

Targets compromised: 57

Ranking: Top 10%

MODULE

PROGRESS

	<div>Intro to Academy</div> <div>8 SectionsFundamentalGeneral</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>Network Enumeration with Nmap</div> <div>12 SectionsEasyOffensive</div> <div>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.</div>	<div>100% Completed</div> <div></div>
	<div>File Transfers</div> <div>10 SectionsMediumOffensive</div> <div>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.</div>	<div>100% Completed</div> <div></div>
	<div>SQL Injection Fundamentals</div> <div>17 SectionsMediumOffensive</div> <div>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.</div>	<div>100% Completed</div> <div></div>
	<div>File Inclusion</div> <div>11 SectionsMediumOffensive</div> <div>File Inclusion is a common web application vulnerability, which can be easily overlooked as part of a web application's functionality.</div>	<div>27.27% Completed</div> <div></div>
	<div>Using the Metasploit Framework</div> <div>15 SectionsEasyOffensive</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>100% Completed</div> <div></div>
	<div>JavaScript Deobfuscation</div> <div>11 SectionsEasyDefensive</div> <div>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.</div>	<div>100% Completed</div> <div></div>




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




Vulnerability Assessment

17 Sections **Easy** **Offensive**

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.

100% Completed




Web Fuzzing

12 Sections **Easy** **Offensive**

In this module, we explore the essential techniques and tools for fuzzing web applications, an essential practice in cybersecurity for identifying hidden vulnerabilities and strengthening web application security.

100% Completed



Pentest in a Nutshell

24 Sections **Easy** **Offensive**

This module focuses on providing a detailed, guided simulation of a real penetration test, emphasizing the fine details of the penetration testing process. It guides you through each step, from reconnaissance to exploitation, mirroring the techniques and methodologies used by professional penetration testers. It offers hands-on experience in a controlled environment and aims to deepen understanding and sharpen skills essential for effective cybersecurity assessments.

37.5% Completed