

Paths completed: 7
Targets compromised: 402
Ranking: Top 1%

PATHS COMPLETED

PROGRESS

<p>Bug Bounty Hunter</p> <p>20 Modules Medium</p>  <p>The Bug Bounty Hunter Job Role Path is for individuals who want to enter the world of Bug Bounty Hunting with little to no prior experience. This path covers core web application security assessment and bug bounty hunting concepts and provides a deep understanding of the attack tactics used during bug bounty hunting. Armed with the necessary theoretical background, multiple practical exercises, and a proven bug bounty hunting methodology, students will go through all bug bounty hunting stages, from reconnaissance and bug identification to exploitation, documentation, and communication to vendors/programs. Upon completing this job role path, you will have become proficient in the most common bug bounty hunting and attack techniques against web applications and be in the position of professionally reporting bugs to a vendor.</p>	<p>100% Completed</p> <div style="width: 100%; background-color: #28a745; height: 10px;"></div>
<p>Operating System Fundamentals</p> <p>2 Modules Easy</p>  <p>To succeed in information security, we must have a deep understanding of the Windows and Linux operating systems and be comfortable navigating the command line on both as a "power user." Much of our time in any role, but especially penetration testing, is spent in a Linux shell, Windows cmd or PowerShell console, so we must have the skills to navigate both types of operating systems with ease, manage system services, install applications, manage permissions, and harden the systems we work from in accordance with security best practices.</p>	<p>100% Completed</p> <div style="width: 100%; background-color: #28a745; height: 10px;"></div>
<p>Cracking into Hack the Box</p> <p>3 Modules Easy</p>  <p>To be successful in any technical information security role, we must have a broad understanding of specialized tools, tactics, and terminology. This path introduces core concepts necessary for anyone interested in a hands-on technical infosec role. The modules also provide the essential prerequisite knowledge for joining the main Hack The Box platform, progressing through Starting Point through easy-rated retired machines, and solving "live" machines with no walkthrough. It also includes helpful information about staying organized, navigating the HTB platforms, common pitfalls, and selecting a penetration testing distribution. Students will complete their first box during this path with a guided walkthrough and be challenged to complete a box on their own by applying the knowledge learned in the Getting Started module.</p>	<p>100% Completed</p> <div style="width: 100%; background-color: #28a745; height: 10px;"></div>
<p>Information Security Foundations</p> <p>12 Modules Easy</p>  <p>Information Security is a field with many specialized and highly technical disciplines. Job roles like Penetration Tester & Information Security Analyst require a solid technical foundational understanding of core IT & Information Security topics. This skill path is made up of modules that will assist learners in developing &/or strengthening a foundational understanding before proceeding with learning the more complex security topics. Every long-standing building first needs a solid foundation. Welcome to Information Security Foundations.</p>	<p>100% Completed</p> <div style="width: 100%; background-color: #28a745; height: 10px;"></div>



Basic Toolset

Basic Toolset

7 Modules Medium

In this path, modules cover the basic tools needed to be successful in network and web application penetration testing. This is not an exhaustive listing of all tools (both open source and commercial) available to us as security practitioners but covers tried and true tools that we find ourselves using on every technical assessment that we perform. Learning how to use the basic toolset is essential, as many different tools are used in penetration testing. We need to understand which of them to use for the various situations we will come across.

100% Completed



Local Privilege Escalation

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



Intro to Binary Exploitation

Intro to Binary Exploitation

4 Modules Hard

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

100% Completed



MODULE

PROGRESS



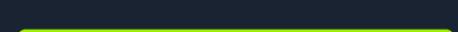
Intro to Academy

Introduction to Academy

8 Sections Fundamental General

This module is recommended for new users. It allows users to become acquainted with the platform and the learning process.

100% Completed



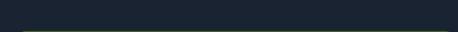
Linux Fundamentals

Linux Fundamentals

18 Sections Fundamental General

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

100% Completed



Windows Fundamentals

Windows Fundamentals

14 Sections Fundamental General

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

100% Completed



Web Requests

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





Setting Up

Setting Up

9 Sections Fundamental General

This module covers topics that will help us be better prepared before conducting penetration tests. Preparations before a penetration test can often take a lot of time and effort, and this module shows how to prepare efficiently.

100% Completed



Introduction to Web Applications

Introduction to Web Applications

17 Sections Fundamental General

In the Introduction to Web Applications module, you will learn all of the basics of how web applications work and begin to look at them from an information security perspective.

100% Completed



Getting Started

Getting Started

23 Sections Fundamental Offensive

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

100% Completed



Learning Process

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



Introduction to Networking

Introduction to Networking

12 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



File Transfers

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.

90% Completed



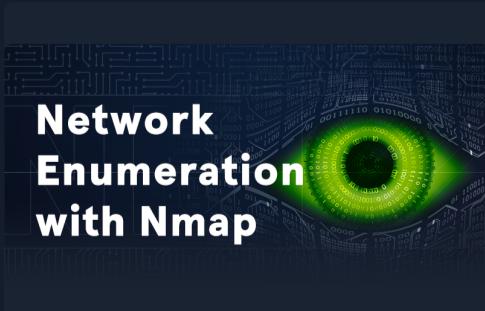
Introduction to Active Directory

Introduction to Active Directory

16 Sections Fundamental General

Active Directory (AD) is present in the majority of corporate environments. Due to its many features and complexity, it presents a vast attack surface. To be successful as penetration testers and information security professionals, we must have a firm understanding of Active Directory fundamentals, AD structures, functionality, common AD flaws, misconfigurations, and defensive measures.

100% Completed



Network Enumeration with Nmap

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



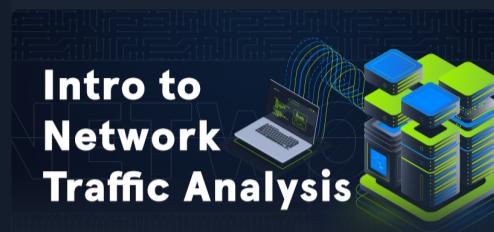


Stack-Based Buffer Overflows on Linux x86

13 Sections | Medium | Offensive

Buffer overflows are common vulnerabilities in software applications that can be exploited to achieve remote code execution (RCE) or perform a Denial-of-Service (DoS) attack. These vulnerabilities are caused by insecure coding, resulting in an attacker being able to overrun a program's buffer and overwrite adjacent memory locations, changing the program's execution path and resulting in unintended actions.

100% Completed



Intro to Network Traffic Analysis

15 Sections | Medium | General

Network traffic analysis is used by security teams to monitor network activity and look for anomalies that could indicate security and operational issues. Offensive security practitioners can use network traffic analysis to search for sensitive data such as credentials, hidden applications, reachable network segments, or other potentially sensitive information "on the wire." Network traffic analysis has many uses for attackers and defenders alike.

100% Completed



Introduction to Python 3

14 Sections | Easy | General

Automating tedious or otherwise impossible tasks is highly valued during both penetration testing engagements and everyday life. Introduction to Python 3 aims to introduce the student to the world of scripting with Python 3 and covers the essential building blocks needed for a beginner to understand programming. Some advanced topics are also covered for the more experienced student. In a guided fashion and starting soft, the final goal of this module is to equip the reader with enough know-how to be able to implement simple yet useful pieces of software.

100% Completed

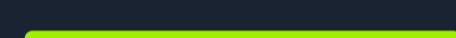


Stack-Based Buffer Overflows on Windows x86

11 Sections | Medium | Offensive

This module is your first step into Windows Binary Exploitation, and it will teach you how to exploit local and remote buffer overflow vulnerabilities on Windows machines.

100% Completed



Login Brute Forcing

11 Sections | Easy | Offensive

Learn how to brute force logins for various types of services and create custom wordlists based on your target.

100% Completed



JavaScript Deobfuscation

11 Sections | Easy | Defensive

This module will take you step-by-step through the fundamentals of JavaScript Deobfuscation until you can deobfuscate basic JavaScript code and understand its purpose.

100% Completed



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



Introduction to Bash Scripting

10 Sections | Easy | General

This module covers the basics needed for working with Bash scripts to automate tasks on Linux systems. A strong grasp of Bash is a fundamental skill for anyone working in a technical information security role. Through the power of automation, we can unlock the Linux operating system's full potential and efficiently perform habitual tasks.

100% Completed



File Inclusion

File Inclusion

11 Sections Medium Offensive

100% Completed

File Inclusion is a common web application vulnerability, which can be easily overlooked as part of a web application's functionality.

SQL Injection Fundamentals

SQL Injection Fundamentals

17 Sections Medium Offensive

100% Completed

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 backend database, or achieve code execution on the underlying server.

Active Directory Enumeration & Attacks

Active Directory Enumeration & Attacks

36 Sections Medium Offensive

97.22% Completed

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.

Using Web Proxies

Using Web Proxies

15 Sections Easy Offensive

100% Completed

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.

Vulnerability Assessment

Vulnerability Assessment

17 Sections Easy Offensive

100% Completed

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.

Password Attacks

Password Attacks

22 Sections Medium Offensive

86.36% Completed

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.

Windows Privilege Escalation

31 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.

96.77% Completed



Windows Privilege Escalation



DNS Enumeration Using Python



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 our 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



Using the Metasploit Framework



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



Penetration Testing Process



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.

93.33% Completed



Bug Bounty Hunting Process



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 and Reporting



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





Footprinting

Footprinting

20 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



Cracking Passwords with Hashcat

Cracking Passwords with Hashcat

14 Sections Medium Offensive

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

100% Completed



Attacking Common Services

Attacking Common Services

19 Sections Medium Offensive

Organizations regularly use a standard set of services for different purposes. It is vital to conduct penetration testing activities on each service internally and externally to ensure that they are not introducing security threats. This module will cover how to enumerate each service and test it against known vulnerabilities and exploits with a standard set of tools.

100% Completed



Information Gathering - Web Edition

Information Gathering - Web Edition

10 Sections Easy Offensive

This module covers techniques for identifying and analyzing an organization's web application-based attack surface and tech stack. Information gathering is an essential part of any web application penetration test, and it can be performed either passively or actively.

100% Completed



Shells & Payloads

Shells & Payloads

17 Sections Medium Offensive

Gain the knowledge and skills to identify and use shells & payloads to establish a foothold on vulnerable Windows & Linux systems. This module utilizes a fictitious scenario where the learner will place themselves in the perspective of a sysadmin trying out for a position on CAT5 Security's network penetration testing team.

100% Completed



Pivoting, Tunneling, and Port Forwarding

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



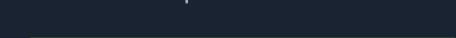
SQLMap Essentials

SQLMap Essentials

11 Sections Easy Offensive

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

100% Completed



Cross-Site Scripting (XSS)

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



File Upload Attacks

File Upload Attacks

11 Sections | Medium | Offensive

Arbitrary file uploads are among the most critical web vulnerabilities. These flaws enable attackers to upload malicious files, execute arbitrary commands on the back-end server, and even take control over the entire server and all web applications hosted on it and potentially gain access to sensitive data or cause a service disruption.

100% Completed



Command Injections

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



Web Attacks

Web Attacks

18 Sections | Medium | Offensive

This module covers three common web vulnerabilities, HTTP Verb Tampering, IDOR, and XXE, each of which can have a significant impact on a company's systems. We will cover how to identify, exploit, and prevent each of them through various methods.

100% Completed



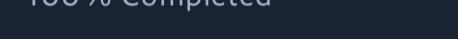
Attacking Common Applications

Attacking Common Applications

22 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



Linux Privilege Escalation

Linux Privilege Escalation

15 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 Enterprise Networks

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



Server-side Attacks

Server-side Attacks

19 Sections | Medium | Offensive

A backend that handles user-supplied input insecurely can lead to sensitive information disclosure and remote code execution. This module covers how to identify and exploit server-side bugs. This module introduces Server-Side Request Forgery (SSRF), Server-Side Template Injection (SSTI), and Server-Side Includes (SSI) injection attacks, alongside other server-side vulnerabilities.

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 currently 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 devastatingly impact an application's overall security.

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



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



Hacking WordPress

16 Sections | Easy | Offensive

WordPress is an open-source Content Management System (CMS) that can be used for multiple purposes.

100% Completed

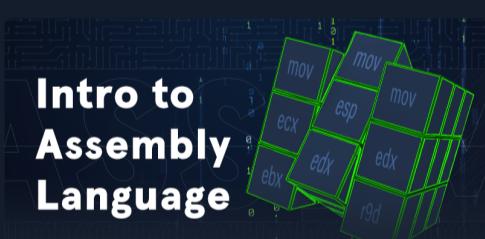


OSINT: Corporate Recon

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



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



Attacking Authentication Mechanisms

18 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 authentication methods, such as JWT, OAuth, and SAML, and potential attacks against each. Knowledge of modern authentication mechanisms will greatly benefit your penetration testing and bug bounty hunting journey when facing web applications.

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



