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

Updated 09/30/2024

Sign up

CRTE© certification training

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

5 days (35 hours)

Presentation

The Certified Red Team Expert (CRTE) course will give you advanced skills for attacking and compromising corporate Windows infrastructures,
multi-domain and multi-forest.

You'll learn how to identify and exploit security vulnerabilities in modern Windows environments, including complex domains with inter-forest trust relationships.

This training course will immerse you in realistic scenarios where you'll have to use the most sophisticated techniques to carry out attacks, elevate your privileges, and rotate between different machines while bypassing the defenses in place.

This program will enable you to develop expertise in large-scale attacks such as the abuse of Kerberos protocols, long-term persistence in Active Directory via Golden and Silver tickets, and complex inter-forest attacks.

By mastering these techniques, you'll be able to simulate Red Team attacks on critical infrastructures, while providing strategic recommendations for improving the security of Windows environments.

This training course will not only prepare you to obtain CRTE certification, but also to enhance your offensive security skills and play a crucial role in protecting companies against sophisticated threats.

Objectives

- Carry out complex attacks on Active Directory environments
- Master lateral movement and privilege climbing techniques
- Understand and use advanced red teaming tools
- Learn how to maintain persistent access and evade detection solutions
- Be able to bypass security mechanisms
- Prepare for Certified Red Team Expert (CRTE) certification

Target audience

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

Prerequisites

- Good understanding of computer networks and protocols used in Windows environments
- In-depth knowledge of Windows Server systems and Active Directory environments
- Prior experience in offensive security (penetration testing, vulnerability exploitation)
- Experience with tools such as Bloodhound, Mimikatz, and PowerShell scripts would be an asset

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

CRTE© training program

Active Directory & Advanced Enumeration

- Introduction to Active Directory (concepts, domains, forests)
- Advanced enumeration techniques :
  - BloodHound
  - Powerview
  - ADRecon
- List of trust relationships between estates and forests
- Identification of privileged users and sensitive groups
- [PRACTICE]: Mapping a multi-domain and multi-forest AD environment

Domain Privilege Escalation & Code Execution

- Escalation of local privileges:
  - Exploiting Windows vulnerabilities: Token Impersonation, UAC Bypass
  - Abuse of SeImpersonatePrivilege

- Code execution through abuse of native :
  - WMI, PowerShell, Scheduled Tasks, GPOs
- Replay of identifiers : Pass-the-Hash and Pass-the-Ticket with Mimikatz
- [PRACTICE] Local privilege escalation and code execution with native tools

Domain Dominance & Persistence

- Antivirus bypass techniques, EDR and application whitelisting (AppLocker, Device Guard)
- Exploiting techniques such as DLL hijacking and binary padding
- Long-term persistence in the field :
  - Abuse of Golden/Silver Tickets, AdminSDHolder, DSRM, DCSync
  - Advanced techniques such as Skeleton Key and ACL abuse
- [PRACTICE] Bypassing countermeasures and implementing persistence methods

Lateral movement & pivoting

- Lateral movement techniques: PSExec, RDP, WinRM
- Bypassing firewall rules via pivoting on Windows machines
- Hunt for corporate secrets with built-in Windows tools
- [PRACTICE]: Lateral movement and exfiltration of sensitive data

Cross Domain Attacks & Cross Forest Attacks

- Escalating privileges in a domain with Kerberoast
- Exploiting trust-based relationships between estates and forests
- Cross-trust attacks and abuse of SID History
- Abuse of SQL Server trusts to escalate privileges
- [PRACTICE] Escalation of privileges in a domain and forests, abuse of SQL trusts

Defenses

- Privilege groups, security flags, and privileged account configurations
- Use of Privilege Administrative Workstations (PAW)
- Time-limited administration with JIT (Just-in-Time) and JEA (Just Enough Administration)
- Understanding the third-party model and the ESAE environment
- Leverage security features such as Credential Guard, WDAC, LAPS, and the Protected Users group

Deception

- Deception techniques in an Active Directory environment
- Use of false information, honeypots and other deception tools
- **[PRACTICE**] Deploying deception mechanisms in an AD environment

Companies concerned

This 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 course: 60% Practical, 40% Theory. Training material distributed in digital format 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.