


Targets compromised: 93  
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>Linux Fundamentals</div> <div>30 Sections Fundamental General</div> <div>This module covers the fundamentals required to work comfortably with the Linux operating system and shell.</div>  | <div>46.67% Completed</div> <div></div> |
|  | <div>Cracking Passwords with Hashcat</div> <div>14 Sections Medium Offensive</div> <div>This module covers the fundamentals of password cracking using the Hashcat tool.</div>   | <div>7.14% Completed</div> <div></div>  |
|  | <div>File Transfers</div> <div>10 Sections Medium Offensive</div> <div>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.</div>   | <div>100% Completed</div> <div></div>   |
|  | <div>SQL Injection Fundamentals</div> <div>17 Sections Medium Offensive</div> <div>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.</div>   | <div>100% Completed</div> <div></div>   |
|  | <div>OSINT: Corporate Recon</div> <div>23 Sections Hard Offensive</div> <div>OSINT (Open-source Intelligence) is a crucial stage of the penetration testing process. A thorough examination of publicly available information can increase the chances of finding a vulnerable system, gaining valid credentials through password spraying, or gaining a foothold via social engineering. There is a vast amount of publicly available information from which relevant information needs to be selected.</div>   | <div>100% Completed</div> <div></div>   |
|  | <div>Introduction to Networking</div> <div>21 Sections Fundamental General</div> <div>As an information security professional, a firm grasp of networking fundamentals and the required components is necessary. Without a strong foundation in networking, it will be tough to progress in any area of information security. Understanding how a network is structured and how the communication between the individual hosts and servers takes place using the various protocols allows us to understand the entire network structure and its network traffic in detail and how different communication standards are handled. This knowledge is essential to create our tools and to interact with the protocols.</div> | <div>100% Completed</div> <div></div>   |




## 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




## 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

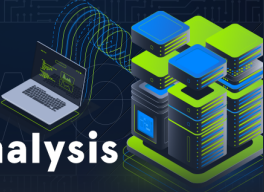


## Login Brute Forcing

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




## 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.

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




## 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




## 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



## Blind SQL Injection

16 Sections Hard Offensive

In this module, we cover blind SQL injection attacks and MSSQL-specific attacks.

100% Completed



## Game Hacking Fundamentals

### Game Hacking Fundamentals

12 Sections Medium Offensive

This module serves as an introduction to fundamental Game Hacking concepts. You will learn how to find and change memory values in a running game as well as explore other tools and techniques.

100% Completed



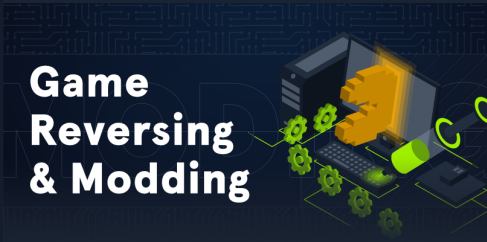
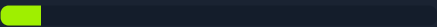
## Security Monitoring & SIEM Fundamentals

### Security Monitoring & SIEM Fundamentals

11 Sections Easy Defensive

This module provides a concise yet comprehensive overview of Security Information and Event Management (SIEM) and the Elastic Stack. It demystifies the essential workings of a Security Operation Center (SOC), explores the application of the MITRE ATT&CK framework within SOCs, and introduces SIEM (KQL) query development. With a focus on practical skills, students will learn how to develop SIEM use cases and visualizations using the Elastic Stack.

9.09% Completed



## Game Reversing & Modding

### Game Reversing & Modding

20 Sections Medium Offensive

This module serves as a follow-up to the Game Hacking Fundamentals module. You will learn how to persist Cheat Engine Scripts by scanning for byte arrays, editing game assemblies, utilising runtime hooking to modify games, and tampering with game network traffic using Burp.

100% Completed



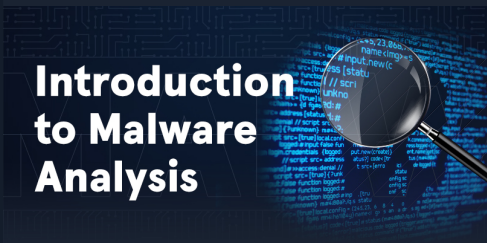
## Brief Intro to Hardware Attacks

### Brief Intro to Hardware Attacks

8 Sections Medium General

This mini-module concisely introduces hardware attacks, covering Bluetooth risks and attacks, Cryptanalysis Side-Channel Attacks, and vulnerabilities like Spectre and Meltdown. It delves into both historical and modern Bluetooth hacking techniques, explores the principles of cryptanalysis and different side-channel attacks, and outlines microprocessor design, optimisation strategies and vulnerabilities, such as Spectre and Meltdown.

100% Completed



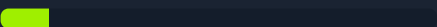
## Introduction to Malware Analysis

### Introduction to Malware Analysis

9 Sections Hard Defensive

This module offers an exploration of malware analysis, specifically targeting Windows-based threats. The module covers Static Analysis utilizing Linux and Windows tools, Malware Unpacking, Dynamic Analysis (including malware traffic analysis), Reverse Engineering for Code Analysis, and Debugging using x64dbg. Real-world malware examples such as WannaCry, DoomJuice, Brbbot, Dharma, and Meterpreter are analyzed to provide practical experience.

11.11% Completed



## Introduction to Binary Fuzzing

### Introduction to Binary Fuzzing

20 Sections Hard Offensive

Fuzzing is a powerful software testing technique that deliberately introduces chaos into your applications. By bombarding your code with unexpected or malformed inputs, fuzzing reveals hidden bugs and security vulnerabilities that might otherwise go unnoticed. This module will explore the history, theory, and practical applications of fuzzing, teaching you how to use this technique to find critical issues in software.

60% Completed

