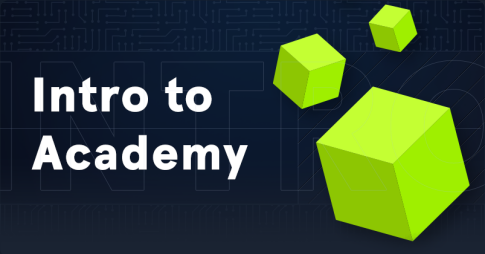



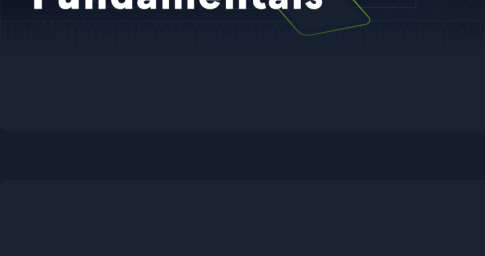
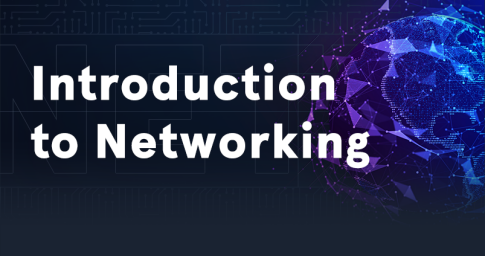


Targets compromised: 24
Ranking: Top 10%

MODULE

PROGRESS

	<div>Introduction to Academy</div> <div>8 Sections Fundamental General</div> <p>This module is recommended for new users. It allows users to become acquainted with the platform and the learning process.</p>	<div>100% Completed</div> <div></div>
	<div>Linux Fundamentals</div> <div>30 Sections Fundamental General</div> <p>This module covers the fundamentals required to work comfortably with the Linux operating system and shell.</p>	<div>33.33% Completed</div> <div></div>
	<div>File Transfers</div> <div>10 Sections Medium Offensive</div> <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>	<div>10% Completed</div> <div></div>
	<div>SQL Injection Fundamentals</div> <div>17 Sections Medium Offensive</div> <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>	<div>100% Completed</div> <div></div>
	<div>Introduction to Networking</div> <div>21 Sections Fundamental General</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>	<div>100% Completed</div> <div></div>
	<div>Using the Metasploit Framework</div> <div>15 Sections Easy Offensive</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>	<div>100% Completed</div> <div></div>



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

