





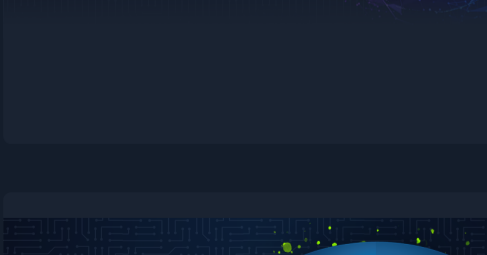


Targets compromised: 70
Ranking: Top 5%

MODULE

PROGRESS

MODULE	PROGRESS
 <h3>Intro to Academy</h3>	<h4>Introduction to Academy</h4> <p>8 Sections Fundamental General</p> <p>This module is recommended for new users. It allows users to become acquainted with the platform and the learning process.</p> <p>100% Completed</p>
 <h3>Learning Process</h3>	<h4>Learning Process</h4> <p>20 Sections Fundamental General</p> <p>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.</p> <p>100% Completed</p>
 <h3>Linux Fundamentals</h3>	<h4>Linux Fundamentals</h4> <p>30 Sections Fundamental General</p> <p>This module covers the fundamentals required to work comfortably with the Linux operating system and shell.</p> <p>86.67% Completed</p>
 <h3>SQL Injection Fundamentals</h3>	<h4>SQL Injection Fundamentals</h4> <p>17 Sections Medium Offensive</p> <p>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.</p> <p>100% Completed</p>
 <h3>Web Requests</h3>	<h4>Web Requests</h4> <p>8 Sections Fundamental General</p> <p>This module introduces the topic of HTTP web requests and how different web applications utilize them to communicate with their backends.</p> <p>100% Completed</p>
 <h3>Introduction to Networking</h3>	<h4>Introduction to Networking</h4> <p>21 Sections Fundamental General</p> <p>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.</p> <p>100% Completed</p>
 <h3>Using the Metasploit Framework</h3>	<h4>Using the Metasploit Framework</h4> <p>15 Sections Easy Offensive</p> <p>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.</p> <p>73.33% Completed</p>

Windows Fundamentals



Windows Fundamentals

14 Sections **Fundamental** **General**

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

100% Completed



Introduction to Web Applications



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



Getting Started

23 Sections **Fundamental** **Offensive**

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

100% Completed



Setting Up



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



Footprinting



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



Web Attacks

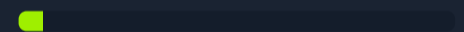


Web Attacks

18 Sections **Medium** **Offensive**

This module covers three common web vulnerabilities, HTTP Verb Tampering, IDOR, and XXE, each of which can have a significant impact on a company's systems. We will cover how to identify, exploit, and prevent each of them through various methods.

5.56% Completed



Information Gathering - Web Edition



Information Gathering - Web Edition

10 Sections **Easy** **Offensive**

This module covers techniques for identifying and analyzing an organization's web application-based attack surface and tech stack. Information gathering is an essential part of any web application penetration test, and it can be performed either passively or actively.

70% Completed



MacOS Fundamentals

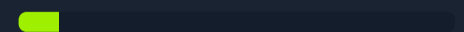


MacOS Fundamentals

11 Sections **Fundamental** **General**

This module covers the fundamentals required to work comfortably within the macOS operating system and shell.

9.09% Completed



Penetration Testing Process



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.

20% Completed

