Paths completed: 1
Targets compromised: 153
Ranking: Top 5%

PATHS COMPLETED

PROGRESS

Cracking into Hack the Box

`3 Modules` `Easy`

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.

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.
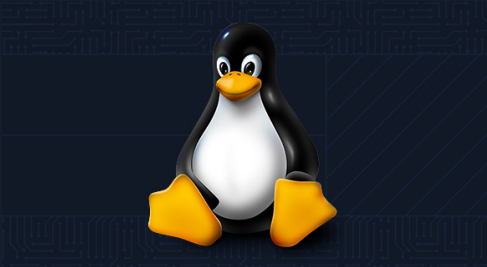
100% Completed

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

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.
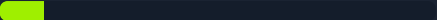
100% Completed

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.
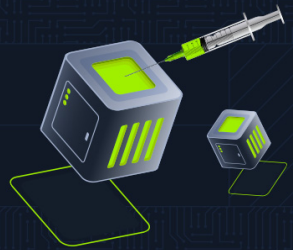
10% Completed

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.
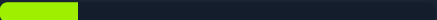
100% Completed

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.

17.65% 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

Introduction to Networking

21 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

Using the Metasploit Framework

15 Sections   Easy   Offensive

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.

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

Windows Fundamentals

14 Sections   Fundamental   General

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

100% 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.

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.

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.
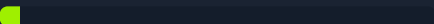
100% Completed

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.

4.55% 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

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

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

Footprinting

21 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

Shells & Payloads

17 Sections | Medium | Offensive

Gain the knowledge and skills to identify and use shells & payloads to establish a foothold on vulnerable Windows & Linux systems. This module utilizes a fictitious scenario where the learner will place themselves in the perspective of a sysadmin trying out for a position on CAT5 Security's network penetration testing team.

100% Completed

Attacking Common Services

19 Sections | Medium | Offensive

Organizations regularly use a standard set of services for different purposes. It is vital to conduct penetration testing activities on each service internally and externally to ensure that they are not introducing security threats. This module will cover how to enumerate each service and test it against known vulnerabilities and exploits with a standard set of tools.

84.21% 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.

100% Completed

Password Attacks

26 Sections | Medium | Offensive

Passwords are still the primary method of authentication in corporate networks. If strong password policies are not enforced, users often choose weak, easy-to-remember passwords that can be cracked offline and leveraged to escalate access. As penetration testers, we encounter passwords in many forms during our assessments. It's essential to understand how passwords are stored, how they can be retrieved, methods for cracking weak passwords, techniques for using hashes that cannot be cracked, and how to identify weak or default password usage.

84.62% Completed

Incident Handling Process

11 Sections | Easy | General

Security Incident handling has become a vital part of every 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.
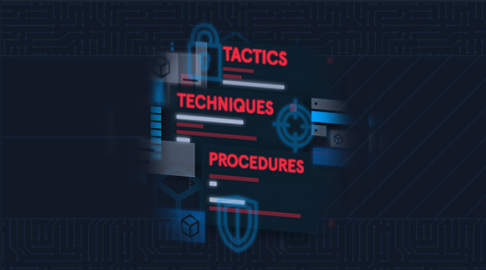
100% Completed

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.

100% Completed

Introduction to Threat Hunting & Hunting With Elastic

`6 Sections` `Medium` `Defensive`

This module initially lays the groundwork for understanding Threat Hunting, ranging from its basic definition, to the structure of a threat hunting team. The module also dives into the threat hunting process, highlighting the interrelationships between threat hunting, risk assessment, and incident handling. Furthermore, the module elucidates the fundamentals of Cyber Threat Intelligence (CTI). It expands on the different types of threat intelligence and offers guidance on effectively interpreting a threat intelligence report. Finally, the module puts theory into practice, showcasing how to conduct threat hunting using the Elastic stack. This practical segment uses real-world logs to provide learners with hands-on experience.
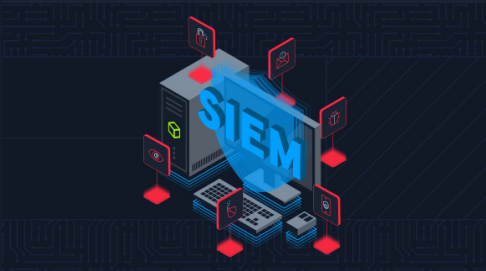
100% Completed

Windows Event Logs & Finding Evil

`6 Sections` `Medium` `Defensive`

This module covers the exploration of Windows Event Logs and their significance in uncovering suspicious activities. Throughout the course, we delve into the anatomy of Windows Event Logs and highlight the logs that hold the most valuable information for investigations. The module also focuses on utilizing Sysmon and Event Logs for detecting and analyzing malicious behavior. Additionally, we delve into Event Tracing for Windows (ETW), explaining its architecture and components, and provide ETW-based detection examples. To streamline the analysis process, we introduce the powerful Get-WinEvent cmdlet.

100% Completed

Understanding Log Sources & Investigating with Splunk

`6 Sections` `Medium` `Defensive`

This module provides a comprehensive introduction to Splunk, focusing on its architecture and the creation of effective detection-related SPL (Search Processing Language) searches. We will learn to investigate with Splunk as a SIEM tool and develop TTP-driven and analytics-driven SPL searches for enhanced threat detection and response. Through hands-on exercises, we will learn to identify and understand the ingested data and available fields within Splunk. We will also gain practical experience in leveraging Splunk's powerful features for security monitoring and incident investigation.

33.33% Completed