


Targets compromised: 91
Ranking: Top 5%

MODULE

PROGRESS

	<div>Network Enumeration with Nmap</div> <div>12 SectionsEasyOffensive</div> <p>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.</p>	<div>100% Completed</div> <div></div>
	<div>File Transfers</div> <div>10 SectionsMediumOffensive</div> <p>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.</p>	<div>100% Completed</div> <div></div>
	<div>Using the Metasploit Framework</div> <div>15 SectionsEasyOffensive</div> <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>	<div>100% Completed</div> <div></div>
	<div>Introduction to Active Directory</div> <div>16 SectionsFundamentalGeneral</div> <p>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.</p>	<div>100% Completed</div> <div></div>
	<div>Getting Started</div> <div>23 SectionsFundamentalOffensive</div> <p>This module covers the fundamentals of penetration testing and an introduction to Hack The Box.</p>	<div>100% Completed</div> <div></div>
	<div>Penetration Testing Process</div> <div>15 SectionsFundamentalGeneral</div> <p>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.</p>	<div>100% Completed</div> <div></div>




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




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.

90.48% Completed




Shells & Payloads

17 Sections **Medium** **Offensive**

Gain the knowledge and skills to identify and use shells & payloads to establish a foothold on vulnerable Windows & Linux systems. This module utilizes a fictitious scenario where the learner will place themselves in the perspective of a sysadmin trying out for a position on CAT5 Security's network penetration testing team.

100% Completed




Attacking Common Services

19 Sections **Medium** **Offensive**

Organizations regularly use a standard set of services for different purposes. It is vital to conduct penetration testing activities on each service internally and externally to ensure that they are not introducing security threats. This module will cover how to enumerate each service and test it against known vulnerabilities and exploits with a standard set of tools.

94.74% Completed




Information Gathering - Web Edition

19 Sections **Easy** **Offensive**

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.

100% Completed




Password Attacks

26 Sections **Medium** **Offensive**

Passwords are still the primary method of authentication in corporate networks. If strong password policies are not enforced, users often choose weak, easy-to-remember passwords that can be cracked offline and leveraged to escalate access. As penetration testers, we encounter passwords in many forms during our assessments. It's essential to understand how passwords are stored, how they can be retrieved, methods for cracking weak passwords, techniques for using hashes that cannot be cracked, and how to identify weak or default password usage.

100% Completed



Incident Handling Process

9 Sections **Fundamental** **General**

Security Incident handling has become a vital part of each organization's defensive strategy, as attacks constantly evolve and successful compromises are becoming a daily occurrence. In this module, we will review the process of handling an incident from the very early stage of detecting a suspicious event, to confirming a compromise and responding to it.

100% Completed



Security Monitoring & SIEM Fundamentals

11 Sections Easy Defensive

This module provides a concise yet comprehensive overview of Security Information and Event Management (SIEM) and the Elastic Stack. It demystifies the essential workings of a Security Operation Center (SOC), explores the application of the MITRE ATT&CK framework within SOCs, and introduces SIEM (KQL) query development. With a focus on practical skills, students will learn how to develop SIEM use cases and visualizations using the Elastic Stack.

100% Completed

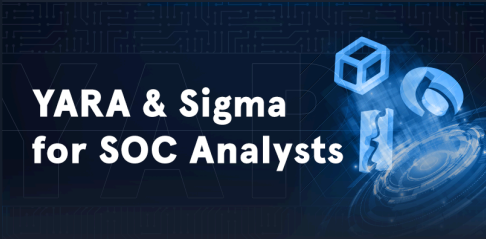


Windows Event Logs & Finding Evil

6 Sections Medium Defensive

This module covers the exploration of Windows Event Logs and their significance in uncovering suspicious activities. Throughout the course, we delve into the anatomy of Windows Event Logs and highlight the logs that hold the most valuable information for investigations. The module also focuses on utilizing Sysmon and Event Logs for detecting and analyzing malicious behavior. Additionally, we delve into Event Tracing for Windows (ETW), explaining its architecture and components, and provide ETW-based detection examples. To streamline the analysis process, we introduce the powerful Get-WinEvent cmdlet.

83.33% Completed



YARA & Sigma for SOC Analysts

11 Sections Easy Defensive

This Hack The Box Academy module covers how to create YARA rules both manually and automatically and apply them to hunt threats on disk, live processes, memory, and online databases. Then, the module switches gears to Sigma rules covering how to build Sigma rules, translate them into SIEM queries using "sigmac", and hunt threats in both event logs and SIEM solutions. It's all hands-on, using real-world malware and techniques.

9.09% Completed

