

Targets compromised: 104
Ranking: Top 1%

MODULE

PROGRESS

	<div>Introduction to Academy</div> <div>8 Sections Fundamental General</div> <div>This module is recommended for new users. It allows users to become acquainted with the platform and the learning process.</div>	<div>100% Completed</div> <div></div>
	<div>Web Requests</div> <div>8 Sections Fundamental General</div> <div>This module introduces the topic of HTTP web requests and how different web applications utilize them to communicate with their backends.</div>	<div>100% Completed</div> <div></div>
	<div>Attacking Web Applications with Ffuf</div> <div>13 Sections Easy Offensive</div> <div>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.</div>	<div>100% Completed</div> <div></div>
	<div>Using the Metasploit Framework</div> <div>15 Sections Easy Offensive</div> <div>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.</div>	<div>100% 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>100% 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>100% Completed</div> <div></div>
	<div>Penetration Testing Process</div> <div>14 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>



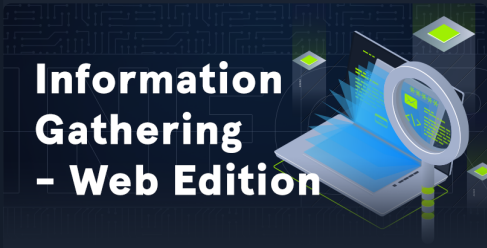
Footprinting

Footprinting

20 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.

100% Completed



Information Gathering - Web Edition

Information Gathering - Web Edition

10 Sections Easy Offensive

This module covers techniques for identifying and analyzing an organization's web application-based attack surface and tech stack. Information gathering is an essential part of any web application penetration test, and it can be performed either passively or actively.

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



File Transfers

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

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



Using Web Proxies

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.

100% Completed



Web Attacks

Web Attacks

18 Sections Medium Offensive

This module covers three common web vulnerabilities, HTTP Verb Tampering, IDOR, and XXE, each of which can have a significant impact on a company's systems. We will cover how to identify, exploit, and prevent each of them through various methods.

100% Completed



SQLMap Essentials

SQLMap Essentials

11 Sections Easy Offensive

The SQLMap Essentials module will teach you the basics of using SQLMap to discover various types of SQL Injection vulnerabilities, all the way to the advanced enumeration of databases to retrieve all data of interest.

100% 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

