

Targets compromised: 213  
Ranking: Top 1%

MODULE

PROGRESS

 <h2>Intro to Academy</h2>	<p>Introduction to Academy 8 Sections <span>Fundamental</span> <span>General</span></p> <p>This module is recommended for new users. It allows users to become acquainted with the platform and the learning process.</p>	<p>100% Completed</p> <div style="width: 100%; background-color: #00ff00; height: 10px;"></div>
 <h2>Network Enumeration with Nmap</h2>	<p>Network Enumeration with Nmap 12 Sections <span>Easy</span> <span>Offensive</span></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>100% Completed</p> <div style="width: 100%; background-color: #00ff00; height: 10px;"></div>
 <h2>File Transfers</h2>	<p>File Transfers 10 Sections <span>Medium</span> <span>Offensive</span></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>100% Completed</p> <div style="width: 100%; background-color: #00ff00; height: 10px;"></div>
 <h2>SQL Injection Fundamentals</h2>	<p>SQL Injection Fundamentals 17 Sections <span>Medium</span> <span>Offensive</span></p> <p>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.</p>	<p>100% Completed</p> <div style="width: 100%; background-color: #00ff00; height: 10px;"></div>
 <h2>File Inclusion</h2>	<p>File Inclusion 11 Sections <span>Medium</span> <span>Offensive</span></p> <p>File Inclusion is a common web application vulnerability, which can be easily overlooked as part of a web application's functionality.</p>	<p>100% Completed</p> <div style="width: 100%; background-color: #00ff00; height: 10px;"></div>
 <h2>Using the Metasploit Framework</h2>	<p>Using the Metasploit Framework 15 Sections <span>Easy</span> <span>Offensive</span></p> <p>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.</p>	<p>100% Completed</p> <div style="width: 100%; background-color: #00ff00; height: 10px;"></div>
 <h2>Attacking Web Applications with Ffuf</h2>	<p>Attacking Web Applications with Ffuf 13 Sections <span>Easy</span> <span>Offensive</span></p> <p>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.</p>	<p>100% Completed</p> <div style="width: 100%; background-color: #00ff00; height: 10px;"></div>



## Login Brute Forcing

### Login Brute Forcing

11 Sections Easy Offensive

Learn how to brute force logins for various types of services and create custom wordlists based on your target.

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



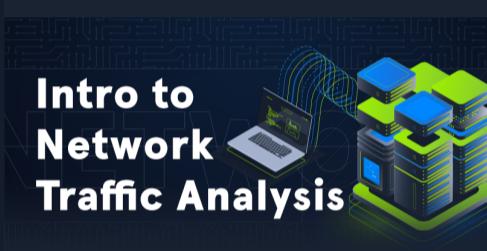
## Getting Started

### Getting Started

23 Sections Fundamental Offensive

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

100% Completed



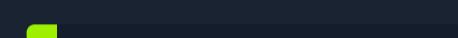
## Intro to Network Traffic Analysis

### 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.

6.67% Completed



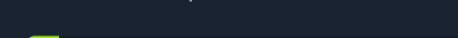
## Introduction to Python 3

### 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.

7.14% 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



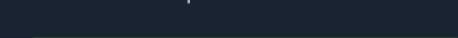
## Cross-Site Scripting (XSS)

### 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.

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



# Command Injections



## 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.

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



# Footprinting



## Footprinting

21 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



# Attacking Common Applications

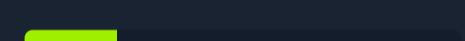


## Attacking Common Applications

33 Sections | Medium | Offensive

Penetration Testers can come across various applications, such as Content Management Systems, custom web applications, internal portals used by developers and sysadmins, and more. It's common to find the same applications across many different environments. While an application may not be vulnerable in one environment, it may be misconfigured or unpatched in the next. It is important as an assessor to have a firm grasp of enumerating and attacking the common applications discussed in this module. This knowledge will help when encountering other types of applications during assessments.

21.21% Completed



# Shells & Payloads



## 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



# Attacking Common Services



## Attacking Common Services

19 Sections | Medium | Offensive

Organizations regularly use a standard set of services for different purposes. It is vital to conduct penetration testing activities on each service internally and externally to ensure that they are not introducing security threats. This module will cover how to enumerate each service and test it against known vulnerabilities and exploits with a standard set of tools.

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



# 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



# File Upload Attacks

## 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.

100% Completed



# Active Directory Enumeration & Attacks

## Active Directory Enumeration & Attacks

36 Sections | Medium | Offensive

Active Directory (AD) is the leading enterprise domain management suite, providing identity and access management, centralized domain administration, authentication, and much more. Due to the many features and complexity of AD, it presents a large attack surface that is difficult to secure properly. To be successful as infosec professionals, we must understand AD architectures and how to secure our enterprise environments. As Penetration testers, having a firm grasp of what tools, techniques, and procedures are available to us for enumerating and attacking AD environments and commonly seen AD misconfigurations is a must.

100% Completed



# Password Attacks

## 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.

100% Completed



# Pivoting, Tunneling, and Port Forwarding

## Pivoting, Tunneling, and Port Forwarding

18 Sections | Medium | Offensive

Once a foothold is gained during an assessment, it may be in scope to move laterally and vertically within a target network. Using one compromised machine to access another is called pivoting and allows us to access networks and resources that are not directly accessible to us through the compromised host. Port forwarding accepts the traffic on a given IP address and port and redirects it to a different IP address and port combination. Tunneling is a technique that allows us to encapsulate traffic within another protocol so that it looks like a benign traffic stream.

100% Completed

