+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated 09/30/2024

Sign up

CRTP© certification preparation training

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

2 days (14 hours)

Presentation

The Certified Red Team Professional (CRTP) course will give you the skills you need to understand and simulate advanced attacks on Active Directory environments.

Through this hands-on training, you'll become experts in identifying security vulnerabilities, simulating real attacks and exploiting vulnerabilities in a Windows environment.

You'll learn how to penetrate complex infrastructures using the most sophisticated techniques, while developing an in-depth understanding of lateral movements, privilege escalation and persistence mechanisms.

With CRTP certification, you'll be able to enhance your offensive security skills and play an active part in organizations' proactive defense against advanced persistent threats (APTs).

This training course will help you master the tools and techniques used by attackers in red team simulations, to demonstrate the risks present in your company's Active Directory systems.

Objectives

- Perform complex attacks on Active Directory.
- Understand and use lateral movement and privilege escalation techniques
- Handling and using red teaming tools
- Learn how to maintain persistent access and evade detection solutions
- Ready to take the Certified Red Team Professional (CRTP) certification

Target audience

- Ethical hackers
- Red teamers
- Sliders
- Offensive Security Auditors
- Cybersecurity consultants

Prerequisites

- A good understanding of computer networks
- Knowledge of Windows systems and Active Directory environments
- Basic knowledge of IT security (penetration testing, vulnerability exploitation)

Note: Ambient IT is not the owner of CRTP©, this certification belongs to AlteredSecurity ©.

CRTP© training program

Introduction to Red Teaming

- Red Teaming definition
- Strategic objectives
- Attack cycle: Planning, reconnaissance, exploitation, privilege escalation and persistence
- Types of simulated attacks :
  - Advanced persistent attacks (APT), targeted attacks on the AD
- Legal and ethical framework

Active Directory recognition

- Active Directory overview: essential structures
  - Organizational units, Security groups, Group policies
  - AD discovery methods (BloodHound, PowerView, SharpHound)
- Identify sensitive accounts (Domain Admins, Enterprise Admins)
- Information gathering using standard tools: native Windows commands (net user, net group)
- Passive recognition techniques: Exploiting network shares, DNS searches, and LDAP

Escalade de Privilèges

- Exploiting Group Policy Objects (GPOs)
- Escalation via service accounts
- UAC (User Access Control) bypass techniques
- Exploiting software vulnerabilities
- Analysis of configuration errors

Persistence in a Compromised Environment

- Creating Scheduled Tasks
- Abuse of Windows services
- Using backdoors in AD
- Advanced persistence techniques

Data Exfiltration

- Data tunneling
- Compressing and masking data
- Use of alternative communication channels
- Silent extraction via PowerShell
- Use of compromised accounts

Windows Environment Attack Simulation

- Simulation of a complete attack scenario
- Practical exercises on lateral movement
- Escalation of privileges
- Persistence workshop
- Simulated exfiltration

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% Practical, 40% Theory. Training material distributed in

to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.