
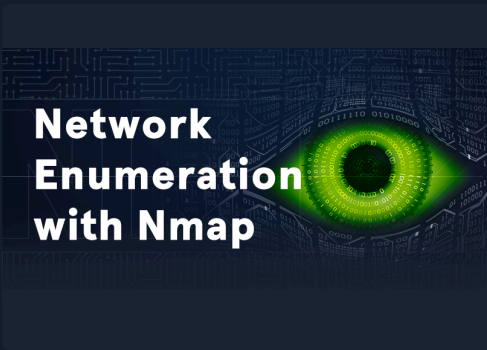






Targets compromised: 55  
Ranking: Top 5%

MODULE

PROGRESS

	<div>Linux Fundamentals</div> <div>30 Sections Fundamental General</div> <div>This module covers the fundamentals required to work comfortably with the Linux operating system and shell.</div>	<div>26.67% 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>33.33% 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>69.57% Completed</div> <div></div>
	<div>Intro to Network Traffic Analysis</div> <div>15 Sections Medium General</div> <div>Network traffic analysis is used by security teams to monitor network activity and look for anomalies that could indicate security and operational issues. Offensive security practitioners can use network traffic analysis to search for sensitive data such as credentials, hidden applications, reachable network segments, or other potentially sensitive information "on the wire." Network traffic analysis has many uses for attackers and defenders alike.</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>Incident Handling Process</div> <div>9 Sections Fundamental General</div> <div>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.</div>	<div>100% Completed</div> <div></div>



Windows Attacks & Defense

16 Sections Medium Defensive

Microsoft Active Directory (AD) has been, for the past 20+ years, the leading enterprise domain management suite, providing identity and access management, centralized domain administration, authentication, and much more. Throughout those years, the more integrated our applications and data have become with AD, the more exposed to a large-scale compromise we have become. In this module, we will walk through the most commonly abused and fruitful attacks against Active Directory environments that allow threat actors to perform horizontal and vertical privilege escalations in addition to lateral movement. One of the module's core goals is to showcase prevention and detection methods against the covered Active Directory attacks.

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



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.

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.

100% Completed



Understanding Log Sources & Investigating with Splunk

6 Sections Medium Defensive

This module provides a comprehensive introduction to Splunk, focusing on its architecture and the creation of effective detection-related SPL (Search Processing Language) searches. We will learn to investigate with Splunk as a SIEM tool and develop TTP-driven and analytics-driven SPL searches for enhanced threat detection and response. Through hands-on exercises, we will learn to identify and understand the ingested data and available fields within Splunk. We will also gain practical experience in leveraging Splunk's powerful features for security monitoring and incident investigation.

100% Completed



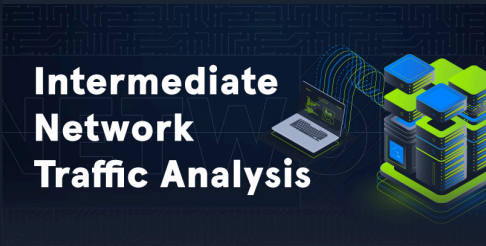
Working with IDS/IPS

11 Sections Medium Defensive

This module offers an in-depth exploration of Suricata, Snort, and Zeek, covering both rule development and intrusion detection. We'll guide you through signature-based and analytics-based rule development, and you'll learn to tackle encrypted traffic. The module features numerous hands-on examples, focusing on the detection of prevalent malware such as PowerShell Empire, Covenant, Sliver, Cerber, Dridex, Ursnif, and Patchwork. We also dive into detecting attacking techniques like DNS exfiltration, TLS/HTTP Exfiltration, PsExec lateral movement, and beaconing through IDS/IPS.

72.73% Completed





Intermediate Network Traffic Analysis

18 Sections   **Easy**   Defensive

Through network traffic analysis, this module sharpens skills in detecting link layer attacks such as ARP anomalies and rogue access points, identifying network abnormalities like IP spoofing and TCP handshake irregularities, and uncovering application layer threats from web-based vulnerabilities to peculiar DNS activities.

100% Completed

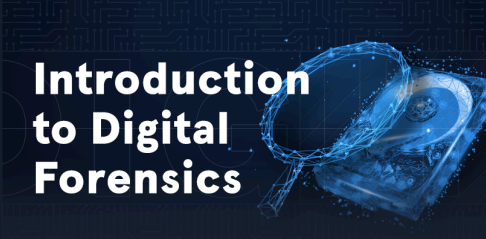


Security Incident Reporting

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



Introduction to Digital Forensics

8 Sections   Medium   Defensive

Dive into Windows digital forensics with Hack The Box Academy's "Introduction to Digital Forensics" module. Gain mastery over core forensic concepts and tools such as FTK Imager, KAPE, Velociraptor, and Volatility. Dive deep into memory forensics, disk image analysis, and rapid triaging procedures. Learn to construct timelines from MFT, USN Journals, and Windows event logs while getting hands-on with key artifacts like MFT, USN Journal, Registry Hives, Prefetch Files, ShimCache, Amcache, BAM, and SRUM data.

37.5% Completed

