




Paths completed: 3

Targets compromised: 157

Ranking: Top 5%


PATHS COMPLETED

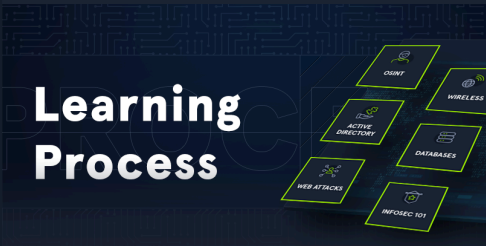
PROGRESS

<div><div><div>Basic Toolset</div><div></div></div></div>	<div>Basic Toolset</div> <div><div>7 Modules</div><div>Medium</div></div> <div>In this path, modules cover the basic tools needed to be successful in network and web application penetration testing. This is not an exhaustive listing of all tools (both open source and commercial) available to us as security practitioners but covers tried and true tools that we find ourselves using on every technical assessment that we perform. Learning how to use the basic toolset is essential, as many different tools are used in penetration testing. We need to understand which of them to use for the various situations we will come across.</div>	<div>100% Completed</div> <div></div>
<div><div><div>Cracking Into HTB</div><div></div></div></div>	<div>Cracking into Hack the Box</div> <div><div>3 Modules</div><div>Easy</div></div> <div>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.</div>	<div>100% Completed</div> <div></div>
<div><div><div>Operating System Fundamentals</div><div></div></div></div>	<div>Operating System Fundamentals</div> <div><div>4 Modules</div><div>Easy</div></div> <div>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.</div>	<div>100% Completed</div> <div></div>

MODULE

PROGRESS

<div><div><div>Intro to Academy</div><div></div></div></div>	<div>Intro to Academy</div> <div><div>8 Sections</div><div>Fundamental</div><div>General</div></div> <div>Your first stop in Hack The Box Academy to become acquainted with the platform, its features, and its learning process.</div>	<div>100% Completed</div> <div></div>
---	---	---------------------------------------



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

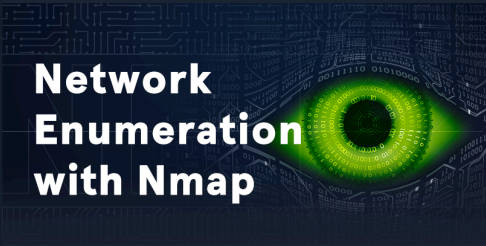


Linux Fundamentals

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



Cracking Passwords with Hashcat

14 Sections Medium Offensive

This module covers the fundamentals of password cracking using the Hashcat tool.

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.

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.

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



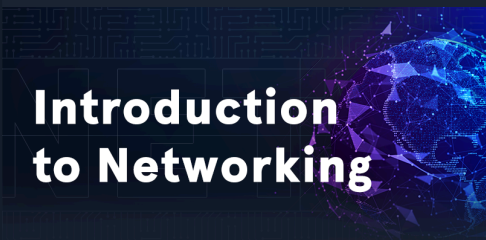
File Inclusion

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





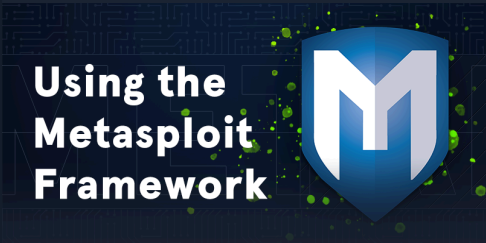
Introduction to Networking

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

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



Stack-Based Buffer Overflows on Linux x86

Stack-Based Buffer Overflows on Linux x86

13 Sections Medium Offensive

Buffer overflows are common vulnerabilities in software applications that can be exploited to achieve remote code execution (RCE) or perform a Denial-of-Service (DoS) attack. These vulnerabilities are caused by insecure coding, resulting in an attacker being able to overrun a program's buffer and overwrite adjacent memory locations, changing the program's execution path and resulting in unintended actions.

100% Completed



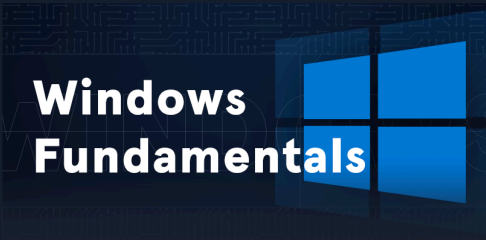
JavaScript Deobfuscation

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



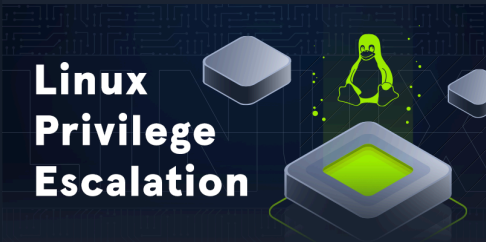
Windows Fundamentals

Windows Fundamentals

14 Sections Fundamental General

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

100% Completed



Linux Privilege Escalation

Linux Privilege Escalation

28 Sections Easy Offensive

Privilege escalation is a crucial phase during any security assessment. During this phase, we attempt to gain access to additional users, hosts, and resources to move closer to the assessment's overall goal. There are many ways to escalate privileges. This module aims to cover the most common methods emphasizing real-world misconfigurations and flaws that we may encounter in a client environment. The techniques covered in this module are not an exhaustive list of all possibilities and aim to avoid extreme "edge-case" tactics that may be seen in a Capture the Flag (CTF) exercise.

100% Completed



Attacking Web Applications with Ffuf

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



Login Brute Forcing


Login Brute Forcing

13 Sections Easy Offensive

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.

84.62% Completed






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.

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.

40.91% Completed



Introduction to Python 3

14 Sections **Easy** **General**

Automating tedious or otherwise impossible tasks is highly valued during both penetration testing engagements and everyday life. Introduction to Python 3 aims to introduce the student to the world of scripting with Python 3 and covers the essential building blocks needed for a beginner to understand programming. Some advanced topics are also covered for the more experienced student. In a guided fashion and starting soft, the final goal of this module is to equip the reader with enough know-how to be able to implement simple yet useful pieces of software.

100% Completed



Stack-Based Buffer Overflows on Windows x86

11 Sections **Medium** **Offensive**

This module is your first step into Windows Binary Exploitation, and it will teach you how to exploit local and remote buffer overflow vulnerabilities on Windows machines.

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



Brief Intro to Hardware Attacks

8 Sections **Medium** **General**

This mini-module concisely introduces hardware attacks, covering Bluetooth risks and attacks, Cryptanalysis Side-Channel Attacks, and vulnerabilities like Spectre and Meltdown. It delves into both historical and modern Bluetooth hacking techniques, explores the principles of cryptanalysis and different side-channel attacks, and outlines microprocessor design, optimisation strategies and vulnerabilities, such as Spectre and Meltdown.

100% Completed

