



Paths completed: 2
Targets compromised: 68
Ranking: Top 5%

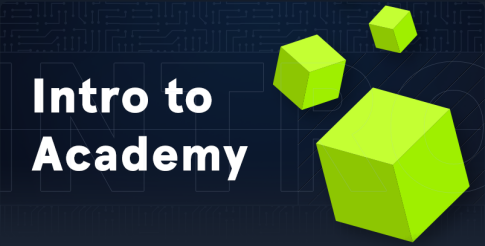


PATHS COMPLETED

PROGRESS

	<div>Operating System Fundamentals</div> <div>2 Modules Easy</div> <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>	<div>100% Completed</div> <div></div>
	<div>Cracking into Hack the Box</div> <div>3 Modules Easy</div> <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>	<div>100% Completed</div> <div></div>

MODULE

PROGRESS

	<div>Introduction to Academy</div> <div>8 Sections Fundamental General</div> <p>This module is recommended for new users. It allows users to become acquainted with the platform and the learning process.</p>	<div>100% Completed</div> <div></div>
	<div>Linux Fundamentals</div> <div>18 Sections Fundamental General</div> <p>This module covers the fundamentals required to work comfortably with the Linux operating system and shell.</p>	<div>100% Completed</div> <div></div>
	<div>Windows Fundamentals</div> <div>14 Sections Fundamental General</div> <p>This module covers the fundamentals required to work comfortably with the Windows operating system.</p>	<div>100% Completed</div> <div></div>



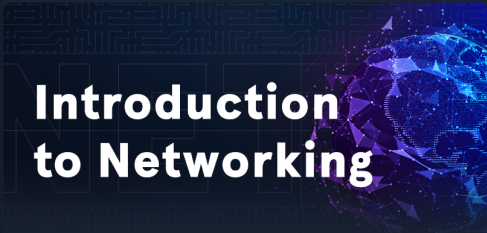
Learning Process

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.

60% Completed



Introduction to Networking

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



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



Attacking Web Applications with Ffuf

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



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



SQL Injection Fundamentals

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



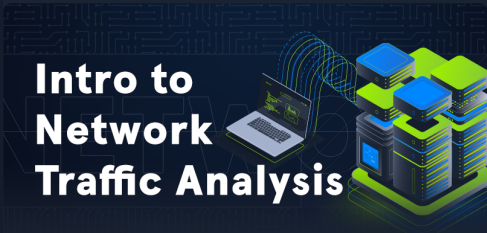
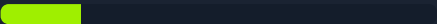
File Inclusion

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.

18.18% 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.

86.67% Completed






JavaScript Deobfuscation

11 SectionsEasyDefensive

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




Setting Up

9 SectionsFundamentalGeneral

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 Active Directory

16 SectionsFundamentalGeneral

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




Vulnerability Assessment

17 SectionsEasyOffensive

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.

70.59% Completed




Introduction to Web Applications

17 SectionsFundamentalGeneral

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



File Transfers

10 SectionsMediumOffensive

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.

10% Completed