Updated 09/30/2024

Sign up

CRTM© certification preparation training

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

5 days (35 hours)

Presentation

The Certified Red Team Master (CRTM) course offers you a unique opportunity to acquire cutting-edge skills for compromising and taking control of complex Windows infrastructures, spread across multiple forests and domains.

This training program will plunge you into advanced scenarios where you'll have to abuse Windows security mechanisms, bypass the most sophisticated defenses, and exploit inter-forest trust relationships.

You'll learn how to manipulate Kerberos tickets, execute multi-level privilege escalations, and perform lateral moves in highly secure environments.

With this training, you'll develop in-depth expertise in cross-forest attacks, credential extraction, delegation abuse and virtual server exploitation.

You'll master techniques such as anti-virus bypassing and ACL (Access Control List) manipulation, while learning how to compromise isolated or restricted environments.

By training with CRTM, you'll be able to simulate large-scale Red Team attacks, navigate complex environments while bypassing advanced defenses, and provide concrete recommendations for improving the security of critical infrastructures.

Objectives

- Carry out large-scale attacks in multi-forest and multi-domain environments
- Master advanced lateral movement and privilege escalation techniques
- Exploiting vulnerabilities in Kerberos privilege and ticket management systems
- Understand and manipulate Red Team tools to compromise isolated environments
- Prepare for Certified Red Team Master (CRTM) certification

Target audience

- Ethical hackers
- Experienced red teamers
- Slotters specialized in Windows environments
- Offensive Security Auditors
- Advanced cybersecurity consultants

Prerequisites

- Solid knowledge of computer networks and protocols used in Windows environments
- Mastery of Active Directory and Windows server environments
- Experience in offensive security and penetration testing in complex environments
- Familiarity with tools such as Bloodhound, Mimikatz, and PowerShell scripts would be a plus

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

CRTM© training program

Exploring areas and abuses of defense mechanisms

- Forest and sub-domain listing
- Analysis of secret management mechanisms
- Exploiting weaknesses in privilege management
- Local escalation of privileges
- Extraction of secrets without using known tools
- Bypassing local restrictions on target machines

Inter-forest pivoting and identifier exploitation

- Pivoting across forest boundaries
- Solving double-hop Kerberos problems
- Replay of inter-forest identifiers
- Extraction of credentials in clear text
- Using administration tools to elevate privileges
- Securing lateral movements in segmented environments

Exploiting delegations and escalating privileges

- Privilege delegation analysis
- Enterprise application operation
- Lateral movement via compromised delegations
- Use of in-house tools
- Escalation of privileges through modification of ACLs (Access Control Lists)
- Extraction of application credentials from remote servers

Abuse of advanced security mechanisms and crossing forest borders

- Bypassing antivirus (AV) solutions
- Using Kerberos tickets for lateral movement
- Managing and resolving Kerberos double-hop problems
- Climbing privileges in a children's forest
- Exploit delegations to elevate privileges up to domain administrator level
- Pivot between domains to access enterprise administration privileges

Abusing remote access points and modifying permissions

- Abusing PowerShell Remoting access points
- Modifying ACLs for privilege escalation
- List of application restrictions and how to get around them
- Exploiting delegation loopholes
- Data analysis and access to confidential documents
- Using administrative permissions

User simulation, payload creation and bypassing restrictions

- Creating payloads to bypass antivirus software
- User simulation to obtain an access point
- Bypass privilege access restrictions on target machines
- Exploiting MS Exchange permissions
- Identity theft and cross-domain movement
- Handling LCDs

Virtual server compromise and final exfiltration

- Abuse of virtual servers and offline domain controllers
- Extracting secrets from memory dumps
- Bypassing Windows Defender Application Guard (WDAG) restrictions
- Abuse of virtualization mechanisms
- Using NTLM to access machines attached to the domain
- Initiation and final exfiltration

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.