


Paths completed: 1
Targets compromised: 145
Ranking: Top 5%

PATHS COMPLETED

PROGRESS



Information Security Foundations


12 Modules Easy

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.

100% Completed

MODULE

PROGRESS




Intro to Academy

8 Sections Fundamental General

Your first stop in Hack The Box Academy to become acquainted with the platform, its features, and its learning process.

100% Completed




Hacking WordPress

16 Sections Easy Offensive

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

12.5% 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

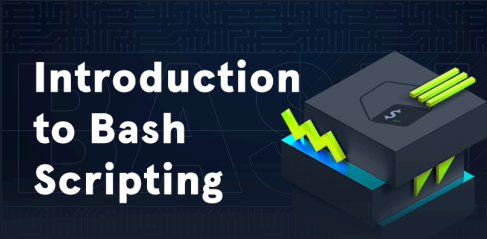


Linux Fundamentals

30 Sections Fundamental General

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

100% Completed





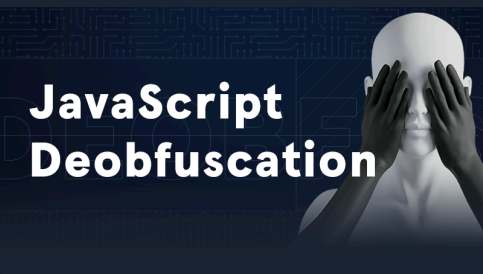






Introduction to Bash Scripting

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

	<h3>SQL Injection Fundamentals</h3> <div>17 SectionsMediumOffensive</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>
	<h3>Web Requests</h3> <div>8 SectionsFundamentalGeneral</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>
	<h3>File Inclusion</h3> <div>11 SectionsMediumOffensive</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 SectionsFundamentalGeneral</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>JavaScript Deobfuscation</h3> <div>11 SectionsEasyDefensive</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>
	<h3>Windows Fundamentals</h3> <div>14 SectionsFundamentalGeneral</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 SectionsEasyOffensive</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>Login Brute Forcing</h3> <div>13 SectionsEasyOffensive</div> <p>The module contains an exploration of brute-forcing techniques, including the use of tools like Hydra and Medusa, and the importance of strong password practices. It covers various attack scenarios, such as targeting SSH, FTP, and web login forms.</p>	84.62% Completed <div></div>




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




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




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




Getting Started

23 Sections Fundamental Offensive

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

78.26% Completed



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 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 impact an application's overall security.

64.29% 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




Setting Up

22 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.

40.91% Completed



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.

100% Completed



Cross-Site Scripting (XSS)

10 Sections **Easy** **Offensive**

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.

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



Using Web Proxies

15 Sections **Easy** **Offensive**

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.

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.

44.44% Completed



Information Gathering - Web Edition

19 Sections **Easy** **Offensive**

This module equips learners with essential web reconnaissance skills, crucial for ethical hacking and penetration testing. It explores both active and passive techniques, including DNS enumeration, web crawling, analysis of web archives and HTTP headers, and fingerprinting web technologies.

63.16% 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



Server-side Attacks

19 Sections **Medium** **Offensive**

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

100% Completed



Incident Handling Process

9 Sections **Fundamental** **General**

Security Incident handling has become a vital part of each organization's defensive strategy, as attacks constantly evolve and successful compromises are becoming a daily occurrence. In this module, we will review the process of handling an incident from the very early stage of detecting a suspicious event, to confirming a compromise and responding to it.

100% Completed

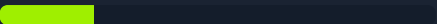


Session Security

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.

21.43% Completed

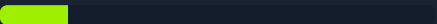


Web Service & API Attacks

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.

15.38% Completed



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



Introduction to Windows Command Line

23 Sections Easy General

As administrators and Pentesters, we may not always be able to utilize a graphical user interface for the actions we need to perform. Introduction to Windows Command Line aims to introduce students to the wide range of uses for Command Prompt and PowerShell within a Windows environment. We will cover basic usage of both key executables for administration, useful PowerShell cmdlets and modules, and different ways to leverage these tools to our benefit.

100% Completed



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

