Paths completed: 1
Targets compromised: 75
Ranking: Top 1%

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

Introduction to Academy

`8 Sections` `Fundamental` `General`

This module is recommended for new users. It allows users to become acquainted with the platform and the learning process.

100% Completed

SQL Injection Fundamentals

`17 Sections` `Medium` `Offensive`

Databases are an important part of web application infrastructure and SQL (Structured Query Language) to store, retrieve, and manipulate information stored in them. SQL injection is a code injection technique used to take advantage of coding vulnerabilities and inject SQL queries via an application to bypass authentication, retrieve data from the back-end database, or achieve code execution on the underlying server.

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

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

Learning Process

`12 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

`18 Sections` `Fundamental` `General`

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

100% Completed

Stack-Based Buffer Overflows on Linux x86

`13 Sections` `Medium` `Offensive`

Buffer overflows are common vulnerabilities in software applications that can be exploited to achieve remote code execution (RCE) or perform a Denial-of-Service (DoS) attack. These vulnerabilities are caused by insecure coding, resulting in an attacker being able to overrun a program's buffer and overwrite adjacent memory locations, changing the program's execution path and resulting in unintended actions.

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

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

Introduction to Networking

`12 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

File Transfers

`8 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

Attacking Web Applications with Ffuf

`13 Sections` `Easy` `Offensive`

This module covers the fundamental enumeration skills of web fuzzing and directory brute forcing using the Ffuf tool. The techniques learned in this module will help us in locating hidden pages, directories, and parameters when targeting web applications.

100% Completed

Windows Fundamentals

14 Sections   Fundamental   General

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

78.57% Completed

File Inclusion

11 Sections   Medium   Offensive

File Inclusion is a common web application vulnerability, which can be easily overlooked as part of a web application's functionality.

63.64% Completed