

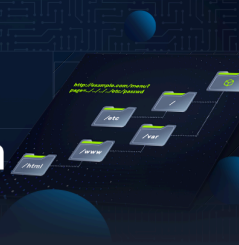
Targets compromised: 229  
Ranking: Top 1%

MODULE

PROGRESS

 <h2>Intro to Academy</h2>	<h3>Intro to Academy</h3> <p>8 Sections <b>Fundamental</b> <b>General</b></p> <p>Your first stop in Hack The Box Academy to become acquainted with the platform, its features, and its learning process.</p>	<p>100% Completed</p> <div><div style="width: 100%;"></div></div>
 <h2>Hacking WordPress</h2>	<h3>Hacking WordPress</h3> <p>16 Sections <b>Easy</b> <b>Offensive</b></p> <p>WordPress is an open-source Content Management System (CMS) that can be used for multiple purposes.</p>	<p>100% Completed</p> <div><div style="width: 100%;"></div></div>
 <h2>Learning Process</h2>	<h3>Learning Process</h3> <p>20 Sections <b>Fundamental</b> <b>General</b></p> <p>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.</p>	<p>20% Completed</p> <div><div style="width: 20%;"></div></div>
 <h2>Linux Fundamentals</h2>	<h3>Linux Fundamentals</h3> <p>30 Sections <b>Fundamental</b> <b>General</b></p> <p>This module covers the fundamentals required to work comfortably with the Linux operating system and shell.</p>	<p>100% Completed</p> <div><div style="width: 100%;"></div></div>
 <h2>Network Enumeration with Nmap</h2>	<h3>Network Enumeration with Nmap</h3> <p>12 Sections <b>Easy</b> <b>Offensive</b></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><div style="width: 100%;"></div></div>
 <h2>File Transfers</h2>	<h3>File Transfers</h3> <p>10 Sections <b>Medium</b> <b>Offensive</b></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><div style="width: 100%;"></div></div>
 <h2>SQL Injection Fundamentals</h2>	<h3>SQL Injection Fundamentals</h3> <p>17 Sections <b>Medium</b> <b>Offensive</b></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><div style="width: 100%;"></div></div>

## File Inclusion



### 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.

100% Completed



## Using the Metasploit Framework



### 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



### 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



## Linux Privilege Escalation



### Linux Privilege Escalation

28 Sections **Easy** **Offensive**

Privilege escalation is a crucial phase during any security assessment. During this phase, we attempt to gain access to additional users, hosts, and resources to move closer to the assessment's overall goal. There are many ways to escalate privileges. This module aims to cover the most common methods emphasizing real-world misconfigurations and flaws that we may encounter in a client environment. The techniques covered in this module are not an exhaustive list of all possibilities and aim to avoid extreme "edge-case" tactics that may be seen in a Capture the Flag (CTF) exercise.

100% 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



## Login Brute Forcing



### Login Brute Forcing

13 Sections **Easy** **Offensive**

The module contains an exploration of brute-forcing techniques, including the use of tools like Hydra and Medusa, and the importance of strong password practices. It covers various attack scenarios, such as targeting SSH, FTP, and web login forms.

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



## Windows Privilege Escalation

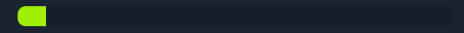


### Windows Privilege Escalation

33 Sections **Medium** **Offensive**

After gaining a foothold, elevating our privileges will provide more options for persistence and may reveal information stored locally that can further our access in the environment. Enumeration is the key to privilege escalation. When you gain initial shell access to the host, it is important to gain situational awareness and uncover details relating to the OS version, patch level, any installed software, our current privileges, group memberships, and more. Windows presents an enormous attack surface and, being that most companies run Windows hosts in some way, we will more often than not find ourselves gaining access to Windows machines during our assessments. This covers common methods while emphasizing real-world misconfigurations and flaws that we may encounter during an assessment. There are many additional "edge-case" possibilities not covered in this module. We will cover both modern and legacy Windows Server and Desktop versions that may be present in a client environment.

6.06% 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



## 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.

100% 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

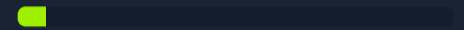


### Attacking Common Applications

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.

6.06% 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

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.

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



## 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.

94.44% Completed

