

Paths completed: 1
Targets compromised: 72
Ranking: Top 5%

PATHS COMPLETED

PROGRESS



Operating System Fundamentals

2 Modules **Easy**

To succeed in information security, we must have a deep understanding of the Windows and Linux operating systems and be comfortable navigating the command line on both as a "power user." Much of our time in any role, but especially penetration testing, is spent in a Linux shell, Windows cmd or PowerShell console, so we must have the skills to navigate both types of operating systems with ease, manage system services, install applications, manage permissions, and harden the systems we work from in accordance with security best practices.

100% Completed



MODULE

PROGRESS



Introduction to Academy

8 Sections **Fundamental** **General**

This module is recommended for new users. It allows users to become acquainted with the platform and the learning process.

100% Completed

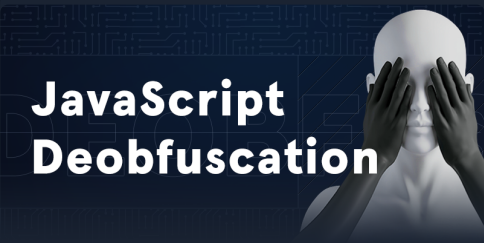


Web Requests

8 Sections **Fundamental** **General**

This module introduces the topic of HTTP web requests and how different web applications utilize them to communicate with their backends.

100% Completed



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



Stack-Based Buffer Overflows on Linux x86

13 Sections **Medium** **Offensive**

Buffer overflows are common vulnerabilities in software applications that can be exploited to achieve remote code execution (RCE) or perform a Denial-of-Service (DoS) attack. These vulnerabilities are caused by insecure coding, resulting in an attacker being able to overrun a program's buffer and overwrite adjacent memory locations, changing the program's execution path and resulting in unintended actions.

84.62% Completed



Linux Fundamentals

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

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

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

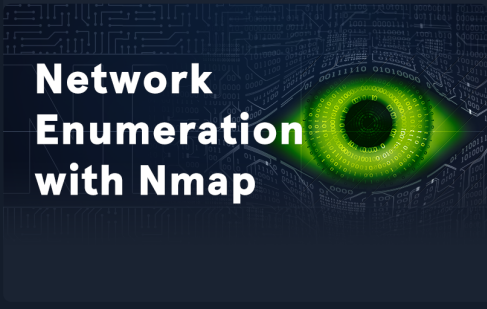
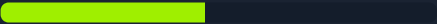


SQL Injection Fundamentals

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.

47.06% Completed



Network Enumeration with Nmap

12 Sections Easy Offensive

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.

100% Completed



Cracking Passwords with Hashcat

14 Sections Medium Offensive

This module covers the fundamentals of password cracking using the Hashcat tool.

85.71% Completed



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.

80% 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.

72.73% Completed



Learning Process

12 Sections Fundamental General

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.

100% Completed




Introduction to Networking

12 Sections Fundamental General

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.

100% 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.

10% Completed




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.

45.45% 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.

100% Completed

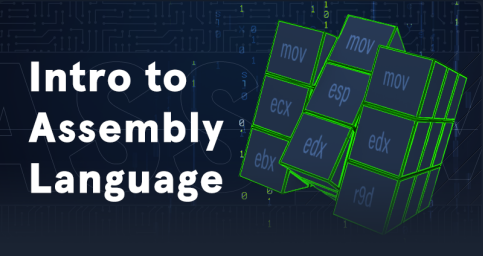


Intro to Network Traffic Analysis

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.

60% Completed




Intro to Assembly Language

24 Sections Medium General

This module builds the core foundation for Binary Exploitation by teaching Computer Architecture and Assembly language basics.

41.67% Completed




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.

84.62% Completed




Hacking WordPress

16 Sections Easy Offensive

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

93.75% Completed



Windows Fundamentals

14 Sections Fundamental General

This module covers the fundamentals required to work comfortably with the Windows operating system.

100% Completed



Introduction to Active Directory

16 Sections Fundamental General

Active Directory (AD) is present in the majority of corporate environments. Due to its many features and complexity, it presents a vast attack surface. To be successful as penetration testers and information security professionals, we must have a firm understanding of Active Directory fundamentals, AD structures, functionality, common AD flaws, misconfigurations, and defensive measures.

100% Completed

