
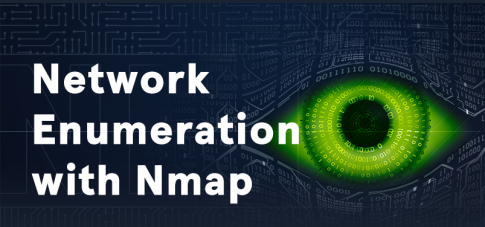







Targets compromised: 37
Ranking: Top 10%

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>Network Enumeration with Nmap</div> <div>12 Sections Easy Offensive</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>Getting Started</div> <div>23 Sections Fundamental Offensive</div> <div>This module covers the fundamentals of penetration testing and an introduction to Hack The Box.</div>	<div>100% Completed</div> <div></div>
	<div>Penetration Testing Process</div> <div>15 Sections Fundamental General</div> <div>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.</div>	<div>100% Completed</div> <div></div>
	<div>Vulnerability Assessment</div> <div>17 Sections Easy Offensive</div> <div>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.</div>	<div>47.06% Completed</div> <div></div>
	<div>Footprinting</div> <div>21 Sections Medium Offensive</div> <div>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.</div>	<div>100% Completed</div> <div></div>
	<div>Information Gathering - Web Edition</div> <div>19 Sections Easy Offensive</div> <div>This module equips learners with essential web reconnaissance skills, crucial for ethical hacking and penetration testing. It explores both active and passive techniques, including DNS enumeration, web crawling, analysis of web archives and HTTP headers, and fingerprinting web technologies.</div>	<div>100% Completed</div> <div></div>

