Student Transcript

14-01-2025

HTB ACADEMY

scriptie

#128555

Certifications obtained: 3
Paths completed: 8
Targets compromised: 895
Ranking: Top 1%

CERTIFICATIONS OBTAINED	CERTIFIED ON

HTB Certified Penetration Testing Specialist

28 Modules · Medium · Penetration Testing

HTB Certified Penetration Testing Specialist (HTB CPTS) is a highly hands-on certification that assesses the candidates' penetration testing skills. HTB Certified Penetration Testing Specialist certification holders will possess technical competency in the ethical hacking and penetration testing domains at an intermediate level. They will also be able to assess the risk at which an infrastructure is exposed and compose a commercial-grade as well as actionable report.

July 04 2023

HTB Certified Bug Bounty Hunter

20 Modules · Medium · Bug Bounty Hunting

HTB Certified Bug Bounty Hunter (HTB CBBH) is a highly hands-on certification that assesses the candidates' bug bounty hunting and web application pentesting skills. HTB Certified Bug Bounty Hunter certification holders will possess technical competency in the bug bounty hunting and web application penetration testing domains at an intermediate level. They will also be able to assess the risk at which a web application, service, or API is exposed and compose a commercial-grade as well as actionable report.

July 19 2024

HTB Certified Defensive Security Analyst

15 Modules · Medium · Security Analysis

HTB Certified Defensive Security Analyst (HTB CDSA) is a highly hands-on certification that assesses the candidates' security analysis, SOC operations, and incident handling skills. HTB Certified Defensive Security Analyst (HTB CDSA) certification holders will possess technical competency in the security analysis, SOC operations, and incident handling domains at an intermediate level. They will be able to spot security incidents and identify avenues of detection that may not be immediately apparent from simply looking at the available data. They will also excel at thinking outside the box, correlating disparate pieces of data, pivoting relentlessly to determine the maximum impact of an incident, and creating actionable security incident reports.

December 27 2024

PATHS COMPLETED	PROGRESS

Bug Bounty Hunter

20 Modules · Medium

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.

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

Local Privilege Escalation

2 Modules · Medium

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.

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

SOC Analyst

15 Modules · Medium

The SOC Analyst Job Role Path is for newcomers to information security who aspire to become professional SOC analysts. This path covers core security monitoring and security analysis concepts and provides a deep understanding of the specialized tools, attack tactics, and methodology used by adversaries. Armed with the necessary theoretical background and multiple practical exercises, students will go through all security analysis stages, from traffic analysis and SIEM monitoring to DFIR activities and reporting. Upon completing this job role path, you will have obtained the practical skills and mindset necessary to monitor enterprise-level infrastructure and detect intrusions at an intermediate level. The SOC Analyst Prerequisites skill path can be considered prerequisite knowledge to be successful while working through this job role path.

100% Completed

Senior Web Penetration Tester

15 Modules Hard

The Senior Web Penetration Tester Job Role Path is designed for individuals who aim to develop skills in identifying advanced and hard-to-find web vulnerabilities using both black box and white box techniques. This path encompasses advanced-level training in web security, web penetration testing, and secure coding concepts. It also provides a deep understanding of the application debugging, source code review, and custom exploit development aspects of web security. Equipped with the necessary theoretical background, multiple practical exercises, and a proven methodology for web vulnerability identification, students will eventually be capable of performing professional security assessments against modern and highly secure web applications, as well as effectively reporting vulnerabilities found in code or arising from logical errors.

100% Completed

Active Directory Penetration Tester

15 Modules Hard

The Active Directory Penetration Tester Job Role Path is designed for individuals who aim to develop skills in pentesting large Active Directory (AD) networks and the components commonly found in such environments. This path equips students with the skills needed to evaluate the security of AD environments, navigate complex Windows networks, and identify elusive attack paths. This path includes advanced hands-on labs where participants will practice techniques such as Kerberos attacks, NTLM relay attacks, and the abuse of services like AD Certificate Services (ADCS), Exchange, WSUS, and MSSQL. Students will also learn how to exploit misconfigurations in Active Directory DACLs and Domain Trusts, perform evasion tactics in Windows environments, and leverage Command and Control (C2) frameworks for post-exploitation activities. By combining theoretical foundations with practical exercises and a structured methodology for identifying AD vulnerabilities, this path enables students to conduct professional security assessments on complex AD infrastructures and effectively report security weaknesses discovered by chaining multiple vulnerabilities.

100% Completed

Active Directory Enumeration

3 Modules Hard

Active Directory (AD) is widely used by companies across all verticals/sectors, non-profits, government agencies, and educational institutions of all sizes. By its nature, AD is easily misconfigured and has many inherent flaws and widely known vulnerabilities. Due to the sheer number of objects and in AD and complex intertwined relationships that form as an AD network grows, it becomes increasingly difficult to secure and presents a vast attack surface. AD environments can become quite large and often hold many obvious and more difficult to discover flaws. A deep understanding of AD enumeration techniques and tools is essential to becoming a well-rounded information security professional.

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.

100% 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.

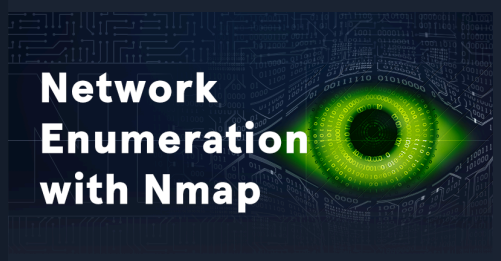
100% Completed

Linux Fundamentals

30 Sections | Fundamental | General

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

36.67% 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.

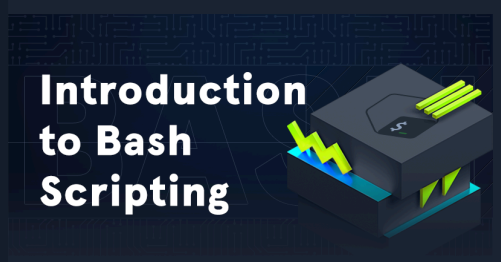
100% Completed

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

Kerberos Attacks

23 Sections | Hard | Offensive

Kerberos is an authentication protocol that allows users to authenticate and access services on a potentially insecure network. Due to its prevalence throughout an Active Directory environment, it presents us with a significant attack surface when assessing internal networks. This module will explain how Kerberos works thoroughly and examines several scenarios to practice the most common attacks against it from multiple perspectives.

100% Completed

Active Directory LDAP

12 Sections | Medium | Offensive

This module provides an overview of Active Directory (AD), introduces core AD enumeration concepts, and covers enumeration with built-in tools.

100% Completed

Active Directory PowerView

9 Sections | Medium | Offensive

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

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

SQL Injection Fundamentals

17 Sections | Medium | Offensive

Databases are an important part of web application infrastructure and SQL (Structured Query Language) to store, retrieve, and manipulate information stored in them. SQL injection is a code injection technique used to take advantage of coding vulnerabilities and inject SQL queries via an application to bypass authentication, retrieve data from the back-end database, or achieve code execution on the underlying server.

100% Completed

Web Requests

8 Sections | Fundamental | General

This module introduces the topic of HTTP web requests and how different web applications utilize them to communicate with their backends.

100% Completed

Secure Coding 101: JavaScript

17 Sections | Hard | Defensive

Learn how to improve your JavaScript code's security through Code Review, Static/Dynamic Analysis, Vulnerability Identification, and Patching.

64.71% 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

Using the Metasploit Framework

15 Sections | Easy | Offensive

The Metasploit Framework is an open-source set of tools used for network enumeration, attacks, testing security vulnerabilities, evading detection, performing privilege escalation attacks, and performing post-exploitation.

100% Completed

Stack-Based Buffer Overflows on Linux x86

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.

23.08% Completed

Whitebox Pentesting 101: Command Injection

19 Sections | Hard | Offensive

This module focuses on discovering Command Injection vulnerabilities in NodeJS servers and exploiting them to control the server.

52.63% 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.

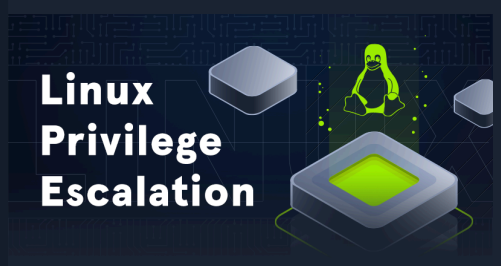
100% Completed

Windows Fundamentals

14 Sections | Fundamental | General

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

7.14% Completed



Linux Privilege Escalation

28 Sections | Easy | Offensive

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

96.43% 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.

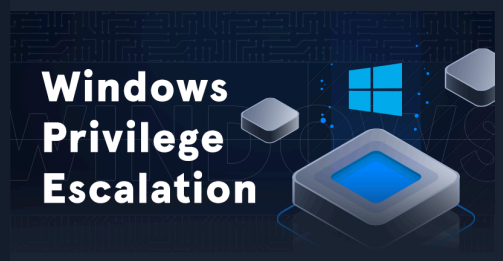
84.62% Completed

SQLMap Essentials

11 Sections | Easy | Offensive

The SQLMap Essentials module will teach you the basics of using SQLMap to discover various types of SQL Injection vulnerabilities, all the way to the advanced enumeration of databases to retrieve all data of interest.

100% Completed



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.

96.97% 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.

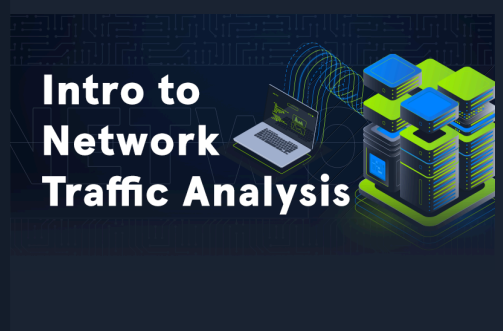
100% Completed

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.

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.

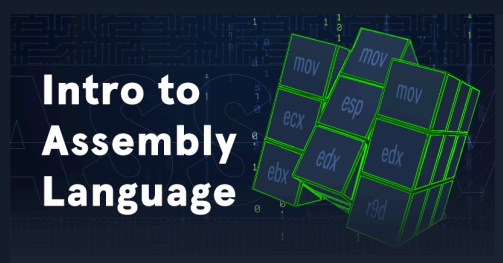
100% Completed

Using CrackMapExec

27 Sections | Medium | Offensive

Active Directory presents a vast attack surface and often requires us to use many different tools during an assessment. The CrackMapExec tool, known as a "Swiss Army Knife" for testing networks, facilitates enumeration, attacks, and post-exploitation that can be leveraged against most any domain using multiple network protocols. It is a versatile and highly customizable tool that should be in any penetration tester's toolbox.

100% Completed

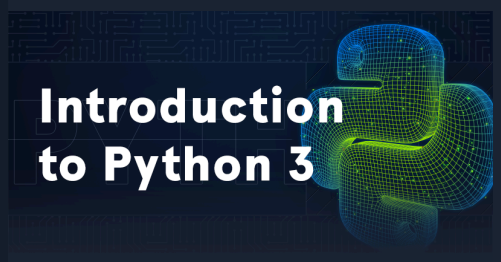


Intro to Assembly Language

24 Sections | Medium | General

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

100% Completed



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

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

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

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

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

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

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.

84.21% 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.

100% Completed

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

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.

100% Completed

Password Attacks

22 Sections | Medium | Offensive

Passwords are still the primary method of authentication in corporate networks. If strong password policies are not in place, users will often opt for weak, easy-to-remember passwords that can often be cracked offline and used to further our access. We will encounter passwords in many forms during our assessments. We must understand the various ways they are stored, how they can be retrieved, methods to crack weak passwords, ways to use hashes that cannot be cracked, and hunting for weak/default password usage.

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

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.

100% Completed

Pivoting, Tunneling, and Port Forwarding

18 Sections | Medium | Offensive

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.

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.

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

Introduction to Deserialization Attacks

15 Sections | Hard | Offensive

In this module, we will explore deserialization attacks with specific examples in Python and PHP.

100% Completed

Attacking Authentication Mechanisms

20 Sections | Medium | Offensive

Authentication plays an essential role in almost every web application. If a vulnerability arises in the application's authentication mechanism, it could result in unauthorized access, data loss, or potentially even remote code execution, depending on the application's functionality. This module will provide an overview of various access control methods, such as JWT, OAuth, and SAML, and potential attacks against each.

90% Completed

Introduction to NoSQL Injection

12 Sections | Medium | Offensive

In this module, we will look at exploiting NoSQL injection vulnerabilities, specifically MongoDB, with examples in Python, PHP, and Node.JS.

100% Completed

Blind SQL Injection

16 Sections | Hard | Offensive

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

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

Game Hacking Fundamentals

12 Sections | Medium | Offensive

This module serves as an introduction to fundamental Game Hacking concepts. You will learn how to find and change memory values in a running game as well as explore other tools and techniques.

100% Completed

HTTPs/TLS Attacks

15 Sections | Medium | Offensive

This module covers details on Transport Layer Security (TLS) and how it helps to make HTTP secure with the widely used HTTPS. That includes how TLS works, how TLS sessions are established, common TLS misconfigurations, as well as famous attacks on TLS. We will discuss how to identify, exploit, and prevent TLS attacks.

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.

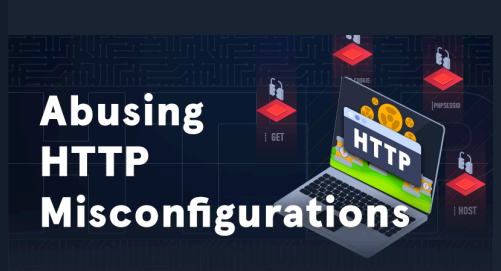
100% Completed

Advanced SQL Injections

12 Sections | Hard | Offensive

This module covers advanced SQL injection techniques with a focus on white-box testing, Java/Spring and PostgreSQL.

100% Completed

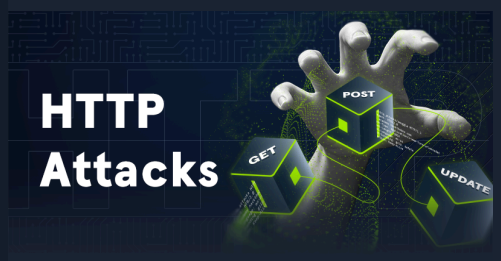


Abusing HTTP Misconfigurations

20 Sections | Hard | Offensive

This module covers three common HTTP vulnerabilities: Web Cache Poisoning, Host Header Vulnerabilities, and Session Puzzling or Session Variable Overloading. These vulnerabilities can arise on the HTTP level due to web server misconfigurations, other systems that have to be considered during real-world deployment such as web caches, or coding mistakes in the web application. We will cover how to identify, exploit, and prevent each of these vulnerabilities.

100% Completed



HTTP Attacks

18 Sections | Hard | Offensive

This module covers three HTTP vulnerabilities: CRLF Injection, HTTP Request Smuggling, and HTTP/2 Downgrading. These vulnerabilities can arise on the HTTP level in real-world deployment settings utilizing intermediary systems such as reverse proxies in front of the web server. We will cover how to identify, exploit, and prevent each of these vulnerabilities.

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.

100% Completed

Whitebox Attacks

15 Sections | Hard | Offensive

This module explores several web vulnerabilities from a whitebox approach: Prototype Pollution, Timing Attacks & Race Conditions, and those arising from Type Juggling. We will discuss how to identify, exploit, and prevent each vulnerability.

100% Completed

Injection Attacks

15 Sections | Medium | Offensive

This module covers three injection attacks: XPath injection, LDAP injection, and HTML injection in PDF generation libraries. While XPath and LDAP injection vulnerabilities can lead to authentication bypasses and data exfiltration, HTML injection in PDF generation libraries can lead to Server-Side Request Forgery (SSRF), Local File Inclusion (LFI), and other common web vulnerabilities. We will cover how to identify, exploit, and prevent each of these injection 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.

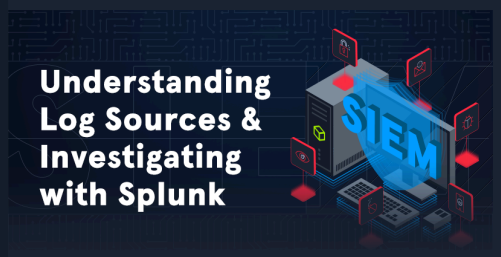
100% Completed

DACL Attacks I

7 Sections | Hard | Offensive

Discretionary Access Control Lists (DACLs), found within security descriptors, are a fundamental component of the security model of Windows and Active Directory, defining and enforcing access to the various system resources. This mini-module will cover enumerating and attacking common DACL misconfigurations, allowing us to escalate our privileges horizontally and vertically and move laterally across an Active Directory network.

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

Game Reversing & Modding

20 Sections | Medium | Offensive

This module serves as a follow-up to the Game Hacking Fundamentals module. You will learn how to persist Cheat Engine Scripts by scanning for byte arrays, editing game assemblies, utilising runtime hooking to modify games, and tampering with game network traffic using Burp.

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.

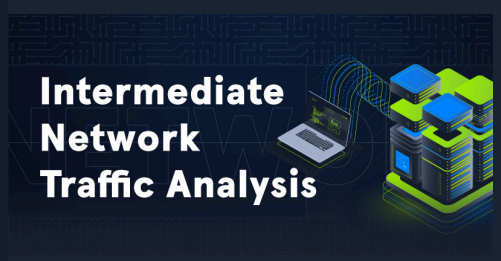
100% Completed

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#.

14.29% Completed

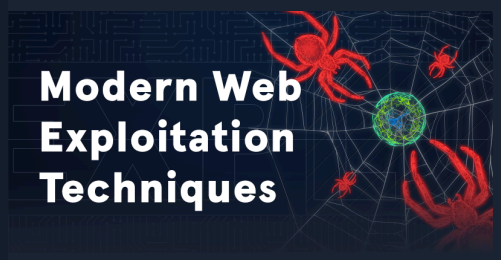


Intermediate Network Traffic Analysis

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

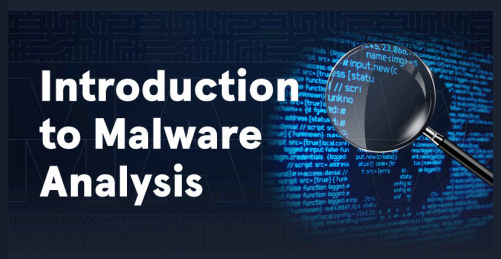


Modern Web Exploitation Techniques

18 Sections | Hard | Offensive

This module covers advanced web concepts and exploitation techniques, including performing DNS Rebinding to bypass faulty SSRF filters and the Same-Origin Policy, identifying and exploiting Second-Order vulnerabilities, and conducting common web attacks via WebSocket connections.

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

NTLM Relay Attacks

10 Sections | Hard | Offensive

The NTLM authentication protocol is commonly used within Windows-based networks to facilitate authentication between clients and servers. However, NTLM's inherent weaknesses make it susceptible to Adversary-in-the-Middle attacks, providing a significant attack vector. This module focuses on the various NTLM relay attacks that attackers use to compromise Active Directory networks.

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.

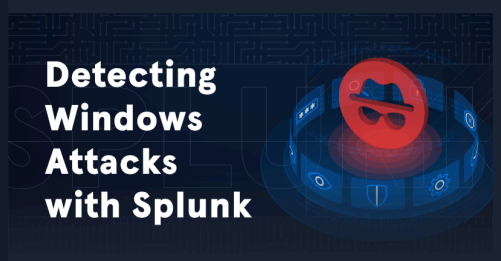
100% Completed

Advanced XSS and CSRF Exploitation

17 Sections | Medium | Offensive

Modern web browsers and applications utilize a variety of security measures to protect against CSRF and XSS vulnerabilities, rendering their exploitation more difficult. This module focuses on exploiting advanced CSRF and XSS vulnerabilities, identifying and bypassing weak and wrongly implemented defensive mechanisms.

100% Completed



Detecting Windows Attacks with Splunk

23 Sections | Medium | Defensive

This Hack The Box Academy module is focused on pinpointing attacks on Windows and Active Directory. Utilizing Splunk as the cornerstone for investigation, this training will arm participants with the expertise to adeptly identify Windows-based threats leveraging Windows Event Logs and Zeek network logs. Furthermore, participants will benefit from actual PCAP files associated with the discussed Windows and Active Directory attacks, enhancing their understanding of the respective attack patterns and techniques.

100% Completed

ADCS Attacks

19 Sections | Hard | Offensive

This module focuses on privilege escalation attacks by abusing misconfigurations in Active Directory Certificate Services.

100% 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

Parameter Logic Bugs

21 Sections | Hard | Defensive

This 'secure coding' module teaches how to identify logic bugs through code review and analysis, and covers three types of logic bugs caused by user input manipulation.

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.

100% Completed

Advanced Deserialization Attacks

13 Sections | Hard | Offensive

This module focuses on developing custom exploits for .NET deserialization vulnerabilities from a whitebox perspective.

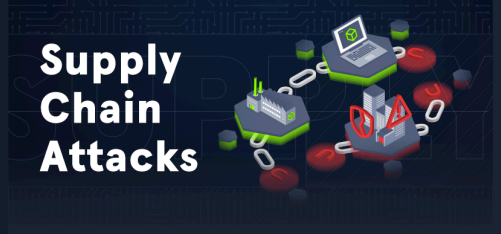
100% Completed

Intro to C2 Operations with Sliver

19 Sections | Hard | Offensive

Active Directory is present in over 90% of corporate environments and it is the prime target for attacks. This module covers the attack chain from getting the initial foothold within a corporate environment to compromising the whole forest with Sliver C2 and other open-source tools.

100% Completed



Supply Chain Attacks

18 Sections | Hard | Offensive

This module provides a detailed overview of Supply Chain Attacks, covering hardware and software aspects. It explores the impact of supply chains, the lifecycle of attacks, specific vulnerabilities, and mitigation strategies.

100% Completed

Intro to Whitebox Pentesting

18 Sections | Hard | Offensive

Whitebox penetration testing enables thorough testing to identify various hard-to-find vulnerabilities. This module covers the process of whitebox pentesting and follows that with a practical demo by exploiting an advanced code injection vulnerability.

100% Completed

User Behavior Forensics

21 Sections | Medium | Defensive

This module covers the critical aspects of user behavior analysis by exploring Windows artifacts. It is specifically designed for digital forensic analysts, incident responders, cybersecurity professionals, and law enforcement officers who seek to investigate the digital footprints left behind by users. It emphasizes examining user-centric artifacts that reveal user activities, preferences, and potential malicious behaviors.

100% Completed

Active Directory Trust Attacks

21 Sections | Hard | Offensive

Active Directory (AD) is the leading solution for organizations to provide identity and access management, centralized domain administration, authentication, and many other tasks. It is possible to connect Active Directory domains and forests via a feature called "trusts". Domain trusts can be set up for a variety of reasons such as resource sharing, centralized management, cross-forest collaboration, migration, enhanced security. With the introduction of trusts into any environment, they bring with them many inherent risks. As skilled AD pentesters we must understand how to enumerate and attack both intra-forest and cross-forest and be able to confidently explain the hardening considerations a customer needs to take into an account to mitigate some of the risk of introducing trusts into their operation environment.

100% Completed

Introduction to Windows Evasion Techniques

14 Sections | Hard | Offensive

In this module we will cover the basics of evading antivirus solutions (Windows Defender specifically) from an attackers point-of-view.

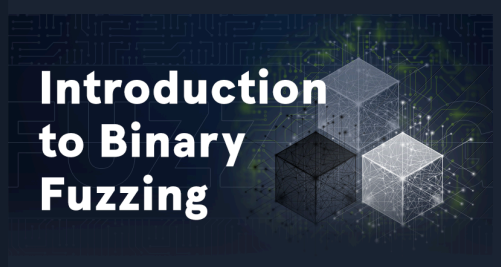
100% Completed

DACL Attacks II

9 Sections | Hard | Offensive

In this second module on Discretionary Access Control Lists (DACLs), we delve into sophisticated attack techniques and strategies within Windows Active Directory environments. Building on the foundation laid in DACL Attacks I, this module explores other DACL misconfigurations and their exploitation. We also introduce methods for detecting and mitigating these DACL-based attacks, equipping learners with both offensive and defensive skills crucial for safeguarding and compromising Active Directory networks.

100% Completed



Introduction to Binary Fuzzing

20 Sections | Hard | Offensive

Fuzzing is a powerful software testing technique that deliberately introduces chaos into your applications. By bombarding your code with unexpected or malformed inputs, fuzzing reveals hidden bugs and security vulnerabilities that might otherwise go unnoticed. This module will explore the history, theory, and practical applications of fuzzing, teaching you how to use this technique to find critical issues in software.

100% Completed

MSSQL, Exchange, and SCCM Attacks

19 Sections | Hard | Offensive

This module covers attacks targeting tightly incorporated technologies in Active Directory environments such as MSSQL, Exchange, and SCCM, and how to identify them.

100% Completed

API Attacks

13 Sections | Medium | Offensive

Web APIs serve as crucial connectors across diverse entities in the modern digital landscape. However, their extensive functionality also exposes them to a range of potential attacks. This module introduces API Attacks, with a specific focus on the OWASP API Security Top 10 - 2023.

100% Completed

Windows Lateral Movement

14 Sections | Medium | Offensive

Windows lateral movement involves techniques to navigate and control remote systems within a network, primarily after gaining initial access. It is crucial in offensive and defensive cybersecurity strategies, allowing attackers to escalate privileges, access sensitive data, and expand their network presence while helping defenders understand, identify, and mitigate such movements. This module delves into various lateral movement techniques on Windows systems, providing a comprehensive understanding and practical examples of executing and defending against these methods.

100% Completed

Attacking GraphQL

9 Sections | Medium | Offensive

GraphQL is a query language for APIs as an alternative to REST APIs. Clients are able to request data through GraphQL queries. If improperly configured or implemented, common web security vulnerabilities such as Information Disclosure, SQL Injection, and Insecure Direct Object Reference (IDOR) may arise.

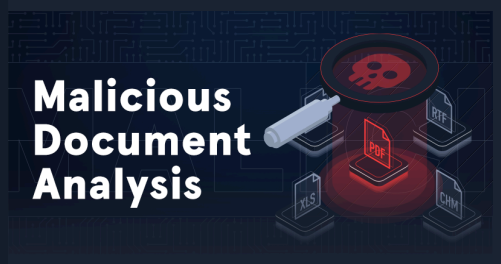
100% Completed

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

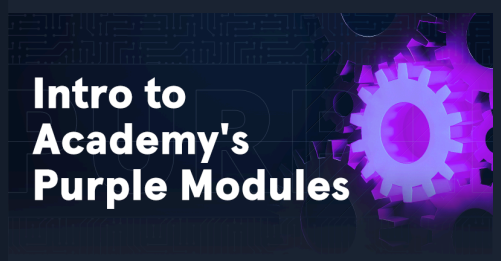


Malicious Document Analysis

22 Sections | Medium | Defensive

This module is focussed on understanding different document formats, and techniques for identifying and analyzing the threats posed by malicious documents. By the end of this course, you will be proficient in identifying various types of malicious documents, extracting and analyzing embedded objects, and applying both static and dynamic analysis techniques to uncover malicious behavior.

100% Completed

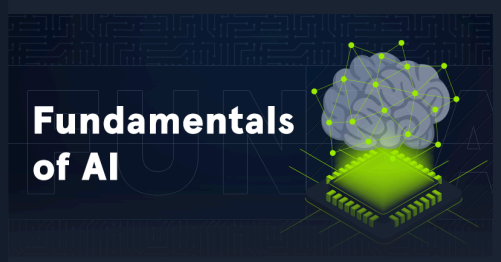


Intro to Academy's Purple Modules

12 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



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