



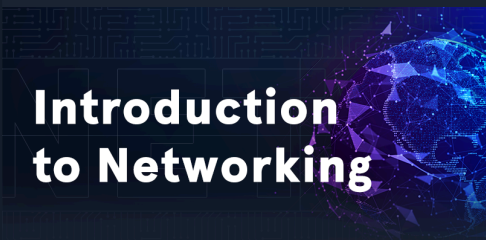
Targets compromised: 230

Ranking: Top 5%

MODULE

PROGRESS

	<div>Linux Fundamentals</div> <div>30 Sections Fundamental General</div> <p>This module covers the fundamentals required to work comfortably with the Linux operating system and shell.</p>	<div>100% Completed</div> <div></div>
	<div>Network Enumeration with Nmap</div> <div>12 Sections Easy Offensive</div> <p>Nmap is one of the most used networking mapping and discovery tools because of its accurate results and efficiency. The tool is widely used by both offensive and defensive security practitioners. This module covers fundamentals that will be needed to use the Nmap tool for performing effective network enumeration.</p>	<div>100% Completed</div> <div></div>
	<div>Introduction to Bash Scripting</div> <div>10 Sections Easy General</div> <p>This module covers the basics needed for working with Bash scripts to automate tasks on Linux systems. A strong grasp of Bash is a fundamental skill for anyone working in a technical information security role. Through the power of automation, we can unlock the Linux operating system's full potential and efficiently perform habitual tasks.</p>	<div>10% Completed</div> <div></div>
	<div>Active Directory LDAP</div> <div>12 Sections Medium Offensive</div> <p>This module provides an overview of Active Directory (AD), introduces core AD enumeration concepts, and covers enumeration with built-in tools.</p>	<div>100% Completed</div> <div></div>
	<div>Active Directory PowerView</div> <div>9 Sections Medium Offensive</div> <p>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.</p>	<div>100% Completed</div> <div></div>
	<div>File Transfers</div> <div>10 Sections Medium Offensive</div> <p>During an assessment, it is very common for us to transfer files to and from a target system. This module covers file transfer techniques leveraging tools commonly available across all versions of Windows and Linux systems.</p>	<div>100% Completed</div> <div></div>
	<div>SQL Injection Fundamentals</div> <div>17 Sections Medium Offensive</div> <p>Databases are an important part of web application infrastructure and SQL (Structured Query Language) to store, retrieve, and manipulate information stored in them. SQL injection is a code injection technique used to take advantage of coding vulnerabilities and inject SQL queries via an application to bypass authentication, retrieve data from the back-end database, or achieve code execution on the underlying server.</p>	<div>100% Completed</div> <div></div>



Introduction to Networking

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



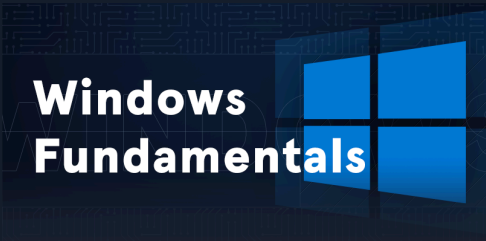
Using the Metasploit Framework

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



Windows Fundamentals

Windows Fundamentals

14 Sections Fundamental General

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

100% Completed



Attacking Web Applications with Ffuf

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

Login Brute Forcing

13 Sections Easy Offensive

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

100% Completed



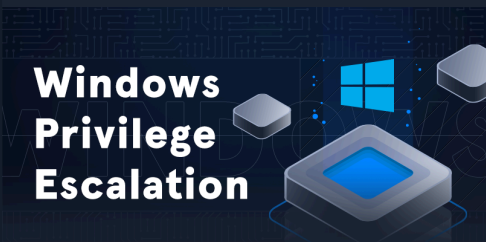
SQLMap Essentials

SQLMap Essentials

11 Sections Easy Offensive

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

100% Completed



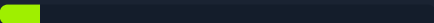
Windows Privilege Escalation









Windows Privilege Escalation


33 Sections Medium Offensive

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

9.09% Completed



	<h3>Introduction to Active Directory</h3> <div>16 Sections Fundamental General</div> <p>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.</p>	43.75% Completed
	<h3>Getting Started</h3> <div>23 Sections Fundamental Offensive</div> <p>This module covers the fundamentals of penetration testing and an introduction to Hack The Box.</p>	100% Completed
	<h3>Using CrackMapExec</h3> <div>27 Sections Medium Offensive</div> <p>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.</p>	100% Completed
	<h3>Penetration Testing Process</h3> <div>15 Sections Fundamental General</div> <p>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.</p>	100% Completed
	<h3>Cross-Site Scripting (XSS)</h3> <div>10 Sections Easy Offensive</div> <p>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.</p>	100% Completed
	<h3>Vulnerability Assessment</h3> <div>17 Sections Easy Offensive</div> <p>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.</p>	100% Completed
	<h3>Using Web Proxies</h3> <div>15 Sections Easy Offensive</div> <p>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.</p>	100% Completed
	<h3>Footprinting</h3> <div>21 Sections Medium Offensive</div> <p>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.</p>	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



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



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



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



Documentation and 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.

12.5% Completed



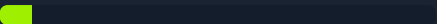
Attacking Enterprise Networks

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.

7.14% Completed



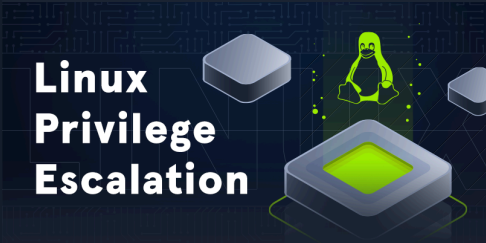
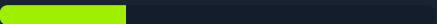
Active Directory BloodHound

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.

28.57% Completed



Linux Privilege Escalation

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.

3.57% Completed

