Paths completed: 1
Targets compromised: 84
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

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.

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.

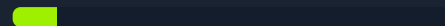100% Completed

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.

10% Completed

File Transfers

10 Sections   Medium   Offensive

During an assessment, it is very common for us to transfer files to and from a target system. This module covers file transfer techniques leveraging tools commonly available across all versions of Windows and Linux systems.

100% Completed

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
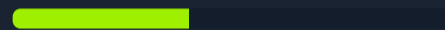
Using the Metasploit Framework

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.

40% Completed

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

14 Sections   Fundamental   General

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

100% Completed

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

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

23 Sections   Fundamental   Offensive

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

100% Completed

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.
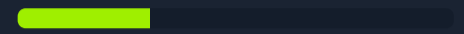
100% Completed

Cross-Site Scripting (XSS)

10 Sections · Easy · Offensive

Cross-Site Scripting (XSS) vulnerabilities are among the most common web application vulnerabilities. An XSS vulnerability may allow an attacker to execute arbitrary JavaScript code within the target's browser and result in complete web application compromise if chained together with other vulnerabilities. This module will teach you how to identify XSS vulnerabilities and exploit them.

30% Completed

Vulnerability Assessment

17 Sections · Easy · Offensive

This module introduces the concept of Vulnerability Assessments. We will review the differences between vulnerability assessments and penetration tests, how to carry out a vulnerability assessment, how to interpret the assessment results, and how to deliver an effective vulnerability assessment report.

100% Completed

Footprinting

21 Sections · Medium · Offensive

This module covers techniques for footprinting the most commonly used services in almost all enterprise and business IT infrastructures. Footprinting is an essential phase of any penetration test or security audit to identify and prevent information disclosure. Using this process, we examine the individual services and attempt to obtain as much information from them as possible.
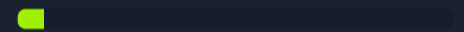
100% Completed

Shells & Payloads

17 Sections · Medium · Offensive

Gain the knowledge and skills to identify and use shells & payloads to establish a foothold on vulnerable Windows & Linux systems. This module utilizes a fictitious scenario where the learner will place themselves in the perspective of a sysadmin trying out for a position on CAT5 Security's network penetration testing team.

5.88% Completed

Information Gathering - Web Edition

19 Sections · Easy · Offensive

This module equips learners with essential web reconnaissance skills, crucial for ethical hacking and penetration testing. It explores both active and passive techniques, including DNS enumeration, web crawling, analysis of web archives and HTTP headers, and fingerprinting web technologies.

100% Completed

Intro to Academy's Purple Modules

12 Sections · Medium · Purple

This module will introduce you to HTB Academy's Purple modules, which bridge the gap between Offensive and Defensive modules and provide a holistic view of both the attacking and defending perspectives on the covered topics. More specifically, the Purple modules will allow for in-depth forensic analysis through detailed logging, traffic and memory capturing, and an installed DFIR toolset within each target after completing the attack part of each section.

50% Completed

Network Foundations

12 Sections Fundamental General

This course introduces the basic concepts essential to understanding the world of networking. Students will learn about various network types such as LANs and WANs, discuss fundamental networking principles including the OSI and TCP/IP models, and explore key network components like routers and servers. The course also covers important topics such as IP addressing, network security, and internet architecture, providing a comprehensive overview of networking that is crucial for any IT professional.

100% Completed

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