Orange Cyberdefense

SensePost Training

Hands-On Hacking Fundamentals

BEGINNER LEVEL

Overview

Our introductory hacking course is focused on the fundamentals of the security landscape, how hackers think and the tools, tactics and techniques they use.

The course presents the background information, technical skills and basic concepts required to those desiring a foundation in the world of information security from an offensive perspective. Understanding the approaches attacker take will greatly enhance the defensive requirements and understanding required to defend against these attacks.

By the end of the course, you will have a good grasp of how vulnerabilities and exploits work, how attackers think about networks and systems and have compromised several of them from an infrastructure, web application and Wi-Fi. perspective.

Who should attend

People wanting to get started with penetration testing including defenders, developers or administrators looking to better understand how attacks work to better defend their systems.

This is also very useful for managers of technical teams looking to upskill in security.

Skills you'll learn

- Hacker Mindset
- Vulnerability discovery
- Web Application Hacking
- Wi-Fi Targeting

Training in a glance

4 core training modules

21 sub-modules and learning objectives

12 hands-on practicals

16 hours of training

Why our training is great

- Our training is provided by active penetration testers and security analyst
- Our training is hands-on with a course spilt of 40% theory and 60% practical
- We teach offensive methodologies to proactively enhance defensive thinking
- Each student gets their own lab environment during the course to practice real-world attacks

training@orangecyberdefense.com

orangecyberdefense.com

Orange Cyberdefense

SensePost Training

Hands-On Hacking Fundamentals (Continued)

BEGINNER LEVEL

Course Modules

1. Introduction To Hacking
   - Hacker mindset
   - Linux command line and usage
   - Risk and business related security
   - History and threat landscape

2. Understanding the Attack
   - Vulnerabilities VS Exploits
   - Attacker methodology
   - Target identification
   - Information gathering
   - Footprinting and fingerprinting
   - Vulnerability discovery
   - Exploits and payloads

3. Web Application Hacking
   - Web and HTTP fundamentals
   - Web application risks
   - Cookies / Hashes / Encoding
   - Person-in-the-Middle Proxies
   - OWASP Top 10

4. Wi-Fi Hacking
   - Wi-Fi fundamentals
   - Risks associated with Wi-Fi networks
   - Traffic monitoring and gathering
   - Capture and crack Wi-Fi password
   - Intercepting traffic

All modules contains several practical exercises and sub-objectives

Key take-aways

How to execute attacks based on an attacker methodology and hacker mindset

A sound technical understanding of the security landscape, vulnerabilities and exploits

Fundamentals required to attack common Web Application and Wi-Fi vulnerabilities

Prerequisites

No security or hacking experience is required. Basic exposure to the IT field is.

What you'll need

A laptop with a modern browser (Chrome or Firefox)

Zoom and/or Microsoft Teams installed

A Discord account

What you'll get

Access to our online class portal with lifetime access to the course resources and practical answer guides

Access to our realistic lab environment during the training to practice your newly taught skills

Value for your organisation

A greater understanding of the potential threat landscape and what to except from attackers

Increased security mindset that can actively be applied to everyday the everyday work environment and tasks at hand.

training@orangecyberdefense.com
orangecyberdefense.com