

Paths completed: 4

Targets compromised: 206

Ranking: Top 1%

PATHS COMPLETED


PROGRESS

	<div>Bug Bounty Hunter</div> <div>20 Modules Medium</div> <p>The Bug Bounty Hunter Job Role Path is for individuals who want to enter the world of Bug Bounty Hunting with little to no prior experience. This path covers core web application security assessment and bug bounty hunting concepts and provides a deep understanding of the attack tactics used during bug bounty hunting. Armed with the necessary theoretical background, multiple practical exercises, and a proven bug bounty hunting methodology, students will go through all bug bounty hunting stages, from reconnaissance and bug identification to exploitation, documentation, and communication to vendors/programs. Upon completing this job role path, you will have become proficient in the most common bug bounty hunting and attack techniques against web applications and be in the position of professionally reporting bugs to a vendor.</p>	<div>100% Completed</div> <div></div>
	<div>Operating System Fundamentals</div> <div>2 Modules Easy</div> <p>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.</p>	<div>100% Completed</div> <div></div>
	<div>Information Security Foundations</div> <div>12 Modules Easy</div> <p>Information Security is a field with many specialized and highly technical disciplines. Job roles like Penetration Tester & Information Security Analyst require a solid technical foundational understanding of core IT & Information Security topics. This skill path is made up of modules that will assist learners in developing &/or strengthening a foundational understanding before proceeding with learning the more complex security topics. Every long-standing building first needs a solid foundation. Welcome to Information Security Foundations.</p>	<div>100% Completed</div> <div></div>
	<div>Cracking into Hack the Box</div> <div>3 Modules Easy</div> <p>To be successful in any technical information security role, we must have a broad understanding of specialized tools, tactics, and terminology. This path introduces core concepts necessary for anyone interested in a hands-on technical infosec role. The modules also provide the essential prerequisite knowledge for joining the main Hack The Box platform, progressing through Starting Point through easy-rated retired machines, and solving "live" machines with no walkthrough. It also includes helpful information about staying organized, navigating the HTB platforms, common pitfalls, and selecting a penetration testing distribution. Students will complete their first box during this path with a guided walkthrough and be challenged to complete a box on their own by applying the knowledge learned in the Getting Started module.</p>	<div>100% Completed</div> <div></div>

MODULE

PROGRESS

 <h2>Intro to Academy</h2>	<h3>Introduction to Academy</h3> <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>	100% Completed <div></div>
 <h2>Web Requests</h2>	<h3>Web Requests</h3> <div> 8 Sections Fundamental General </div> <p>This module introduces the topic of HTTP web requests and how different web applications utilize them to communicate with their backends.</p>	100% Completed <div></div>
 <h2>Introduction to Web Applications</h2>	<h3>Introduction to Web Applications</h3> <div> 17 Sections Fundamental General </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>
 <h2>Using Web Proxies</h2>	<h3>Using Web Proxies</h3> <div> 15 Sections Easy Offensive </div> <p>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.</p>	100% Completed <div></div>
 <h2>Information Gathering - Web Edition</h2>	<h3>Information Gathering - Web Edition</h3> <div> 10 Sections Easy Offensive </div> <p>This module covers techniques for identifying and analyzing an organization's web application-based attack surface and tech stack. Information gathering is an essential part of any web application penetration test, and it can be performed either passively or actively.</p>	100% Completed <div></div>
 <h2>Attacking Web Applications with Ffuf</h2>	<h3>Attacking Web Applications with Ffuf</h3> <div> 13 Sections Easy Offensive </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>
 <h2>JavaScript Deobfuscation</h2>	<h3>JavaScript Deobfuscation</h3> <div> 11 Sections Easy Defensive </div> <p>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.</p>	100% Completed <div></div>
 <h2>Cross-Site Scripting (XSS)</h2>	<h3>Cross-Site Scripting (XSS)</h3> <div> 10 Sections Easy Offensive </div> <p>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.</p>	100% Completed <div></div>
 <h2>SQL Injection Fundamentals</h2>	<h3>SQL Injection Fundamentals</h3> <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>	100% Completed <div></div>




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




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




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




Server-side Attacks

Server-side Attacks

19 Sections Medium Offensive

A backend that handles user-supplied input insecurely can lead to sensitive information disclosure and remote code execution. This module covers how to identify and exploit server-side bugs. This module introduces Server-Side Request Forgery (SSRF), Server-Side Template Injection (SSTI), and Server-Side Includes (SSI) injection attacks, alongside other server-side vulnerabilities.

100% Completed




Login Brute Forcing

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




Broken Authentication

Broken Authentication

14 Sections Medium Offensive

Authentication is probably the most straightforward and prevalent measure used to secure access to resources, and it's the first line of defense against unauthorized access. Broken authentication is currently listed as #7 on the 2021 OWASP Top 10 Web Application Security Risks, falling under the broader category of Identification and Authentication failures. A vulnerability or misconfiguration at the authentication stage can devastatingly impact an application's overall security.

100% Completed




Learning Process

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



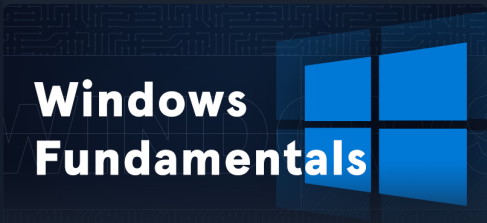
Linux Fundamentals

Linux Fundamentals

18 Sections Fundamental General

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

100% Completed



Windows Fundamentals

14 Sections Fundamental General

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

100% Completed

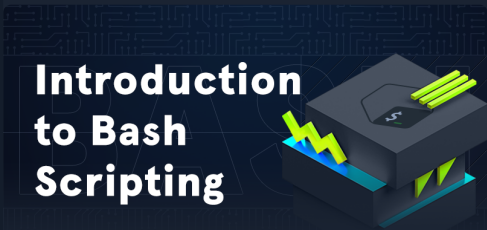


Setting Up

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

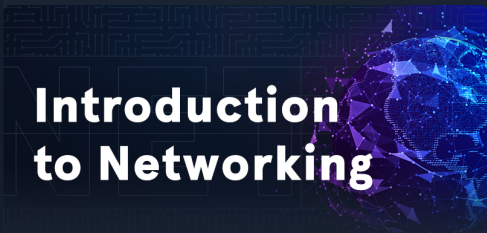


Introduction to Bash Scripting

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

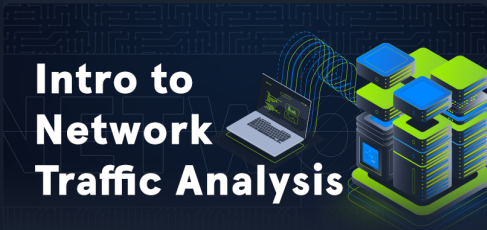


Introduction to Networking

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



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



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



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





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



Session Security

Session Security

14 Sections Medium Offensive

Maintaining and keeping track of a user's session is an integral part of web applications. It is an area that requires extensive testing to ensure it is set up robustly and securely. This module covers the most common attacks and vulnerabilities that can affect web application sessions, such as Session Hijacking, Session Fixation, Cross-Site Request Forgery, Cross-Site Scripting, and Open Redirects.

100% Completed



Web Service & API Attacks

Web Service & API Attacks

13 Sections Medium Offensive

Web services and APIs are frequently exposed to provide certain functionalities in a programmatic way between heterogeneous devices and software components. Both web services and APIs can assist in integrating different applications or facilitate separation within a given application. This module covers how to identify the functionality a web service or API offers and exploit any security-related inefficiencies.

100% Completed



Hacking WordPress

Hacking WordPress

16 Sections Easy Offensive

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

100% Completed



Bug Bounty Hunting Process

Bug Bounty Hunting Process

6 Sections Easy General

Bug bounty programs encourage security researchers to identify bugs and submit vulnerability reports. Getting into the world of bug bounty hunting without any prior experience can be a daunting task, though. This module covers the bug bounty hunting process to help you start bug bounty hunting in an organized and well-structured way. It's all about effectiveness and professionally communicating your findings.

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.

93.33% Completed



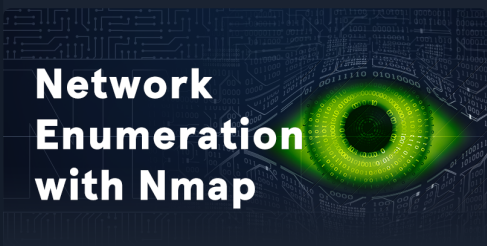
Getting Started

Getting Started

23 Sections Fundamental Offensive

This module covers the fundamentals of penetration testing and an introduction to Hack The Box.

100% Completed



Network Enumeration with Nmap

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





Footprinting

20 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



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



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.

20% Completed

