Student Transcript

24-04-2025

HTB ACADEMY

Danny Stephens

#1788318

Targets compromised: 68
Ranking: Top 10%

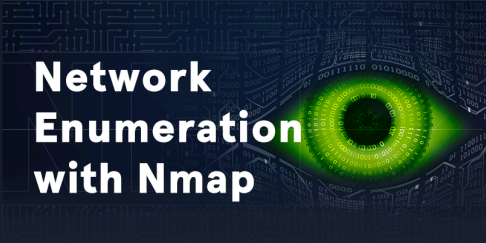| MODULE		PROGRESS

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

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.

100% Completed

File Transfers

10 Sections `Medium` `Offensive`

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.

100% Completed

SQL Injection Fundamentals

17 Sections `Medium` `Offensive`

Databases are an important part of web application infrastructure and SQL (Structured Query Language) to store, retrieve, and manipulate information stored in them. SQL injection is a code injection technique used to take advantage of coding vulnerabilities and inject SQL queries via an application to bypass authentication, retrieve data from the back-end database, or achieve code execution on the underlying server.
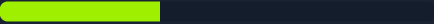
100% Completed

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.

36.36% 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.

100% 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

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.

100% Completed

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

Password Attacks

22 Sections · Medium · Offensive

Passwords are still the primary method of authentication in corporate networks. If strong password policies are not in place, users will often opt for weak, easy-to-remember passwords that can often be cracked offline and used to further our access. We will encounter passwords in many forms during our assessments. We must understand the various ways they are stored, how they can be retrieved, methods to crack weak passwords, ways to use hashes that cannot be cracked, and hunting for weak/default password usage.

13.64% Completed

Web Fuzzing

12 Sections · Easy · Offensive

In this module, we explore the essential techniques and tools for fuzzing web applications, an essential practice in cybersecurity for identifying hidden vulnerabilities and strengthening web application security.

100% Completed

Pentest in a Nutshell

24 Sections · Easy · Offensive

This module focuses on providing a detailed, guided simulation of a real penetration test, emphasizing the fine details of the penetration testing process. It guides you through each step, from reconnaissance to exploitation, mirroring the techniques and methodologies used by professional penetration testers. It offers hands-on experience in a controlled environment and aims to deepen understanding and sharpen skills essential for effective cybersecurity assessments.

100% Completed