HOOYIA

E-HOOYIA

Offensive Security (Red Team)

Presented by:
Hooyia

+237 691435485
+237 697907096

e-hooyia.com

Bafoussam, Cameroon

contact@e-hooyia.com

Module 1: Offensive Security (Red Team)

Course Overview

This intensive module is designed to provide participants with a deep and practical understanding of how cyber-attacks are executed. The core philosophy of this course is to learn to think and operate like an attacker to proactively identify and neutralize vulnerabilities before they can be exploited by malicious actors.[1] The curriculum is highly hands-on, focusing on the practical application of offensive techniques across various attack vectors. By mastering the adversary's perspective, students will be uniquely equipped to build more resilient and robust defensive strategies. This approach moves beyond traditional, reactive security models, offering a more sophisticated and proactive methodology that is highly valued in the modern cybersecurity landscape.

Targeted Audience

This module is specifically crafted for professionals who aspire to specialize in offensive security roles. The skills and knowledge gained are essential for those pursuing careers as a Pentester (Penetration Tester), Red Teamer, Exploit Developer, or a Malware Analyst.[1]

Module Objectives

Upon successful completion of this module, participants will be able to:

- Demonstrate a foundational understanding of offensive security principles and the ethical guidelines of hacking.[1]
- Apply penetration testing methodologies and utilize industry-standard tools, including Metasploit, Burp Suite, and Nmap, to discover system vulnerabilities.[1]
- Conduct realistic and comprehensive attack simulations, such as phishing campaigns and network infiltration, to test an organization's security posture.[1]
- Analyze and create offensive malware, understanding its function, obfuscation techniques, and how to test its behavior in isolated environments like sandboxes.[1]
- Develop a basic grasp of exploit development to leverage identified vulnerabilities for testing purposes.[1]

Course Structure

The module is structured as an immersive training experience, combining theoretical knowledge with hands-on projects.

- **Week 1: Introduction to Offensive Security & Ethical Hacking**
  - Introduction to the offensive security landscape and its ethical considerations.
  - Setting up a virtual lab environment for safe and legal practice.
  - Overview of the Penetration Testing lifecycle and methodology.
  - Introduction to foundational tools like Nmap for reconnaissance and network scanning.
- **Week 2: Penetration Testing & Red Teaming Simulations**
  - Deep dive into the use of tools like Metasploit and Burp Suite for vulnerability exploitation.
  - Learning and practicing various Red Teaming attack simulations, including social engineering attacks like phishing and physical security considerations.[1]
  - Project: A controlled network penetration test from initial access to privilege escalation.
- **Week 3: Exploit Development & Malware Analysis**
  - Fundamentals of software vulnerability analysis and exploit creation.
  - An in-depth look into the anatomy of various types of offensive malware.[1]
  - Techniques for malware obfuscation to evade detection.

- Practical exercise: Deploying a test malware in a sandboxed environment to analyze its behavior.