Orange
Cyberdefense

orange™

SensePost Training

Introduction To Red Teaming

ADVANCED LEVEL

Red Team
SENSEPOST TRAINING

Overview

It is often said that penetration testers emulate other penetration testers rather than real threat actors, leaving organisations exposed to what they miss.

This course aims to change that. By combining our red teaming experience with two decades of teaching experience, we've put together a course to teach you how to test your organisations like a real criminal would; getting Domain Admin isn't the goal.

This course covers some of our unique red teaming approaches including; a repeatable methodology for AV and EDR bypasses and a focus on business system compromise with a fully functional SWIFT environment.

You will be challenged to adjust your methodology to become stealthy and explore alternative ways of reaching actions on objectives.

Who should attend

Penetration testers, network administrators, red/blue teams, security professionals, and IT security enthusiasts who have a need to acquaint themselves with real-world offensive tactics, techniques and tools.

Skills you'll learn

Phishing

AV Evasion

SWIFT Exploitation

Red Teaming

Training in a glance

9	core training modules
35	sub-modules and learning objectives
17	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

orange™

SensePost Training

Introduction To Red Teaming

ADVANCED LEVEL

Red Team
SENSEPOST TRAINING

Course Modules

1. Introduction to Red teaming
2. Reconnaissance
3. Stages of exploitation
4. Payload preparation
5. Foothold
6. Maintaining access
7. Precision
8. Data exfiltration
9. Action on objectives

All modules contains several sub-modules and practical exercises.

The above provides a summarised course outline, full course outline available on request.

Key take-aways

Greater understanding of the approaches real attackers take

An increased exposure to the tools and techniques used during red team engagements

Practical skills to achieve goals and execute exploit objectives

Prerequisites

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

At least 2 years of work in a penetrating testing role.

What you'll need

A laptop with a modern browser (Chrome or Firefox) and a Kali VM with OpenVPN installed

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

Increase your security team's skill set to that of world class red teamers with exposure to the latest techniques, tactics, and procedures.

Enable your defensive teams to understand real world risks and skills of attackers to better prepare and defend against their attacks.