





Paths completed: 8

Targets compromised: 544

Ranking: Top 1%

PATHS COMPLETED

PROGRESS

	<div>Bug Bounty Hunter</div> <div>20 ModulesMedium</div> <p>The Bug Bounty Hunter Job Role Path is for individuals who want to enter the world of Bug Bounty Hunting with little to no prior experience. This path covers core web application security assessment and bug bounty hunting concepts and provides a deep understanding of the attack tactics used during bug bounty hunting. Armed with the necessary theoretical background, multiple practical exercises, and a proven bug bounty hunting methodology, students will go through all bug bounty hunting stages, from reconnaissance and bug identification to exploitation, documentation, and communication to vendors/programs. Upon completing this job role path, you will have become proficient in the most common bug bounty hunting and attack techniques against web applications and be in the position of professionally reporting bugs to a vendor.</p>	100% Completed
	<div>Basic Toolset</div> <div>7 ModulesMedium</div> <p>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.</p>	100% Completed
	<div>Cracking into Hack the Box</div> <div>3 ModulesEasy</div> <p>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.</p>	100% Completed
	<div>Local Privilege Escalation</div> <div>2 ModulesMedium</div> <p>Privilege escalation is a vital phase of the penetration testing process, one we may revisit multiple times during an engagement. During our assessments, we will encounter a large variety of operating systems and applications. Most often, if we can exploit a vulnerability and gain a foothold on a host, it will be running some version of Windows or Linux. Both present a large attack surface with many tactics and techniques available to us for escalating privileges. This path teaches the core concepts of local privilege escalation necessary for being successful against Windows and Linux systems. The path covers manual enumeration and exploitation and the use of tools to aid in the process.</p>	100% Completed



Penetration Tester

28 Modules Medium

The Penetration Tester Job Role Path is for newcomers to information security who aspire to become professional penetration testers. This path covers core security assessment concepts and provides a deep understanding of the specialized tools, attack tactics, and methodology used during penetration testing. Armed with the necessary theoretical background and multiple practical exercises, students will go through all penetration testing stages, from reconnaissance and enumeration to documentation and reporting. Upon completing this job role path, you will have obtained the practical skills and mindset necessary to perform professional security assessments against enterprise-level infrastructure at an intermediate level. The Information Security Foundations skill path can be considered prerequisite knowledge to be successful while working through this job role path.

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



Junior Cybersecurity Analyst

20 Modules Easy

The Junior Cybersecurity Analyst Job Role Path is the first step to enter and gain practical, hands-on experience in the cybersecurity field. This path covers essential cybersecurity concepts and builds a foundational understanding of operating systems, offensive and defensive tools, attack tactics, log analysis, and methodologies employed by penetration testers and security operations centers. Students will explore key principles while gaining practical experience in both offensive and defensive cybersecurity assessments, including the basics of penetration testing and security analysis. This job role path equips you with the skills and mindset needed to launch a career in cybersecurity, offering a well-rounded foundation in both offensive and defensive techniques that reflects the evolving demands of real-world cybersecurity operations.

100% Completed



MODULE

PROGRESS



Learning Process







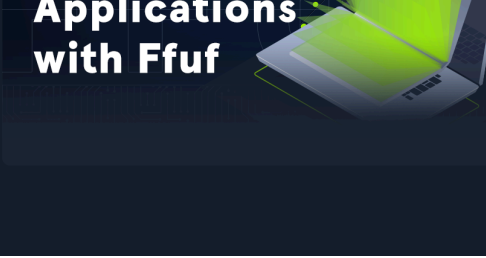
20 Sections Fundamental General


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



	<h3>Intro to Academy</h3> <div> 8 Sections Fundamental General </div> <p>Your first stop in Hack The Box Academy to become acquainted with the platform, its features, and its learning process.</p>	100% Completed <div></div>
	<h3>Hacking WordPress</h3> <div> 16 Sections Easy Offensive </div> <p>WordPress is an open-source Content Management System (CMS) that can be used for multiple purposes.</p>	100% Completed <div></div>
	<h3>Linux Fundamentals</h3> <div> 30 Sections Fundamental General </div> <p>This module covers the fundamentals required to work comfortably with the Linux operating system and shell.</p>	100% Completed <div></div>
	<h3>Network Enumeration with Nmap</h3> <div> 12 Sections Easy Offensive </div> <p>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.</p>	100% Completed <div></div>
	<h3>Cracking Passwords with Hashcat</h3> <div> 14 Sections Medium Offensive </div> <p>This module covers the fundamentals of password cracking using the Hashcat tool.</p>	100% Completed <div></div>
	<h3>Introduction to Bash Scripting</h3> <div> 10 Sections Easy General </div> <p>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.</p>	100% Completed <div></div>
	<h3>File Inclusion</h3> <div> 11 Sections Medium Offensive </div> <p>File Inclusion is a common web application vulnerability, which can be easily overlooked as part of a web application's functionality.</p>	100% Completed <div></div>
	<h3>File Transfers</h3> <div> 10 Sections Medium Offensive </div> <p>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.</p>	100% Completed <div></div>
	<h3>OSINT: Corporate Recon</h3> <div> 23 Sections Hard Offensive </div> <p>OSINT (Open-source Intelligence) is a crucial stage of the penetration testing process. A thorough examination of publicly available information can increase the chances of finding a vulnerable system, gaining valid credentials through password spraying, or gaining a foothold via social engineering. There is a vast amount of publicly available information from which relevant information needs to be selected.</p>	100% Completed <div></div>

	<h3>SQL Injection Fundamentals</h3> <div>17 SectionsMediumOffensive</div> <p>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.</p>	100% Completed
	<h3>Introduction to Networking</h3> <div>21 SectionsFundamentalGeneral</div> <p>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.</p>	100% Completed
	<h3>Web Requests</h3> <div>8 SectionsFundamentalGeneral</div> <p>This module introduces the topic of HTTP web requests and how different web applications utilize them to communicate with their backends.</p>	100% Completed
	<h3>Using the Metasploit Framework</h3> <div>15 SectionsEasyOffensive</div> <p>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.</p>	100% Completed
	<h3>JavaScript Deobfuscation</h3> <div>11 SectionsEasyDefensive</div> <p>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.</p>	100% Completed
	<h3>Windows Fundamentals</h3> <div>14 SectionsFundamentalGeneral</div> <p>This module covers the fundamentals required to work comfortably with the Windows operating system.</p>	100% Completed
	<h3>Linux Privilege Escalation</h3> <div>28 SectionsEasyOffensive</div> <p>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.</p>	100% Completed
	<h3>Attacking Web Applications with Ffuf</h3> <div>13 SectionsEasyOffensive</div> <p>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.</p>	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.

100% Completed




SQLMap Essentials

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




Windows Privilege Escalation

Windows Privilege Escalation

33 Sections Medium Offensive

After gaining a foothold, elevating our privileges will provide more options for persistence and may reveal information stored locally that can further our access in the environment. Enumeration is the key to privilege escalation. When you gain initial shell access to the host, it is important to gain situational awareness and uncover details relating to the OS version, patch level, any installed software, our current privileges, group memberships, and more. Windows presents an enormous attack surface and, being that most companies run Windows hosts in some way, we will more often than not find ourselves gaining access to Windows machines during our assessments. This covers common methods while emphasizing real-world misconfigurations and flaws that we may encounter during an assessment. There are many additional "edge-case" possibilities not covered in this module. We will cover both modern and legacy Windows Server and Desktop versions that may be present in a client environment.

100% Completed




Introduction to Active Directory

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

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

Getting Started

23 Sections Fundamental Offensive

This module covers the fundamentals of penetration testing and an introduction to Hack The Box.

100% Completed



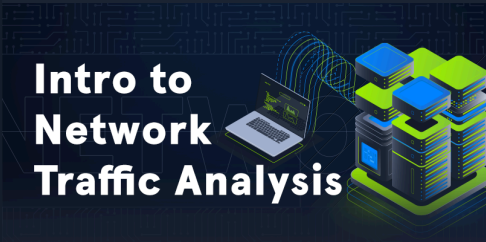
Broken Authentication

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.

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



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



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.

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





Attacking Common Applications

Attacking Common Applications

33 Sections Medium Offensive

Penetration Testers can come across various applications, such as Content Management Systems, custom web applications, internal portals used by developers and sysadmins, and more. It's common to find the same applications across many different environments. While an application may not be vulnerable in one environment, it may be misconfigured or unpatched in the next. It is important as an assessor to have a firm grasp of enumerating and attacking the common applications discussed in this module. This knowledge will help when encountering other types of applications during assessments.

100% Completed



Shells & Payloads

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

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.

100% Completed



Web Attacks

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

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.

100% Completed



Active Directory Enumeration & Attacks

Active Directory Enumeration & Attacks

36 Sections Medium Offensive

Active Directory (AD) is the leading enterprise domain management suite, providing identity and access management, centralized domain administration, authentication, and much more. Due to the many features and complexity of AD, it presents a large attack surface that is difficult to secure properly. To be successful as infosec professionals, we must understand AD architectures and how to secure our enterprise environments. As Penetration testers, having a firm grasp of what tools, techniques, and procedures are available to us for enumerating and attacking AD environments and commonly seen AD misconfigurations is a must.

100% Completed



Information Gathering - Web Edition





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



	<h3>Server-side Attacks</h3> <p>19 Sections Medium Offensive</p> <p>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.</p>	100% Completed
	<h3>Password Attacks</h3> <p>26 Sections Medium Offensive</p> <p>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.</p>	100% Completed
	<h3>Incident Handling Process</h3> <p>9 Sections Fundamental General</p> <p>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.</p>	100% Completed
	<h3>Session Security</h3> <p>14 Sections Medium Offensive</p> <p>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.</p>	100% Completed
	<h3>MacOS Fundamentals</h3> <p>11 Sections Fundamental General</p> <p>This module covers the fundamentals required to work comfortably within the macOS operating system and shell.</p>	100% Completed
	<h3>Pivoting, Tunneling, and Port Forwarding</h3> <p>18 Sections Medium Offensive</p> <p>Once a foothold is gained during an assessment, it may be in scope to move laterally and vertically within a target network. Using one compromised machine to access another is called pivoting and allows us to access networks and resources that are not directly accessible to us through the compromised host. Port forwarding accepts the traffic on a given IP address and port and redirects it to a different IP address and port combination. Tunneling is a technique that allows us to encapsulate traffic within another protocol so that it looks like a benign traffic stream.</p>	100% Completed
	<h3>Web Service & API Attacks</h3> <p>13 Sections Medium Offensive</p> <p>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.</p>	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.

100% Completed



Attacking Enterprise Networks

14 Sections Medium Offensive

We often encounter large and complex networks during our assessments. We must be comfortable approaching an internal or external network, regardless of the size, and be able to work through each phase of the penetration testing process to reach our goal. This module will guide students through a simulated penetration testing engagement, from start to finish, with an emphasis on hands-on testing steps that are directly applicable to real-world engagements.

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

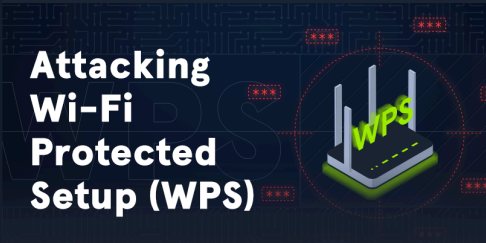


Wired Equivalent Privacy (WEP) Attacks

13 Sections Medium Offensive

In this module, we delve into Wired Equivalent Privacy (WEP) and the various attacks that can compromise it. We'll explore how to identify access points configured with WEP and demonstrate different methods to exploit its vulnerabilities. As WEP is an outdated and insecure protocol, understanding its weaknesses is crucial for recognizing the need to upgrade to more secure protocols. This module aims to provide insights into WEP's vulnerabilities and practical techniques for testing its security.

100% Completed



Attacking Wi-Fi Protected Setup (WPS)

13 Sections Medium Offensive

In this module, we delve into the intricacies of WPS, uncovering the common vulnerabilities that plague this technology. From brute-force attacks to more sophisticated exploitation techniques, we will explore how attackers compromise WPS-enabled networks. By understanding these vulnerabilities and their related attacks, you will gain the knowledge necessary to protect your networks and mitigate the risks associated with WPS.

100% 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.

80% 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

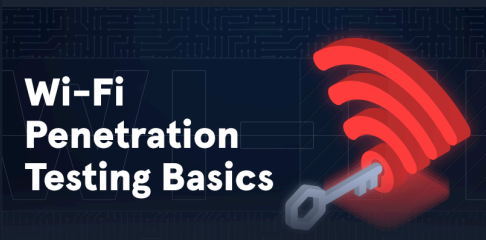


Windows Event Logs & Finding Evil

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



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



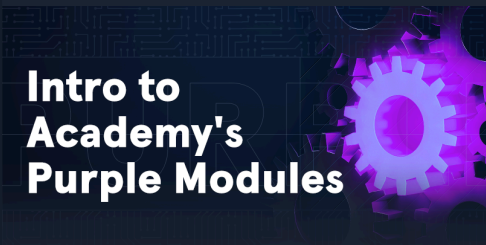
Brief Intro to Hardware Attacks

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





Intro to Academy's Purple Modules

14 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.

100% Completed

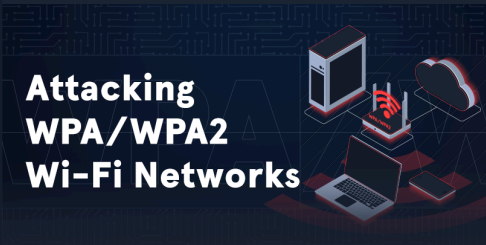


Web Fuzzing

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

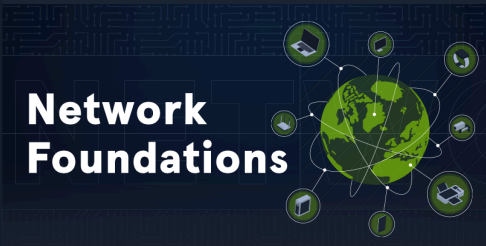


Attacking WPA/WPA2 Wi-Fi Networks

15 Sections Medium Offensive

This module explores the security challenges of WPA and WPA2 Wi-Fi networks, focusing on WPA/WPA2-Personal and WPA/WPA2-Enterprise. Although these protocols aim to secure wireless communication, attackers can exploit various weaknesses in home and enterprise environments. This module will delve deeper into WPA-Personal and WPA-Enterprise, demonstrating multiple attack vectors to compromise each. Understanding these attack vectors will give you insight into the vulnerabilities that could compromise WPA/WPA2 networks and how to secure them.

100% Completed

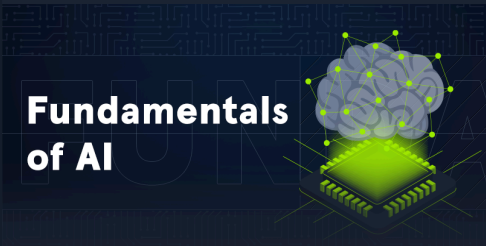


Network Foundations

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



Wi-Fi Evil Twin Attacks

16 Sections Medium Offensive

This module explores the concept of evil twin attacks on Wi-Fi networks, focusing on WPA2, WPA3, and WPA-Enterprise. Despite these protocols being designed with strong security measures, they remain vulnerable to social engineering and rogue access point attacks. We will delve into both manual and automated methods for executing evil twin attacks, demonstrating practical approaches for each network type. Additionally, we will cover advanced MiTM techniques, including DNS spoofing and SSL interception, to highlight how attackers can exploit compromised connections for data interception.

100% Completed



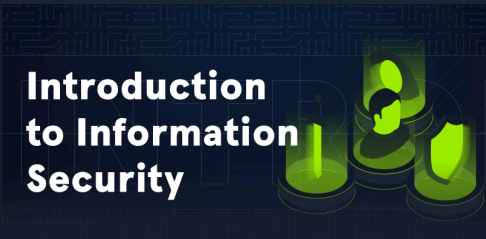


Applications of AI in InfoSec

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.

96% 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.

100% Completed



Bypassing Wi-Fi Captive Portals

17 Sections Medium Offensive

In this module, we delve into a range of methods for identifying and bypassing captive portals, employing both indirect and direct exploitation techniques. We cover tactics such as MAC spoofing, ARP poisoning, DNS tunneling, and credential interception, alongside direct attack vectors like Cross-Site Scripting (XSS), file upload vulnerabilities, file inclusion, and brute force attacks. Additionally, we will examine client hijacking strategies to extract credentials and circumvent portal restrictions. By understanding these attack methods, we can evaluate and enhance the security of captive portal implementations.

100% Completed



Wi-Fi Password Cracking Techniques

16 Sections Medium Offensive

Password cracking is a cornerstone of wireless penetration testing, as many real-world assessments hinge on the strength of the Wi-Fi password and our ability to break it. Despite its importance, many testers continue to rely solely on dictionary attacks with basic tools and minimal customization. In this module, we'll go beyond the basics and explore the full spectrum of practical techniques, targeted strategies, and performance-driven optimizations for cracking Wi-Fi passwords.

100% Completed

