

Targets compromised: 29

Ranking: Top 20%

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

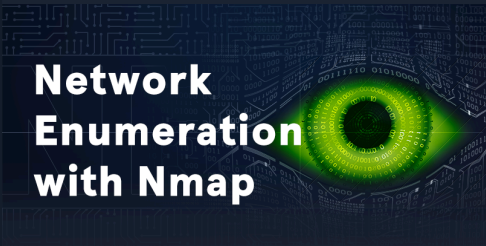


Learning Process

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



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



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



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.

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



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

