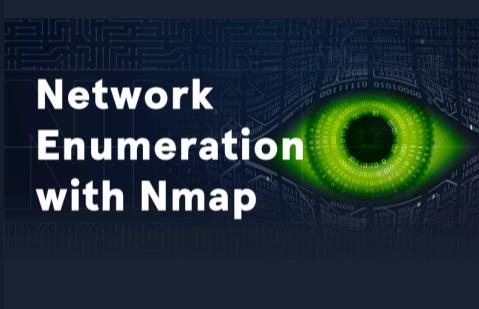


Targets compromised: 34

Ranking: Top 5%

MODULE

PROGRESS

 <h2>Intro to Academy</h2>	<p>Intro to Academy</p> <p>8 Sections Fundamental General</p> <p>Your first stop in Hack The Box Academy to become acquainted with the platform, its features, and its learning process.</p>	<p>100% Completed</p> <div style="width: 100%; background-color: #00ff00; height: 10px;"></div>
 <h2>Learning Process</h2>	<p>Learning Process</p> <p>20 Sections Fundamental General</p> <p>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.</p>	<p>100% Completed</p> <div style="width: 100%; background-color: #00ff00; height: 10px;"></div>
 <h2>Linux Fundamentals</h2>	<p>Linux Fundamentals</p> <p>30 Sections Fundamental General</p> <p>This module covers the fundamentals required to work comfortably with the Linux operating system and shell.</p>	<p>43.33% Completed</p> <div style="width: 43.33%; background-color: #00ff00; height: 10px;"></div>
 <h2>Network Enumeration with Nmap</h2>	<p>Network Enumeration with Nmap</p> <p>12 Sections Easy Offensive</p> <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>	<p>41.67% Completed</p> <div style="width: 41.67%; background-color: #00ff00; height: 10px;"></div>
 <h2>Introduction to Bash Scripting</h2>	<p>Introduction to Bash Scripting</p> <p>10 Sections Easy General</p> <p>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.</p>	<p>10% Completed</p> <div style="width: 10%; background-color: #00ff00; height: 10px;"></div>
 <h2>File Transfers</h2>	<p>File Transfers</p> <p>10 Sections Medium Offensive</p> <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>	<p>10% Completed</p> <div style="width: 10%; background-color: #00ff00; height: 10px;"></div>
 <h2>Web Requests</h2>	<p>Web Requests</p> <p>8 Sections Fundamental General</p> <p>This module introduces the topic of HTTP web requests and how different web applications utilize them to communicate with their backends.</p>	<p>100% Completed</p> <div style="width: 100%; background-color: #00ff00; height: 10px;"></div>

File Inclusion

Introduction to Networking

Using the Metasploit Framework

JavaScript Deobfuscation

Linux Privilege Escalation

Introduction to Active Directory

Getting Started

File Inclusion

11 Sections Medium Offensive

File Inclusion is a common web application vulnerability, which can be easily overlooked as part of a web application's functionality.

18.18% Completed



Introduction to Networking

21 Sections Fundamental General

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.

38.1% Completed



Using the Metasploit Framework

15 Sections Easy Offensive

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.

20% Completed



JavaScript Deobfuscation

11 Sections Easy Defensive

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.

100% Completed



Linux Privilege Escalation

28 Sections Easy Offensive

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.

14.29% Completed



Introduction to Active Directory

16 Sections Fundamental General

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.

81.25% Completed



Getting Started

23 Sections Fundamental Offensive

This module covers the fundamentals of penetration testing and an introduction to Hack The Box.

30.43% Completed





Intro to Network Traffic Analysis

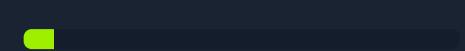
15 Sections | Medium | General

Intro to Network Traffic Analysis

15 Sections | Medium | General

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.

6.67% Completed



Setting Up

Setting Up

9 Sections | Fundamental | General

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.

100% Completed



Penetration Testing Process

Penetration Testing Process

15 Sections | Fundamental | General

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.

100% Completed



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



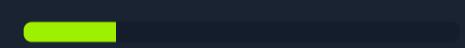
Information Gathering - Web Edition

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.

21.05% Completed



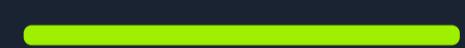
Incident Handling Process

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



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





Bug Bounty Hunting Process

6 Sections Easy General

Bug bounty programs encourage security researchers to identify bugs and submit vulnerability reports. Getting into the world of bug bounty hunting without any prior experience can be a daunting task, though. This module covers the bug bounty hunting process to help you start bug bounty hunting in an organized and well-structured way. It's all about effectiveness and professionally communicating your findings.

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.

50% Completed



Wi-Fi Penetration Testing Basics

16 Sections Medium Offensive

In today's digital age, wireless networks are ubiquitous, connecting countless devices in homes, businesses, and public spaces. With this widespread connectivity comes an increased risk of security vulnerabilities that can be exploited by malicious actors. As such, understanding and securing Wi-Fi networks has become a crucial aspect of cybersecurity. Whether you are an aspiring ethical hacker, a network administrator, or simply a tech enthusiast, gaining a solid foundation in Wi-Fi penetration testing is essential for safeguarding your digital environment.

31.25% Completed

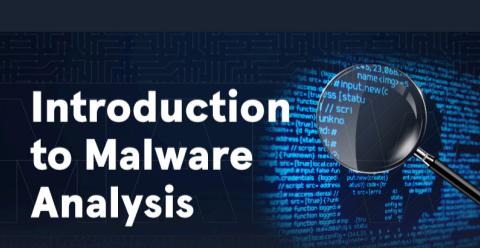


Brief Intro to Hardware Attacks

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

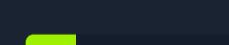


Introduction to Malware Analysis

9 Sections Hard Defensive

This module offers an exploration of malware analysis, specifically targeting Windows-based threats. The module covers Static Analysis utilizing Linux and Windows tools, Malware Unpacking, Dynamic Analysis (including malware traffic analysis), Reverse Engineering for Code Analysis, and Debugging using x64dbg. Real-world malware examples such as WannaCry, DoomJuice, Brbbot, Dharma, and Meterpreter are analyzed to provide practical experience.

11.11% 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



Introduction to Digital Forensics

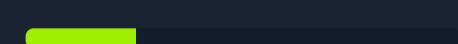


Introduction to Digital Forensics

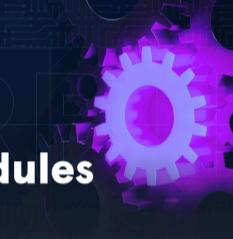
8 Sections Medium Defensive

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.

25% Completed



Intro to Academy's Purple Modules



Intro to Academy's Purple Modules

12 Sections Medium Purple

This module will introduce you to HTB Academy's Purple modules, which bridge the gap between Offensive and Defensive modules and provide a holistic view of both the attacking and defending perspectives on the covered topics. More specifically, the Purple modules will allow for in-depth forensic analysis through detailed logging, traffic and memory capturing, and an installed DFIR toolset within each target after completing the attack part of each section.

25% Completed

