Orange
Cyberdefense

orange™

SensePost Training

Advanced Active Directory Exploitation

ADVANCED LEVEL

Active Directory
SENSEPOST TRAINING

Overview

Defenders are becoming more aware of the tactics and techniques used by attackers. Common attacks performed in the past to compromise enterprise networks are being left behind due to the security industry improvements and awareness.

Although enterprise networks are now more secure, mature networks could continue making use of obsolete configurations that have been maintained for business requirements. This is the case of Active Directory. Additionally, new implementations and configurations can introduce new security issues that could aid an attacker in successfully compromising a company's network.

During the Advance Active Directory Exploitation (AADE) course, you will dive into an immersive, real-world simulated and isolated Active Directory enterprise network. We will take advantage of common misconfigurations we have found in real-world environments that can be abused to totally compromise multi-forest domains.

Who should attend

Penetration testers, network administrators and IT security enthusiasts who have a need to acquaint themselves with real-world offensive tactics to target Active Directory environments. This is also for defenders who are looking to enhance their understandings of these attacks.

Skills you'll learn

- AD Fundamentals
- Domain Enumeration
- Kerberos Attacks
- AD Take-Over

Training in a glance

11	core training modules
35	sub-modules and learning objectives
15	hands-on practicals
32	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

Orange
Cyberdefense

orange™

SensePost Training

Advanced Active Directory Exploitation

ADVANCED LEVEL

Active Directory
SENSEPOST TRAINING

Course Modules

1. Obtaining a foothold
2. Host Reconnaissance and Domain Enumeration
3. Local Privilege Escalation
4. Windows Authentication
5. Post-Exploitation
6. Lateral Movement
7. Security Descriptors
8. Kerberos
9. Kerberos Delegation
10. Domain Trusts
11. DCSync

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

Become familiar with Active Directory enterprise environments

Make use of built-in as well as public tools to conduct Active Directory attacks

Dive into a simulated real-life and isolated Active Directory environment

Prerequisites

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

2 years of work in a penetrating testing role.

A strong familiarity with Active Directory networks and administration.

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

Understanding the potential risks associated to internal and Active Directory networks.
Explore the threats your organization may be susceptible to from an internal perspective.

Practical exposure to exploitation of a multi-forest domain and internal network take-over leading to better defensive approaches.