Student Transcript

30-06-2025

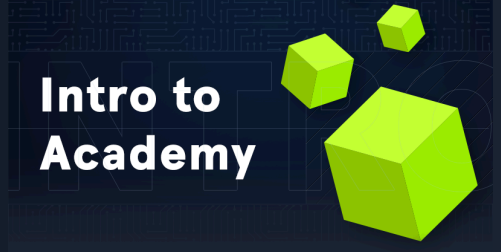
HTB ACADEMY

Lance Rosengarten
#432758

Paths completed: 4
Targets compromised: 212
Ranking: Top 1%

PATHS COMPLETED		PROGRESS
	Basic Toolset 7 Modules Medium 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.	100% Completed
	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
	Operating System Fundamentals 4 Modules Easy 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.	100% Completed
	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.

93.75% 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.

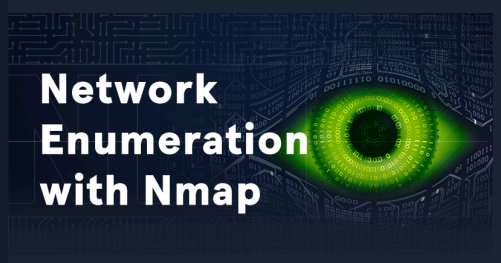
100% Completed

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

Cracking Passwords with Hashcat

14 Sections | Medium | Offensive

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

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

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.

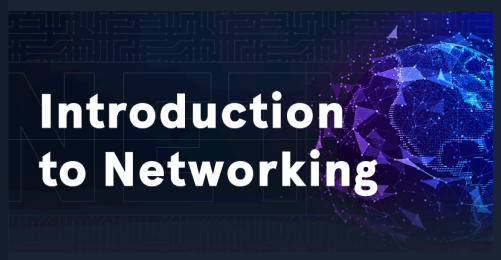
100% Completed

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.

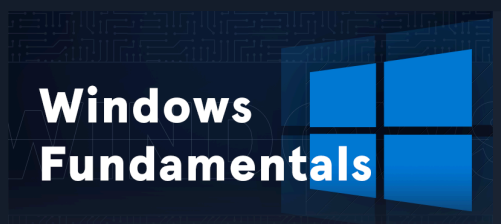
100% Completed

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

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.

92.31% 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.

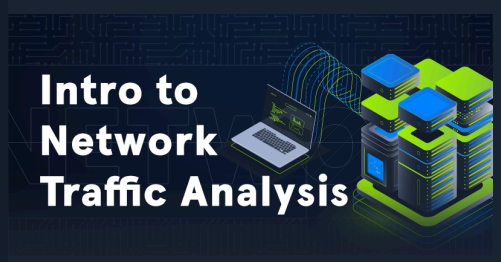
100% Completed

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.

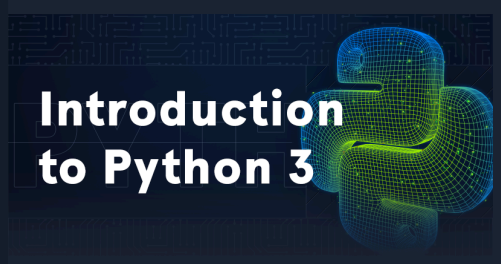
100% Completed

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.

100% 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

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

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

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.

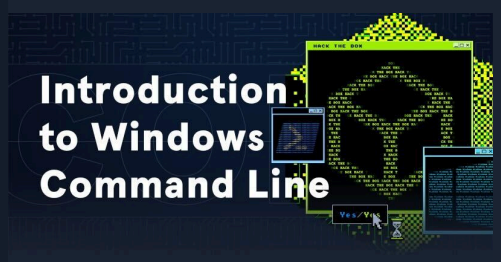
100% Completed

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



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

Windows Attacks & Defense

16 Sections | Medium | Purple

Microsoft Active Directory (AD) has been, for the past 20+ years, the leading enterprise domain management suite, providing identity and access management, centralized domain administration, authentication, and much more. Throughout those years, the more integrated our applications and data have become with AD, the more exposed to a large-scale compromise we have become. In this module, we will walk through the most commonly abused and fruitful attacks against Active Directory environments that allow threat actors to perform horizontal and vertical privilege escalations in addition to lateral movement. One of the module's core goals is to showcase prevention and detection methods against the covered Active Directory attacks.

100% Completed

Active Directory BloodHound

14 Sections | Medium | Offensive

This module covers AD enumeration focusing on the BloodHound tool. We will cover various techniques for enumerating key AD objects that will inform our attacks in later modules.

21.43% Completed

Android Fundamentals

20 Sections | Fundamental | General

This module introduces fundamental concepts of the Android environment, focusing on the operating system, its security features, and the structure of applications. It provides students with details about the different styles of application development and familiarizes them with their development environment. This module also explains how apps communicate in the Android environment, highlighting why this is critical information for their security. Students are also introduced to setting up a testing environment to prepare for the Application Penetration Testing process.

35% 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.

100% Completed

Wi-Fi Penetration Testing Basics

16 Sections | Medium | Offensive

In today's digital age, wireless networks are ubiquitous, connecting countless devices in homes, businesses, and public spaces. With this widespread connectivity comes an increased risk of security vulnerabilities that can be exploited by malicious actors. As such, understanding and securing Wi-Fi networks has become a crucial aspect of cybersecurity. Whether you are an aspiring ethical hacker, a network administrator, or simply a tech enthusiast, gaining a solid foundation in Wi-Fi penetration testing is essential for safeguarding your digital environment.

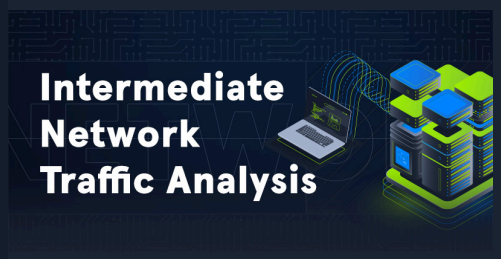
100% Completed

Working with IDS/IPS

11 Sections | Medium | Defensive

This module offers an in-depth exploration of Suricata, Snort, and Zeek, covering both rule development and intrusion detection. We'll guide you through signature-based and analytics-based rule development, and you'll learn to tackle encrypted traffic. The module features numerous hands-on examples, focusing on the detection of prevalent malware such as PowerShell Empire, Covenant, Sliver, Cerber, Dridex, Ursnif, and Patchwork. We also dive into detecting attacking techniques like DNS exfiltration, TLS/HTTP Exfiltration, PsExec lateral movement, and beaconing through IDS/IPS.

100% Completed

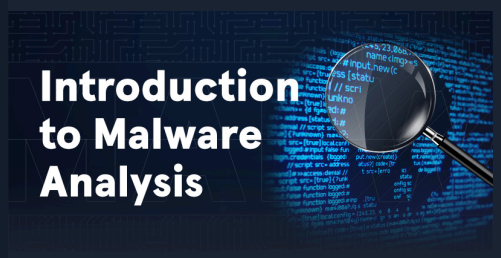


Intermediate Network Traffic Analysis

18 Sections | Easy | Defensive

Through network traffic analysis, this module sharpens skills in detecting link layer attacks such as ARP anomalies and rogue access points, identifying network abnormalities like IP spoofing and TCP handshake irregularities, and uncovering application layer threats from web-based vulnerabilities to peculiar DNS activities.

100% Completed



Introduction to Malware Analysis

9 Sections | Hard | Defensive

This module offers an exploration of malware analysis, specifically targeting Windows-based threats. The module covers Static Analysis utilizing Linux and Windows tools, Malware Unpacking, Dynamic Analysis (including malware traffic analysis), Reverse Engineering for Code Analysis, and Debugging using x64dbg. Real-world malware examples such as WannaCry, DoomJuice, Brbbot, Dharma, and Meterpreter are analyzed to provide practical experience.

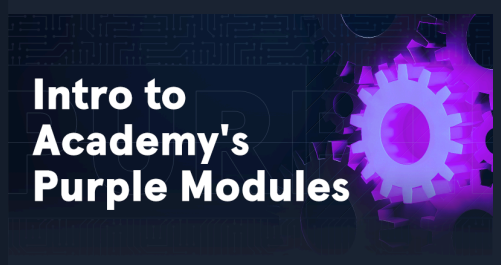
100% Completed

YARA & Sigma for SOC Analysts

11 Sections | Easy | Defensive

This Hack The Box Academy module covers how to create YARA rules both manually and automatically and apply them to hunt threats on disk, live processes, memory, and online databases. Then, the module switches gears to Sigma rules covering how to build Sigma rules, translate them into SIEM queries using "sigmac", and hunt threats in both event logs and SIEM solutions. It's all hands-on, using real-world malware and techniques.

27.27% Completed



Intro to Academy's Purple Modules

13 Sections | Medium | Purple

This module will introduce you to HTB Academy's Purple modules, which bridge the gap between Offensive and Defensive modules and provide a holistic view of both the attacking and defending perspectives on the covered topics. More specifically, the Purple modules will allow for in-depth forensic analysis through detailed logging, traffic and memory capturing, and an installed DFIR toolset within each target after completing the attack part of each section.

38.46% Completed