Student Transcript

05-08-2025

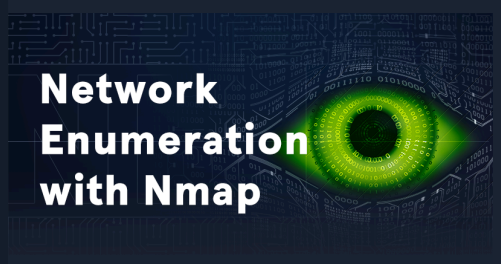
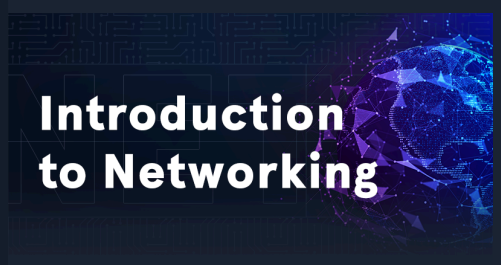
HTB ACADEMY

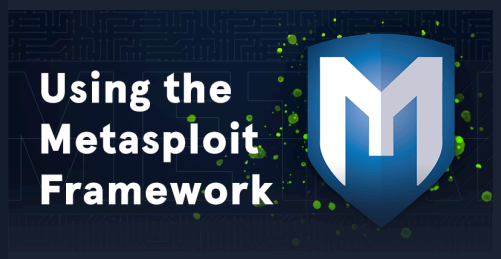
V4l3nt1n45

#484093

Targets compromised: 47

Ranking: Top 10%

MODULE		PROGRESS
	Intro to Academy 8 Sections · Fundamental · General Your first stop in Hack The Box Academy to become acquainted with the platform, its features, and its learning process.	100% Completed
	Learning Process 20 Sections · Fundamental · General 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.	100% Completed
	Linux Fundamentals 30 Sections · Fundamental · General This module covers the fundamentals required to work comfortably with the Linux operating system and shell.	100% Completed
	Network Enumeration with Nmap 12 Sections · Easy · Offensive 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.	75% Completed
	Web Requests 8 Sections · Fundamental · General This module introduces the topic of HTTP web requests and how different web applications utilize them to communicate with their backends.	100% Completed
	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.	42.86% 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.

66.67% Completed

Stack-Based Buffer Overflows on Linux x86

13 Sections | Medium | Offensive

Buffer overflows are common vulnerabilities in software applications that can be exploited to achieve remote code execution (RCE) or perform a Denial-of-Service (DoS) attack. These vulnerabilities are caused by insecure coding, resulting in an attacker being able to overrun a program's buffer and overwrite adjacent memory locations, changing the program's execution path and resulting in unintended actions.

100% Completed

Windows Fundamentals

14 Sections | Fundamental | General

This module covers the fundamentals required to work comfortably with the Windows operating system.

21.43% Completed

Attacking Web Applications with Ffuf

13 Sections | Easy | Offensive

This module covers the fundamental enumeration skills of web fuzzing and directory brute forcing using the Ffuf tool. The techniques learned in this module will help us in locating hidden pages, directories, and parameters when targeting web applications.

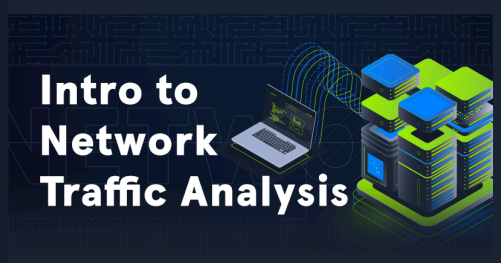
69.23% Completed

Introduction to Web Applications

17 Sections | Fundamental | General

In the Introduction to Web Applications module, you will learn all of the basics of how web applications work and begin to look at them from an information security perspective.

100% Completed

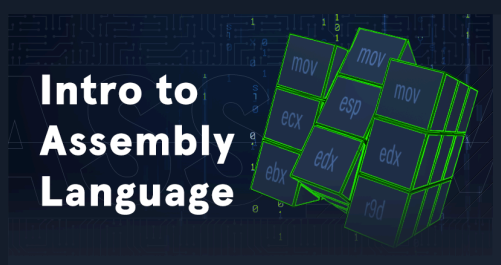


Intro to Network Traffic Analysis

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

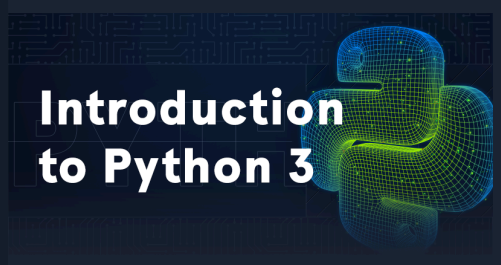


Intro to Assembly Language

24 Sections | Medium | General

This module builds the core foundation for Binary Exploitation by teaching Computer Architecture and Assembly language basics.

100% Completed



Introduction to Python 3

14 Sections | Easy | General

Automating tedious or otherwise impossible tasks is highly valued during both penetration testing engagements and everyday life. Introduction to Python 3 aims to introduce the student to the world of scripting with Python 3 and covers the essential building blocks needed for a beginner to understand programming. Some advanced topics are also covered for the more experienced student. In a guided fashion and starting soft, the final goal of this module is to equip the reader with enough know-how to be able to implement simple yet useful pieces of software.

100% Completed

Stack-Based Buffer Overflows on Windows x86

11 Sections | Medium | Offensive

This module is your first step into Windows Binary Exploitation, and it will teach you how to exploit local and remote buffer overflow vulnerabilities on Windows machines.

27.27% Completed

Using Web Proxies

15 Sections | Easy | Offensive

Web application penetration testing frameworks are an essential part of any web penetration test. This module will teach you two of the best frameworks: Burp Suite and OWASP ZAP.

20% 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.

31.58% Completed

File Upload Attacks

11 Sections | Medium | Offensive

Arbitrary file uploads are among the most critical web vulnerabilities. These flaws enable attackers to upload malicious files, execute arbitrary commands on the back-end server, and even take control over the entire server and all web applications hosted on it and potentially gain access to sensitive data or cause a service disruption.

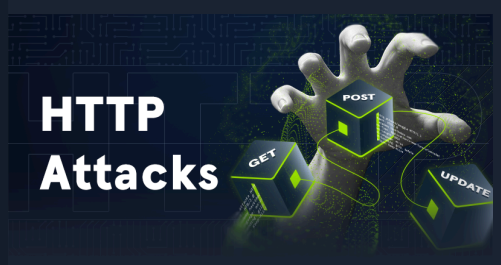
9.09% Completed

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.

6.67% Completed



HTTP Attacks

18 Sections | Hard | Offensive

This module covers three HTTP vulnerabilities: CRLF Injection, HTTP Request Smuggling, and HTTP/2 Downgrading. These vulnerabilities can arise on the HTTP level in real-world deployment settings utilizing intermediary systems such as reverse proxies in front of the web server. We will cover how to identify, exploit, and prevent each of these vulnerabilities.

11.11% 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