

Paths completed: 4
Targets compromised: 80
Ranking: Top 5%

PATHS COMPLETED

PROGRESS

 <p>Cracking Into HTB</p>	<p>Cracking into Hack the Box</p> <p>3 Modules Easy</p> <p>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.</p>	<p>100% Completed</p> <div style="width: 100%;"><div style="width: 100%;"></div></div>
 <p>Operating System Fundamentals</p>	<p>Operating System Fundamentals</p> <p>3 Modules Easy</p> <p>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.</p>	<p>100% Completed</p> <div style="width: 100%;"><div style="width: 100%;"></div></div>
 <p>Information Security Foundations</p>	<p>Information Security Foundations</p> <p>12 Modules Easy</p> <p>Information Security is a field with many specialized and highly technical disciplines. Job roles like Penetration Tester & Information Security Analyst require a solid technical foundational understanding of core IT & Information Security topics. This skill path is made up of modules that will assist learners in developing &/or strengthening a foundational understanding before proceeding with learning the more complex security topics. Every long-standing building first needs a solid foundation. Welcome to Information Security Foundations.</p>	<p>100% Completed</p> <div style="width: 100%;"><div style="width: 100%;"></div></div>
 <p>SOC Analyst Prerequisites</p>	<p>SOC Analyst Prerequisites</p> <p>10 Modules Easy</p> <p>The SOC Analyst Prerequisites path is designed for those looking to become SOC/Security Analysts. It dives into fundamental IT and Information Security subjects including networking, Linux and Windows operating systems, basic programming and scripting, as well as working with Assembly. In addition, students will be exposed to the fundamental concepts of information security and penetration testing. This skill path is made up of modules that will assist learners in developing and strengthening a foundational understanding before proceeding with learning more complex security topics.</p>	<p>100% Completed</p> <div style="width: 100%;"><div style="width: 100%;"></div></div>

Intro to Academy



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



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



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



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



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



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



Login Brute Forcing

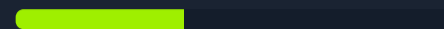


Login Brute Forcing

13 Sections **Easy** **Offensive**

The module contains an exploration of brute-forcing techniques, including the use of tools like Hydra and Medusa, and the importance of strong password practices. It covers various attack scenarios, such as targeting SSH, FTP, and web login forms.

38.46% 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 Network Traffic Analysis



Intro to Network Traffic Analysis

15 Sections **Medium** **General**

Network traffic analysis is used by security teams to monitor network activity and look for anomalies that could indicate security and operational issues. Offensive security practitioners can use network traffic analysis to search for sensitive data such as credentials, hidden applications, reachable network segments, or other potentially sensitive information "on the wire." Network traffic analysis has many uses for attackers and defenders alike.

100% Completed



Intro to Assembly Language



Intro to Assembly Language

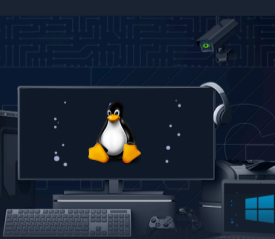
24 Sections **Medium** **General**

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

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



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



Introduction to Information Security



Introduction to Information Security

24 Sections **Fundamental** **General**

This theoretical module provides a comprehensive introduction to the foundational components of information security, focusing on the structure and operation of effective InfoSec frameworks. It explores the theoretical roles of security applications across networks, software, mobile devices, cloud environments, and operational systems, emphasizing their importance in protecting organizational assets. Students will gain an understanding of common threats, including malware and advanced persistent threats (APTs), alongside strategies for mitigating these risks. The module also introduces the roles and responsibilities of security teams and InfoSec professionals, equipping students with the confidence to advance their knowledge and explore specialized areas within the field.

100% Completed



Introduction to Penetration Testing



Introduction to Penetration Testing

21 Sections **Fundamental** **Offensive**

In this module, we will get into the fundamentals of penetration testing, a critical aspect of cybersecurity theory that explains how professionals in the field operate and underscores the significance of penetration testing within cybersecurity practices.

100% Completed

