Ethical Hacking

Commitment:
4 weeks of study
10-20 hours/week

Ethical Hacking Basics

Discover ethical hacking principles, including techniques for information gathering and understanding target systems. You'll learn the foundations of ethical penetration testing and the legal implications of hacking.

Advanced Attack Strategies

Dive deeper into ethical hacking with network scanning, system hacking basics, and malware analysis. You'll explore sniffing techniques, social engineering tactics, and their impact on security.

Defense Evasion Techniques

Learn about DoS attacks, session hijacking, and methods to bypass security measures like IDS and firewalls. This knowledge is crucial for understanding and countering advanced cybersecurity threats.

About the Course

In this course, you will delve into the intriguing world of ethical hacking, a key component of cybersecurity. Starting with a solid foundation, you'll learn about the principles and scope of ethical hacking, understanding how to legally and effectively assess systems for vulnerabilities. This course offers a comprehensive look at the tools and techniques used by ethical hackers, ensuring you understand both the theory and practice of this critical cybersecurity skill.

As you progress, you'll explore advanced topics such as network scanning, system hacking, and the use of various types of malware. Practical sessions on sniffing and social engineering methods will enhance your understanding of how hackers exploit human and system weaknesses. This hands-on approach ensures you not only grasp the concepts but also know how to apply them in real-world scenarios.

The final part of the course focuses on advanced attack strategies and defense evasion. You'll learn about tactics like Denial of Service (DoS) attacks, session hijacking, and methods to evade intrusion detection systems, firewalls, and honeypots. This knowledge is vital for those seeking to understand and protect against sophisticated cybersecurity threats.

At the end, you will be able to

1. Understand and apply ethical hacking principles and methodologies.
2. Conduct network scanning and understand system vulnerabilities.
3. Analyze and implement strategies against various types of malware and social engineering attacks.
4. Execute advanced techniques for DoS attacks, session hijacking, and evading security systems like IDS and firewalls.

WEEK 1

Ethical Hacking Fundamentals

This week, you'll start your journey into ethical hacking. You'll learn about the principles and scope of ethical hacking, understanding the legal and ethical implications.

We'll cover techniques for information gathering and analyzing a target system's footprint. This foundational knowledge is essential for identifying and exploiting vulnerabilities in a controlled and legal manner.

WEEK 2

Network Scanning and System Hacking

Dive into network scanning tactics and basic system hacking methods. You'll explore different approaches to network enumeration and techniques for gaining unauthorized access to systems.

This week is crucial for understanding how attackers operate and how to defend against these methods.

WEEK 3

Malware and Sniffing

Focus on malware and sniffing this week, you'll study various types of malware, their impacts, and learn about network traffic interception techniques.

The session will also cover social engineering tactics, teaching you how attackers manipulate individuals to obtain confidential information. This knowledge is vital for both offense and defense in cybersecurity.

WEEK 4

Advanced Attack Strategies and Exam

In the final week, learn about advanced attack strategies, including DoS attacks and session hijacking. You'll also discover how to evade intrusion detection systems, firewalls, and honeypots.

This week is about synthesizing all you've learned and preparing for the Nucamp CyHacker exam, setting you up for success in the field of ethical hacking.