Student Transcript

22-07-2025

HTB ACADEMY

Jrew Simpson
#1756641

Targets compromised: 57
Ranking: Top 5%

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.

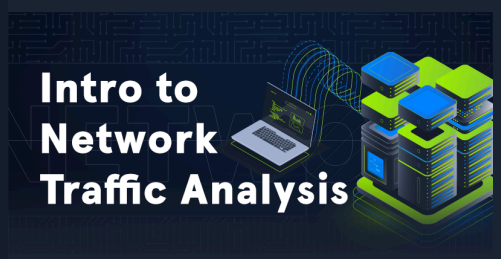
100% Completed

Linux Fundamentals

30 Sections | Fundamental | General

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

100% Completed

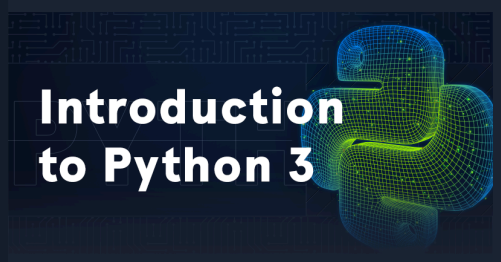


Intro to Network Traffic Analysis

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

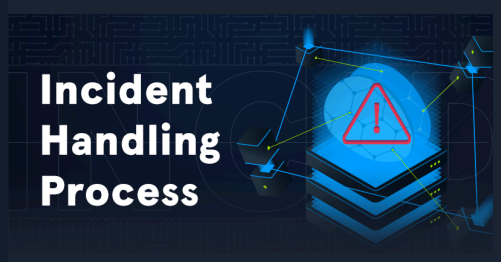


Introduction to Python 3

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



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

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

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.

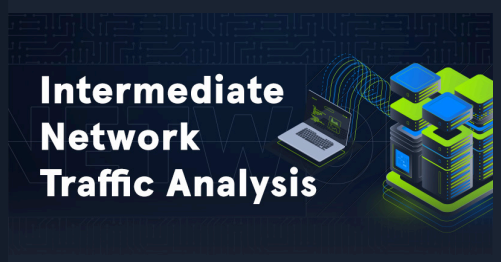
100% Completed

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

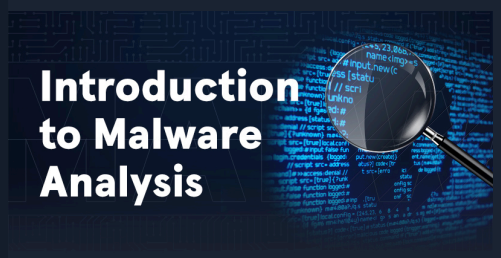


Intermediate Network Traffic Analysis

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.

11.11% Completed

Introduction to Information Security

24 Sections | Fundamental | General

This theoretical module provides a comprehensive introduction to the foundational components of information security, focusing on the structure and operation of effective InfoSec frameworks. It explores the theoretical roles of security applications across networks, software, mobile devices, cloud environments, and operational systems, emphasizing their importance in protecting organizational assets. Students will gain an understanding of common threats, including malware and advanced persistent threats (APTs), alongside strategies for mitigating these risks. The module also introduces the roles and responsibilities of security teams and InfoSec professionals, equipping students with the confidence to advance their knowledge and explore specialized areas within the field.

100% Completed