Orange Cyberdefense

SensePost Training

Enterprise Infrastructure Hacking

INTERMEDIATE LEVEL

Overview

This course is all about compromising companies through their infrastructure. It will take you on a journey of gathering information through to stealthy exploitation of critical infrastructure. Developed to transfer the methodologies we use for our external and internal network penetration testing and this course will provide a complete offensive understanding of attacking organisational infrastructure.

The course has a narrative starting with understanding your target, moving through initial compromise, then post exploitation and lastly going after the crown jewels.

By the end of this course you'll have a deep understanding of the potential threats organisational infrastructure could be vulnerable to and also expand your defensive thinking based on the offensive approaches taught.

Who should attend

This is aimed at intermediate penetration testers or technically minded people wanting to understand how to go about compromising their organisation to better defend it.

This course is also helpful for network defenders, architects and administrators.

Skills you'll learn

- Reconnaissance
- Vulnerability Discovery
- Exploiting Active Directory
- Attacker Methodology

Training in a glance

10 core training modules

44 sub-modules and learning objectives

21 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

Enterprise Infrastructure Hacking (Continued)

INTERMEDIATE LEVEL

Course Modules

1. Hacking mindset and methodology
   - How to think like a hacker
   - Methodology to target organisations
2. Intelligence Gathering
   - Target acquisition methodology
   - Open source intelligence gathering
3. Footprinting
   - Finding targets
   - Verification of targets
   - Mapping the attack surface
4. Fingerprinting
   - Exploring device and network technologies
   - Identify services and versions
   - Understanding the attack surface
5. Vulnerability Identification and Exploitation
   - Identification of vulnerabilities
   - Payloads and attack frameworks
6. Post-Exploitation
   - Privilege escalation
   - Understanding authentication mechanisms
   - Password cracking
   - Lateral movement techniques
7. Active Directory
   - Understanding Active Directory infrastructure
   - Modern AD exploitation
   - Domain compromise
8. Red Teaming Introduction
   - Introduction to red teaming
9. Blue Teaming Introduction
   - Introduction to blue teaming

All modules contains several practical exercises and sub-objectives

Key take-aways

Understanding how attackers target enterprise infrastructure

Navigating an internal network and finding vulnerabilities

How active directory networks can be abused

Prerequisites

A strong familiarity with Linux command line usage and basic security concepts.

A basic/entry-level understanding of organisational networks (Windows networks) and security would be beneficial.

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 and attack network during the training

Value for your organisation

A greater understanding of the potential threats your organization may be susceptible to and what to except from attackers

Increased security mindset that can actively be applied to the security and defense mechanisms in place.

training@orangecyberdefense.com

orangecyberdefense.com