


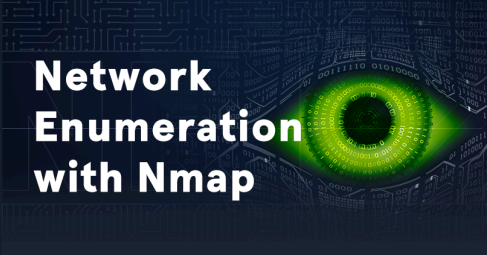






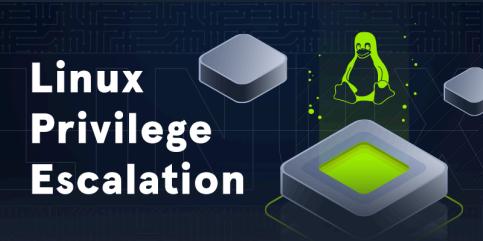



Targets compromised: 27

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>Learning Process</div> <div>20 SectionsFundamentalGeneral</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 SectionsFundamentalGeneral</div> <div>This module covers the fundamentals required to work comfortably with the Linux operating system and shell.</div>	<div>43.33% 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>41.67% Completed</div> <div></div>
	<div>Introduction to Bash Scripting</div> <div>10 SectionsEasyGeneral</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>10% 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>10% Completed</div> <div></div>
	<div>Web Requests</div> <div>8 SectionsFundamentalGeneral</div> <div>This module introduces the topic of HTTP web requests and how different web applications utilize them to communicate with their backends.</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>	18.18% Completed <div></div>
	<div>Introduction to Networking</div> <div>21 SectionsFundamentalGeneral</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>	38.1% Completed <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>	100% Completed <div></div>
	<div>Linux Privilege Escalation</div> <div>28 SectionsEasyOffensive</div> <div>Privilege escalation is a crucial phase during any security assessment. During this phase, we attempt to gain access to additional users, hosts, and resources to move closer to the assessment's overall goal. There are many ways to escalate privileges. This module aims to cover the most common methods emphasizing real-world misconfigurations and flaws that we may encounter in a client environment. The techniques covered in this module are not an exhaustive list of all possibilities and aim to avoid extreme "edge-case" tactics that may be seen in a Capture the Flag (CTF) exercise.</div>	14.29% Completed <div></div>
	<div>Introduction to Active Directory</div> <div>16 SectionsFundamentalGeneral</div> <div>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.</div>	68.75% Completed <div></div>
	<div>Getting Started</div> <div>23 SectionsFundamentalOffensive</div> <div>This module covers the fundamentals of penetration testing and an introduction to Hack The Box.</div>	30.43% Completed <div></div>
	<div>Setting Up</div> <div>9 SectionsFundamentalGeneral</div> <div>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.</div>	100% Completed <div></div>
	<div>Penetration Testing Process</div> <div>15 SectionsFundamentalGeneral</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>	100% Completed <div></div>



Vulnerability Assessment

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



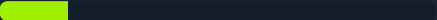
Web Service & API Attacks

Web Service & API Attacks

13 Sections **Medium** **Offensive**

Web services and APIs are frequently exposed to provide certain functionalities in a programmatic way between heterogeneous devices and software components. Both web services and APIs can assist in integrating different applications or facilitate separation within a given application. This module covers how to identify the functionality a web service or API offers and exploit any security-related inefficiencies.

15.38% Completed



Introduction to Threat Hunting & Hunting With Elastic

Introduction to Threat Hunting & Hunting With Elastic

6 Sections **Medium** **Defensive**

This module initially lays the groundwork for understanding Threat Hunting, ranging from its basic definition, to the structure of a threat hunting team. The module also dives into the threat hunting process, highlighting the interrelationships between threat hunting, risk assessment, and incident handling. Furthermore, the module elucidates the fundamentals of Cyber Threat Intelligence (CTI). It expands on the different types of threat intelligence and offers guidance on effectively interpreting a threat intelligence report. Finally, the module puts theory into practice, showcasing how to conduct threat hunting using the Elastic stack. This practical segment uses real-world logs to provide learners with hands-on experience.

50% Completed



Brief Intro to Hardware Attacks

Brief Intro to Hardware Attacks

8 Sections **Medium** **General**

This mini-module concisely introduces hardware attacks, covering Bluetooth risks and attacks, Cryptanalysis Side-Channel Attacks, and vulnerabilities like Spectre and Meltdown. It delves into both historical and modern Bluetooth hacking techniques, explores the principles of cryptanalysis and different side-channel attacks, and outlines microprocessor design, optimisation strategies and vulnerabilities, such as Spectre and Meltdown.

100% Completed



Security Incident Reporting

Security Incident Reporting

5 Sections **Easy** **General**

Tailored to provide a holistic understanding, this Hack The Box Academy module ensures participants are adept at identifying, categorizing, and documenting security incidents with utmost accuracy and professionalism. The module meticulously breaks down the elements of a robust incident report and then presents participants with a real-world incident report, offering practical insights into the application of the concepts discussed.

100% Completed

