.

100% Completed



## JavaScript Deobfuscation



### JavaScript Deobfuscation

11 Sections **Easy** **Defensive**

This module will take you step-by-step through the fundamentals of JavaScript Deobfuscation until you can deobfuscate basic JavaScript code and understand its purpose.

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



## 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



## 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



## Introduction to Python 3



### Introduction to Python 3

14 Sections **Easy** **General**

Automating tedious or otherwise impossible tasks is highly valued during both penetration testing engagements and everyday life. Introduction to Python 3 aims to introduce the student to the world of scripting with Python 3 and covers the essential building blocks needed for a beginner to understand programming. Some advanced topics are also covered for the more experienced student. In a guided fashion and starting soft, the final goal of this module is to equip the reader with enough know-how to be able to implement simple yet useful pieces of software.

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.

30.43% Completed

