


Targets compromised: 90
Ranking: Top 5%

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></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>83.33% Completed</div> <div><div></div></div>
	<div>Login Brute Forcing</div> <div>11 Sections Easy Offensive</div> <div>Learn how to brute force logins for various types of services and create custom wordlists based on your target.</div>	<div>90.91% Completed</div> <div><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></div>
	<div>JavaScript Deobfuscation</div> <div>11 Sections Easy Defensive</div> <div>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.</div>	<div>100% Completed</div> <div><div></div></div>
	<div>Web Attacks</div> <div>18 Sections Medium Offensive</div> <div>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.</div>	<div>22.22% Completed</div> <div><div></div></div>
	<div>Setting Up</div> <div>9 Sections Fundamental General</div> <div>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.</div>	<div>100% Completed</div> <div><div></div></div>




Getting Started

Getting Started

23 Sections Fundamental Offensive

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

30.43% Completed




Cross-Site Scripting (XSS)

Cross-Site Scripting (XSS)

10 Sections Easy Offensive

Cross-Site Scripting (XSS) vulnerabilities are among the most common web application vulnerabilities. An XSS vulnerability may allow an attacker to execute arbitrary JavaScript code within the target's browser and result in complete web application compromise if chained together with other vulnerabilities. This module will teach you how to identify XSS vulnerabilities and exploit them.

40% 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




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.

90.91% Completed




Hacking WordPress

Hacking WordPress

16 Sections Easy Offensive

WordPress is an open-source Content Management System (CMS) that can be used for multiple purposes.

100% Completed




Intro to Network Traffic Analysis

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.

40% Completed




Attacking Web Applications with Ffuf

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



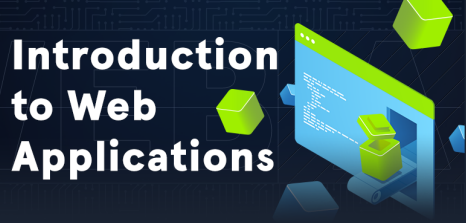
Using Web Proxies

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




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




Command Injections

12 Sections **Medium** **Offensive**

Command injection vulnerabilities can be leveraged to compromise a hosting server and its entire network. This module will teach you how to identify and exploit command injection vulnerabilities and how to use various filter bypassing techniques to avoid security mitigations.

91.67% Completed

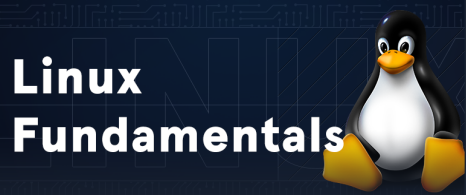


Information Gathering - Web Edition

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.

60% Completed

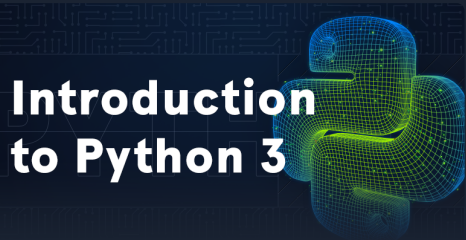


Linux Fundamentals

18 Sections **Fundamental** **General**

This module covers the fundamentals required to work comfortably with the Linux operating system and shell.

88.89% 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.

42.86% Completed

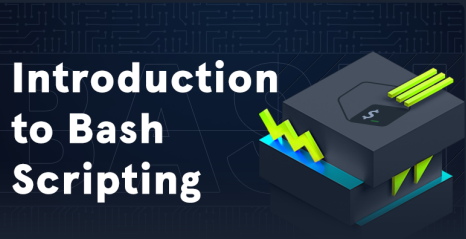


File Inclusion

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.

54.55% Completed

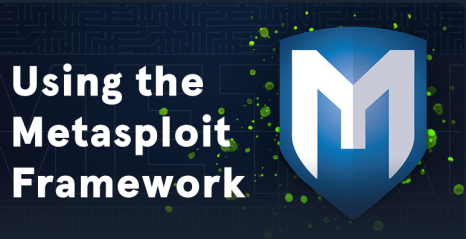


Introduction to Bash Scripting

10 Sections **Easy** **General**

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.

50% 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