Student Transcript

02-06-2026

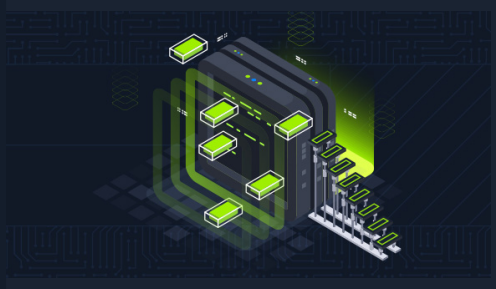
HTB ACADEMY

rian friedt

#738641

Certifications obtained: 2
Paths completed: 6
Targets compromised: 625
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.	September 28 2025
	HTB Certified Active Directory Pentesting Expert 15 Modules · Hard · Advanced Penetration Testing HTB Certified Active Directory Pentesting Expert (HTB CAPE) is a highly hands-on certification assessing candidates' skills in identifying and exploiting advanced Active Directory (AD) vulnerabilities. HTB CAPE certification holders will possess technical competency in both internal and external AD and Windows penetration testing, understanding complex attack paths, and employing advanced techniques to exploit them. HTB CAPE certification holders will demonstrate proficiency in executing sophisticated attacks abusing different authentication protocols such as Kerberos and NTLM and abusing misconfigurations within AD components such as ADCS, WSUS, Exchange, and Domain Trusts. Furthermore, they will be adept at leveraging specialized tools to exploit AD from Linux and Windows and utilizing Command and Control (C2) frameworks for post-exploitation operations.	January 26 2026

PATHS COMPLETED		PROGRESS
	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

AI Red Teamer

12 Modules Hard

The AI Red Teamer Job Role Path, in collaboration with Google, trains cybersecurity professionals to assess, exploit, and secure AI systems. Covering prompt injection, model privacy attacks, adversarial AI, supply chain risks, and deployment threats, it combines theory with hands-on exercises. Aligned with Google's Secure AI Framework (SAIF), it ensures relevance to real-world AI security challenges. Learners will gain skills to manipulate model behaviors, develop AI-specific red teaming strategies, and perform offensive security testing against AI-driven applications.

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

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.

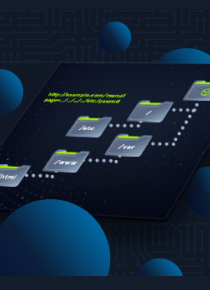
100% Completed

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.	62.5% 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
 **Linux Fundamentals** 30 Sections · Fundamental · General This module covers the fundamentals required to work comfortably with the Linux operating system and shell.	100% Completed
 **Network Enumeration with Nmap** 12 Sections · Easy · Offensive Nmap is one of the most used networking mapping and discovery tools because of its accurate results and efficiency. The tool is widely used by both offensive and defensive security practitioners. This module covers fundamentals that will be needed to use the Nmap tool for performing effective network enumeration.	100% Completed
 **Cracking Passwords with Hashcat** 14 Sections · Medium · Offensive This module covers the fundamentals of password cracking using the Hashcat tool.	14.29% 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
 **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
 **File Inclusion** 11 Sections · Medium · Offensive File Inclusion is a common web application vulnerability, which can be easily overlooked as part of a web application's functionality.	100% Completed
 **File Transfers** 10 Sections · Medium · Offensive During an assessment, it is very common for us to transfer files to and from a target system. This module covers file transfer techniques leveraging tools commonly available across all versions of Windows and Linux systems.	100% Completed

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.

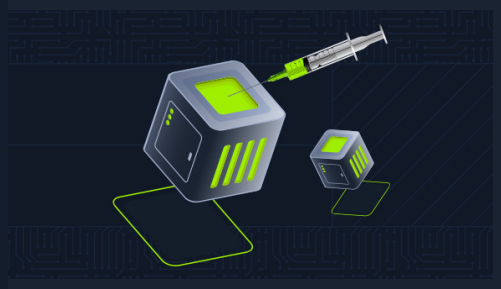
100% Completed

OSINT: Corporate Recon

23 Sections | Hard | Offensive

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.

100% Completed



SQL Injection Fundamentals

17 Sections | Medium | Offensive

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

100% Completed

Introduction to Networking

21 Sections | Fundamental | General

As an information security professional, a firm grasp of networking fundamentals and the required components is necessary. Without a strong foundation in networking, it will be tough to progress in any area of information security. Understanding how a network is structured and how the communication between the individual hosts and servers takes place using the various protocols allows us to understand the entire network structure and its network traffic in detail and how different communication standards are handled. This knowledge is essential to create our tools and to interact with the protocols.

100% Completed

Web Requests

8 Sections | Fundamental | General

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

100% Completed

Using the Metasploit Framework

15 Sections | Easy | Offensive

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

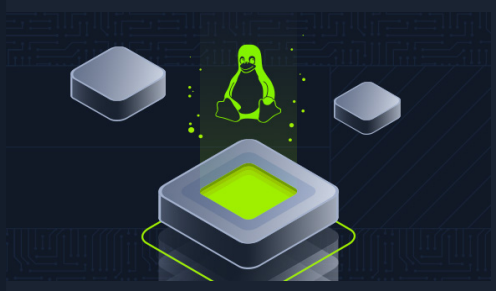
100% Completed

Windows Fundamentals

14 Sections | Fundamental | General

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

100% 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.

100% Completed

Attacking Web Applications with Ffuf

13 Sections | Easy | Offensive

This module covers the fundamental enumeration skills of web fuzzing and directory brute forcing using the Ffuf tool. The techniques learned in this module will help us in locating hidden pages, directories, and parameters when targeting web applications.

100% Completed

Login Brute Forcing

13 Sections | Easy | Offensive

The module contains an exploration of brute-forcing techniques, including the use of tools like Hydra and Medusa, and the importance of strong password practices. It covers various attack scenarios, such as targeting SSH, FTP, and web login forms.

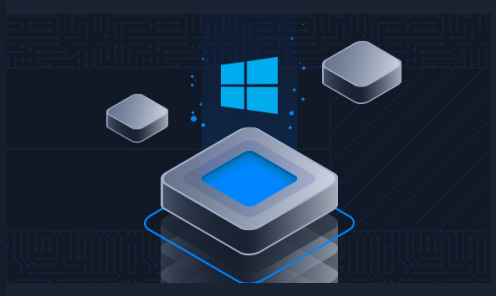
100% Completed

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

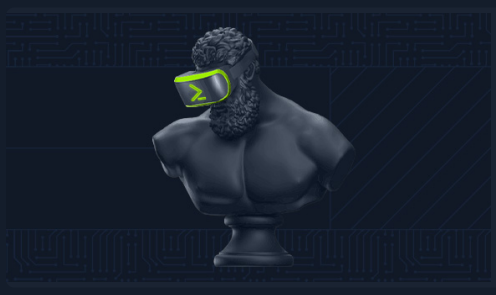


Windows Privilege Escalation

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.

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

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

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.

43.75% 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.

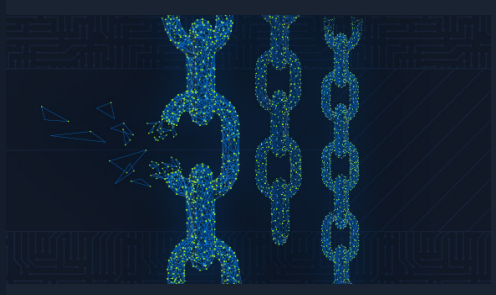
100% Completed

Getting Started

23 Sections | Fundamental | Offensive

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

100% Completed

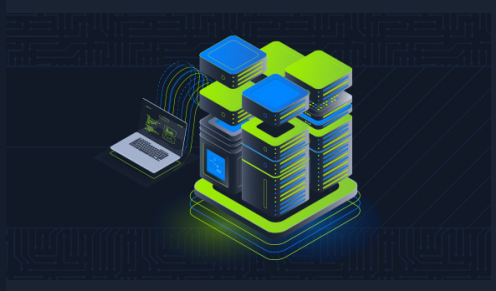


Broken Authentication

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.

28.57% 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

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.

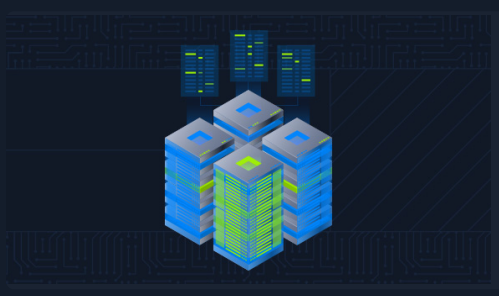
100% Completed

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.

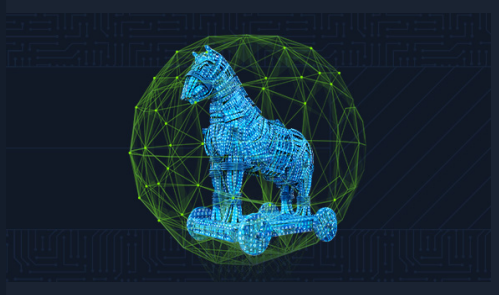
100% Completed

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.

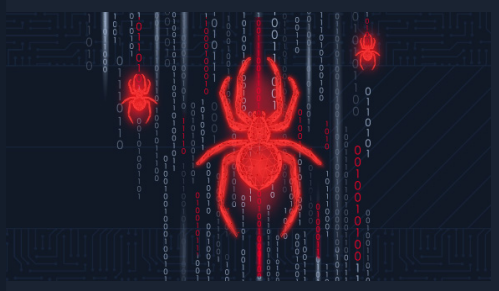
100% Completed

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

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

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

Password Attacks

26 Sections | Medium | Offensive

Passwords are still the primary method of authentication in corporate networks. If strong password policies are not enforced, users often choose weak, easy-to-remember passwords that can be cracked offline and leveraged to escalate access. As penetration testers, we encounter passwords in many forms during our assessments. It's essential to understand how passwords are stored, how they can be retrieved, methods for cracking weak passwords, techniques for using hashes that cannot be cracked, and how to identify weak or default password usage.

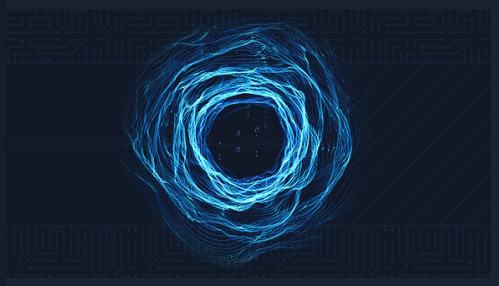
100% Completed

Incident Handling Process

11 Sections | Easy | General

Security Incident handling has become a vital part of every 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

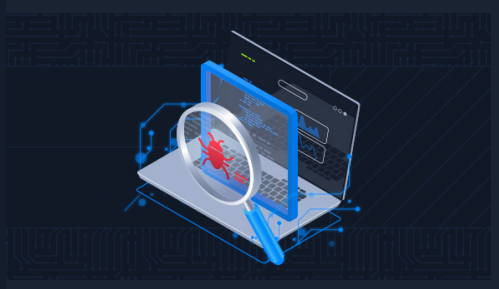


Pivoting, Tunneling, and Port Forwarding

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

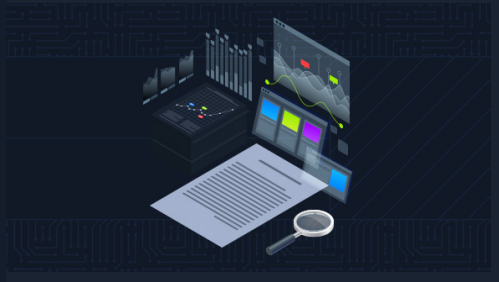


Bug Bounty Hunting Process

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.

16.67% Completed

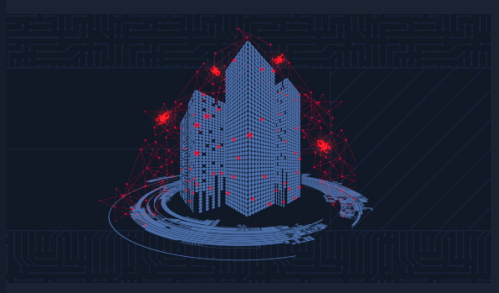


Documentation & Reporting

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.

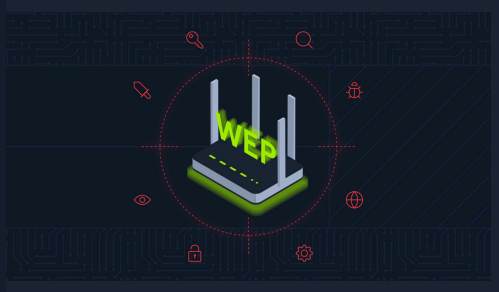
100% Completed

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.

38.46% 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.

69.23% 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.

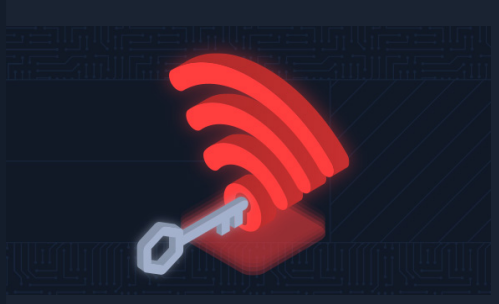
100% Completed

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

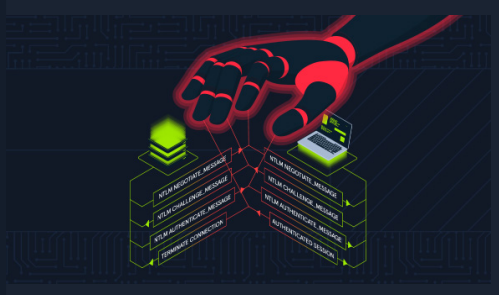


Wi-Fi Penetration Testing Basics

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.

93.75% 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.

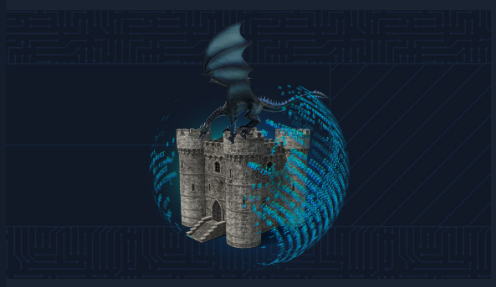
100% Completed

ADCS Attacks

19 Sections | Hard | Offensive

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

100% Completed

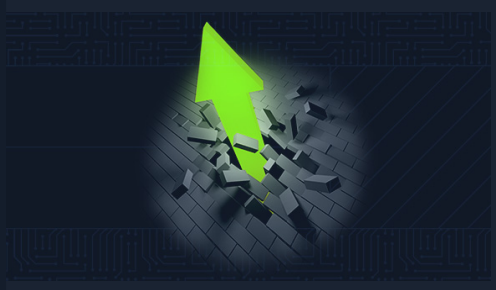


Intro to C2 Operations with Sliver

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



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.

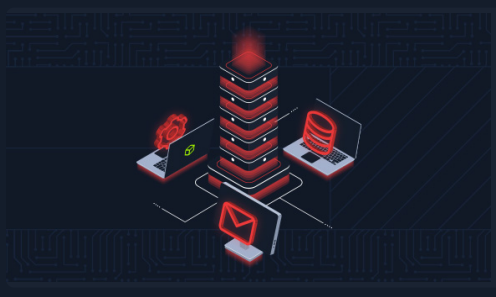
100% Completed

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



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

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.

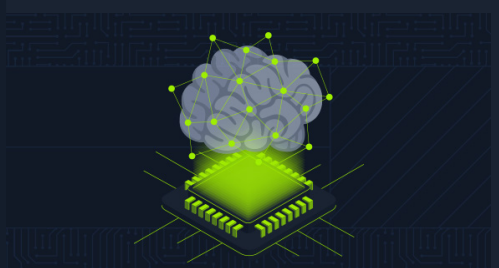
25% Completed

Network Foundations

12 Sections | Fundamental | General

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

100% Completed

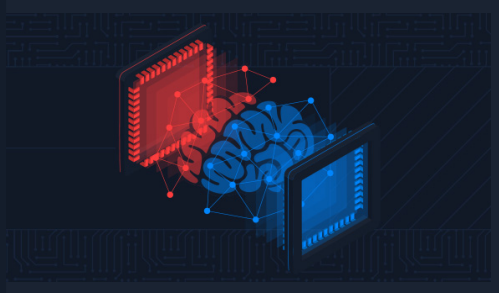


Fundamentals of AI

24 Sections | Medium | General

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

100% Completed



Applications of AI in InfoSec

25 Sections | Medium | General

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

100% 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 Red Teaming AI

11 Sections | Medium | Offensive

This module provides a comprehensive introduction to the world of red teaming Artificial Intelligence (AI) and systems utilizing Machine Learning (ML) deployments. It covers an overview of common security vulnerabilities in these systems and the types of attacks that can be launched against their components.

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.

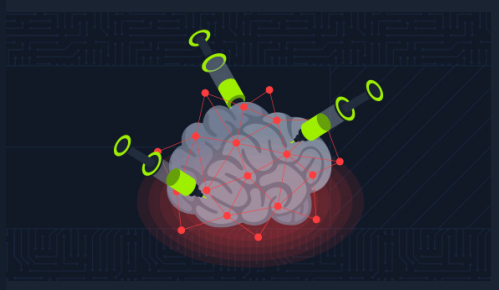
100% Completed

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

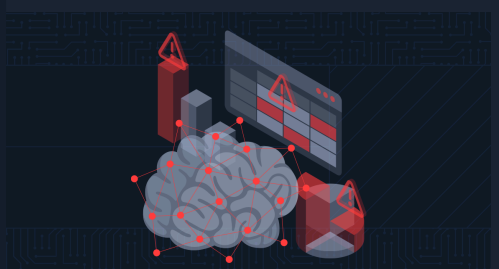


Prompt Injection Attacks

12 Sections | Medium | Offensive

This module comprehensively introduces one of the most prominent attacks on large language models (LLMs): Prompt Injection. It introduces prompt injection basics and covers detailed attack vectors based on real-world vulnerability reports. Furthermore, the module touches on academic research in the fields of novel prompt injection techniques and jailbreaks.

100% Completed



AI Data Attacks

25 Sections | Hard | Offensive

This module explores the intersection of Data and Artificial Intelligence, exposing how vulnerabilities within AI data pipelines can be exploited, ultimately aiming to degrade performance, achieve specific misclassifications, or execute arbitrary code.

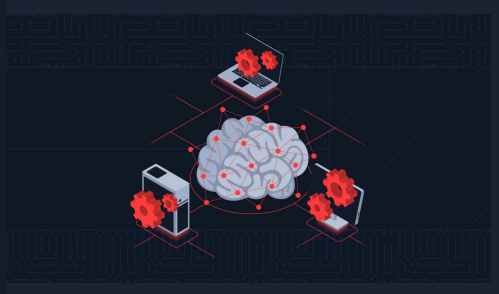
100% Completed

LLM Output Attacks

14 Sections | Medium | Offensive

In this module, we will explore different LLM output vulnerabilities resulting from improper handling of LLM outputs and insecure LLM applications. We will also touch on LLM abuse attacks, such as hate speech campaigns and misinformation generation, with a particular focus on the detection and mitigation of these attacks.

100% Completed

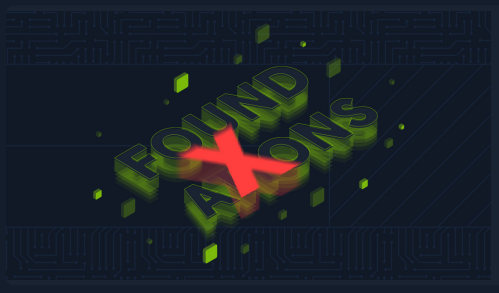


Attacking AI - Application and System

14 Sections | Medium | Offensive

In this module, we will explore security vulnerabilities in the application and system components of AI deployments. We will also discuss the Model Context Protocol (MCP), an orchestration protocol for AI deployments introduced in 2024, including a deep dive into how the protocol works and how security vulnerabilities may arise.

100% Completed

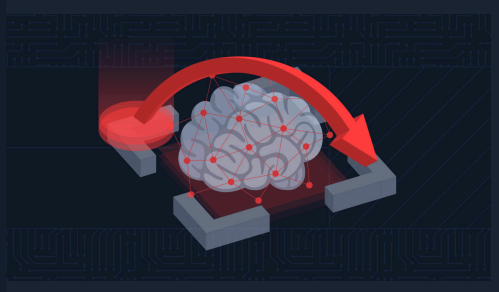


AI Evasion - Foundations

12 Sections | Medium | Offensive

This module explores the foundations of inference-time evasion attacks against AI models, showing how to manipulate inputs to bypass classifiers and force targeted misclassifications in white- and black-box settings.

100% Completed



AI Evasion - First-Order Attacks

23 Sections | Hard | Offensive

This module explores gradient-based adversarial attacks that manipulate neural network inputs at inference time, showing how to craft perturbations that cause misclassification through white-box access to model gradients.

100% Completed

AI Evasion - Sparsity Attacks

28 Sections | Hard | Offensive

This module explores sparsity-constrained adversarial attacks that minimize the number of modified input features rather than perturbation magnitude, showing how to craft targeted misclassifications by changing only the most impactful pixels through L0-focused optimization and saliency-guided feature selection.

100% Completed

AI Defense

21 Sections | Medium | Defensive

In this module, we will explore how to defend AI applications from the attack vectors discussed in the AI Red Teamer path. We will examine adversarial training, adversarial tuning, and LLM guardrails, including the fundamental concepts and practical implementation of these defensive measures.

100% Completed

AI Privacy

21 Sections | Medium | Defensive

This module explores privacy attacks against machine learning models and the differential privacy defenses that protect models from such attacks.

100% Completed