Student Transcript

30-07-2025

HTB ACADEMY

Piotr Wojnarowski
#1494935

Paths completed: 5
Targets compromised: 233
Ranking: Top 1%

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

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

Intro to Binary Exploitation

4 Modules Hard

Binary exploitation is a core tenet of penetration testing, but learning it can be daunting. This is mainly due to the complexity of binary files and their underlying machine code and how binary files interact with computer memory and the processor. To learn the basics of binary exploitation, we must first have a firm grasp of Computer Architecture and the Assembly Language. To move into more advanced binary exploitation, we must have a firm grasp on basic buffer overflow attacks, principles such as CPU architecture, and CPU registers for 32-bit Windows and Linux systems. Furthermore, a strong foundation in Python scripting is essential for writing and understanding exploit scripts.

100% Completed

SOC Analyst Prerequisites

10 Modules | Easy

The SOC Analyst Prerequisites path is designed for those looking to become SOC/Security Analysts. It dives into fundamental IT and Information Security subjects including networking, Linux and Windows operating systems, basic programming and scripting, as well as working with Assembly. In addition, students will be exposed to the fundamental concepts of information security and penetration testing. This skill path is made up of modules that will assist learners in developing and strengthening a foundational understanding before proceeding with learning more complex security topics.

100% Completed

MODULE

PROGRESS

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

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.

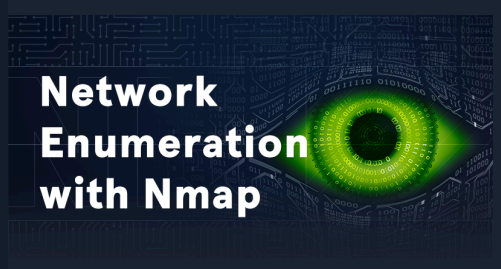
75% Completed

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.

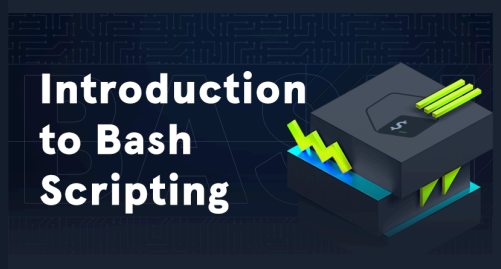
100% Completed

Cracking Passwords with Hashcat

14 Sections | Medium | Offensive

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

71.43% 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 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

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

DNS Enumeration Using Python

11 Sections | Medium | General

As a penetration tester or red teamer, it is imperative that we understand the tools that we use inside and out and also have the ability to write out own, even simple, tools if we are on an assessment with certain constraints such as no internet or the requirement to use a customer provided host as our "attack box." A strong understanding of DNS as well as the various ways to interact with fundamental when performing any security assessment.

100% Completed

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.

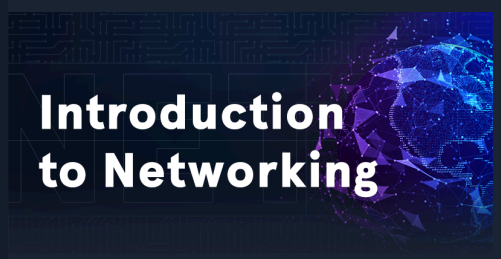
100% Completed

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



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.

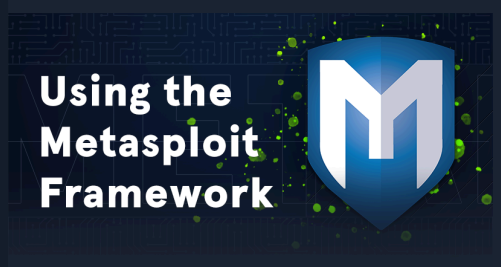
100% Completed

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



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

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.

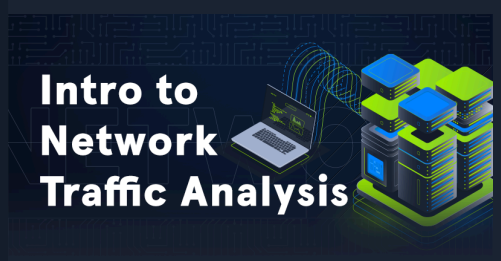
100% Completed

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.

50% Completed

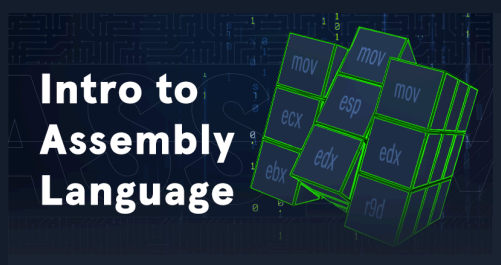


Intro to Network Traffic Analysis

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



Intro to Assembly Language

24 Sections | Medium | General

This module builds the core foundation for Binary Exploitation by teaching Computer Architecture and Assembly language basics.

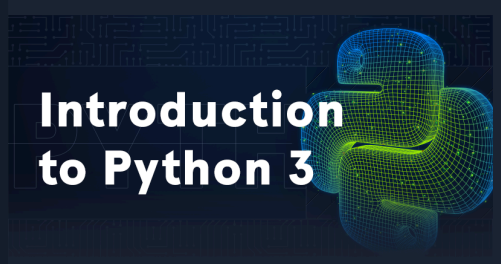
100% Completed

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

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.

88.24% 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.

50% 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.

100% 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.

36.36% 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.

89.47% 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.

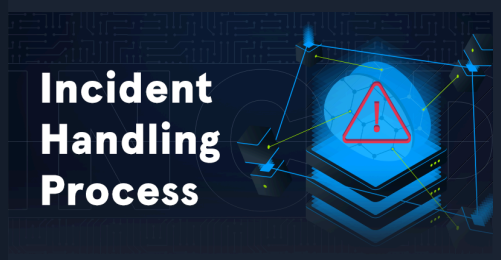
52.63% Completed

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.

23.08% 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.

92.86% Completed

MacOS Fundamentals

11 Sections | Fundamental | General

This module covers the fundamentals required to work comfortably within the macOS operating system and shell.

100% 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.

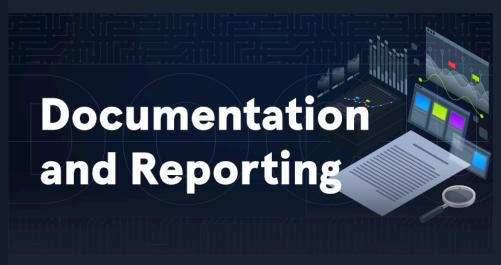
100% Completed

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



Documentation & Reporting

8 Sections | Easy | General

Proper documentation is paramount during any engagement. The end goal of a technical assessment is the report deliverable which will often be presented to a broad audience within the target organization. We must take detailed notes and be very organized in our documentation, which will help us in the event of an incident during the assessment. This will also help ensure that our reports contain enough detail to illustrate the impact of our findings properly.

87.5% 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

Blind SQL Injection

16 Sections | Hard | Offensive

In this module, we cover blind SQL injection attacks and MSSQL-specific attacks.

37.5% 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.

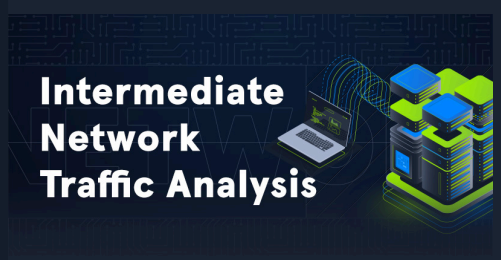
85% Completed

Introduction to C#

21 Sections | Easy | General

Introduction to C# aims to provide a solid foundation to understand and work with C# code. Covering the crucial foundations and more intricate concepts, providing a comprehensive depth of knowledge in C#.

90.48% 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.

5.56% 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

Introduction to Digital Forensics

8 Sections | Medium | Defensive

Dive into Windows digital forensics with Hack The Box Academy's "Introduction to Digital Forensics" module. Gain mastery over core forensic concepts and tools such as FTK Imager, KAPE, Velociraptor, and Volatility. Dive deep into memory forensics, disk image analysis, and rapid triaging procedures. Learn to construct timelines from MFT, USN Journals, and Windows event logs while getting hands-on with key artifacts like MFT, USN Journal, Registry Hives, Prefetch Files, ShimCache, Amcache, BAM, and SRUM data.

50% Completed

Security Incident Reporting

5 Sections | Easy | General

Tailored to provide a holistic understanding, this Hack The Box Academy module ensures participants are adept at identifying, categorizing, and documenting security incidents with utmost accuracy and professionalism. The module meticulously breaks down the elements of a robust incident report and then presents participants with a real-world incident report, offering practical insights into the application of the concepts discussed.

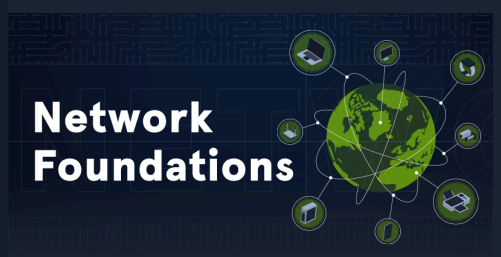
100% Completed

Web Fuzzing

12 Sections | Easy | Offensive

In this module, we explore the essential techniques and tools for fuzzing web applications, an essential practice in cybersecurity for identifying hidden vulnerabilities and strengthening web application security.

100% Completed



Network Foundations

12 Sections | Fundamental | General

This course introduces the basic concepts essential to understanding the world of networking. Students will learn about various network types such as LANs and WANs, discuss fundamental networking principles including the OSI and TCP/IP models, and explore key network components like routers and servers. The course also covers important topics such as IP addressing, network security, and internet architecture, providing a comprehensive overview of networking that is crucial for any IT professional.

100% Completed

Fundamentals of AI

24 Sections | Medium | General

This module provides a comprehensive guide to the theoretical foundations of Artificial Intelligence (AI). It covers various learning paradigms, including supervised, unsupervised, and reinforcement learning, providing a solid understanding of key algorithms and concepts.

100% Completed

Applications of AI in InfoSec

25 Sections | Medium | General

This module is a practical introduction to building AI models that can be applied to various infosec domains. It covers setting up a controlled AI environment using Miniconda for package management and JupyterLab for interactive experimentation. Students will learn to handle datasets, preprocess and transform data, and implement structured workflows for tasks such as spam classification, network anomaly detection, and malware classification. Throughout the module, learners will explore essential Python libraries like Scikit-learn and PyTorch, understand effective approaches to dataset processing, and become familiar with common evaluation metrics, enabling them to navigate the entire lifecycle of AI model development and experimentation.

52% 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

Introduction to Penetration Testing

21 Sections | Fundamental | Offensive

In this module, we will get into the fundamentals of penetration testing, a critical aspect of cybersecurity theory that explains how professionals in the field operate and underscores the significance of penetration testing within cybersecurity practices.

100% Completed

Pentest in a Nutshell

24 Sections | Easy | Offensive

This module focuses on providing a detailed, guided simulation of a real penetration test, emphasizing the fine details of the penetration testing process. It guides you through each step, from reconnaissance to exploitation, mirroring the techniques and methodologies used by professional penetration testers. It offers hands-on experience in a controlled environment and aims to deepen understanding and sharpen skills essential for effective cybersecurity assessments.

37.5% Completed