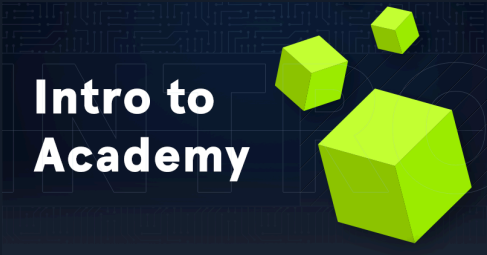


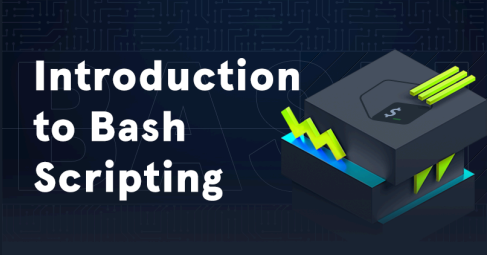
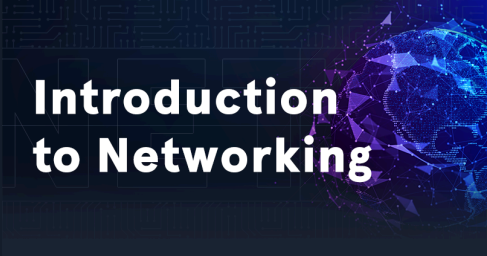
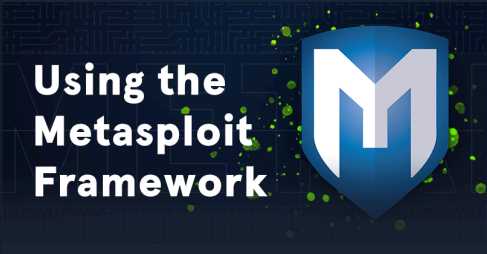



Targets compromised: 50
Ranking: Top 10%

MODULE

PROGRESS

	<div>Intro to Academy</div> <div>8 Sections Fundamental General</div> <div>Your first stop in Hack The Box Academy to become acquainted with the platform, its features, and its learning process.</div>	<div>100% Completed</div> <div></div>
	<div>Learning Process</div> <div>20 Sections Fundamental General</div> <div>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.</div>	<div>100% Completed</div> <div></div>
	<div>Linux Fundamentals</div> <div>30 Sections Fundamental General</div> <div>This module covers the fundamentals required to work comfortably with the Linux operating system and shell.</div>	<div>100% Completed</div> <div></div>
	<div>Introduction to Bash Scripting</div> <div>10 Sections Easy General</div> <div>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.</div>	<div>100% Completed</div> <div></div>
	<div>Introduction to Networking</div> <div>21 Sections Fundamental General</div> <div>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.</div>	<div>100% Completed</div> <div></div>
	<div>Using the Metasploit Framework</div> <div>15 Sections Easy Offensive</div> <div>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.</div>	<div>26.67% Completed</div> <div></div>
	<div>Windows Fundamentals</div> <div>14 Sections Fundamental General</div> <div>This module covers the fundamentals required to work comfortably with the Windows operating system.</div>	<div>100% Completed</div> <div></div>

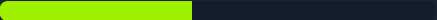


Introduction to Active Directory

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.

43.75% Completed

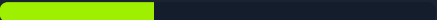


Introduction to Web Applications

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.

35.29% Completed

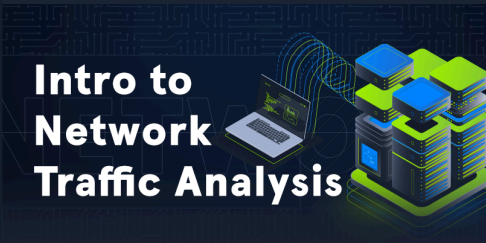


Getting Started

23 Sections Fundamental Offensive

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

100% Completed

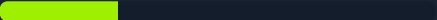


Intro to Network Traffic Analysis

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.

26.67% Completed



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

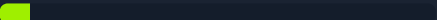


Penetration Testing Process

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.

6.67% Completed



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

