


Paths completed: 1  
Targets compromised: 44  
Ranking: Top 5%

PATHS COMPLETED

PROGRESS



### Operating System Fundamentals

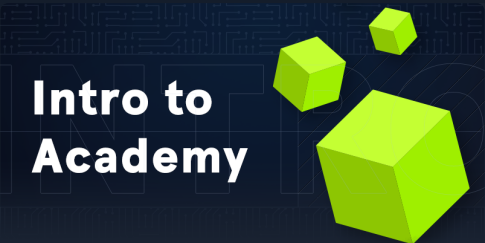
2 Modules **Easy**

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




### Intro 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




### Learning Process

20 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

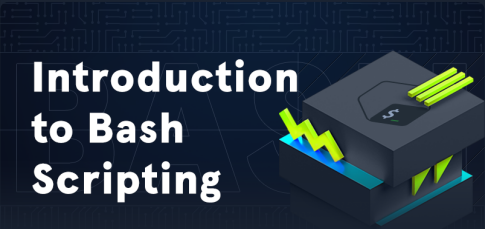


### Linux Fundamentals

30 Sections **Fundamental** **General**

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

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.

100% Completed


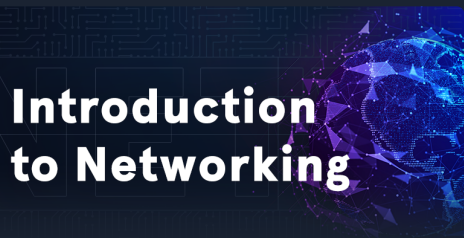
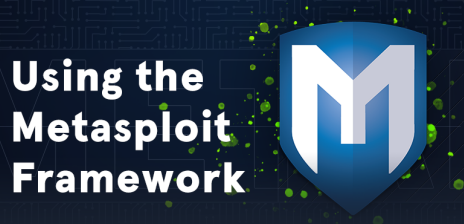




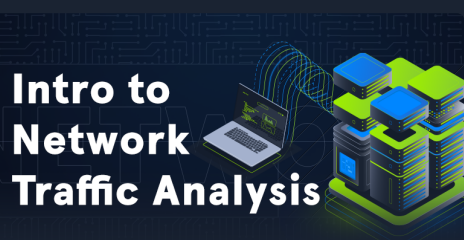


### Web Requests

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

	<h3>File Inclusion</h3> <div>11 Sections <span>Medium</span> <span>Offensive</span></div> <p>File Inclusion is a common web application vulnerability, which can be easily overlooked as part of a web application's functionality.</p>	9.09% Completed <div></div>
	<h3>Introduction to Networking</h3> <div>21 Sections <span>Fundamental</span> <span>General</span></div> <p>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.</p>	100% Completed <div></div>
	<h3>Using the Metasploit Framework</h3> <div>15 Sections <span>Easy</span> <span>Offensive</span></div> <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>	100% Completed <div></div>
	<h3>Windows Fundamentals</h3> <div>14 Sections <span>Fundamental</span> <span>General</span></div> <p>This module covers the fundamentals required to work comfortably with the Windows operating system.</p>	100% Completed <div></div>
	<h3>Attacking Web Applications with Ffuf</h3> <div>13 Sections <span>Easy</span> <span>Offensive</span></div> <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>	100% Completed <div></div>
	<h3>Introduction to Active Directory</h3> <div>16 Sections <span>Fundamental</span> <span>General</span></div> <p>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.</p>	100% Completed <div></div>
	<h3>Introduction to Web Applications</h3> <div>17 Sections <span>Fundamental</span> <span>General</span></div> <p>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.</p>	100% Completed <div></div>
	<h3>Intro to Network Traffic Analysis</h3> <div>15 Sections <span>Medium</span> <span>General</span></div> <p>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.</p>	100% Completed <div></div>



Setting Up

- 9 Sections
- Fundamental
- General

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.

100% Completed

