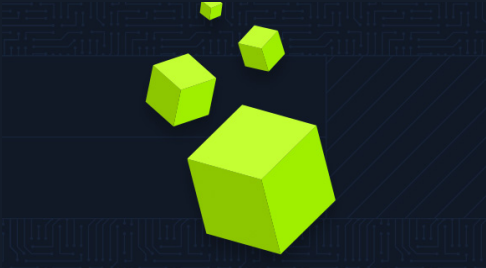


Targets compromised: 92
Ranking: Top 10%

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



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



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

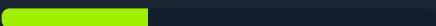


Introduction to Networking

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.

33.33% 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



Getting Started

23 Sections Fundamental Offensive

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

100% Completed

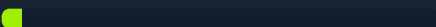


Setting Up

22 Sections Fundamental General

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

4.55% 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



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



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



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



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



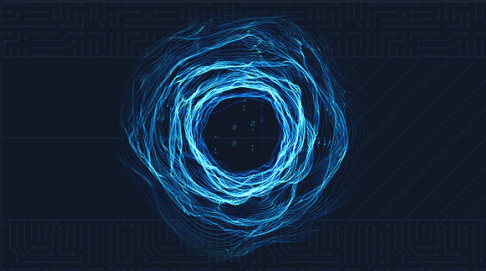
Password Attacks

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.

96.15% 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.

66.67% Completed

