Updated on 12/17/2024

Sign up

CARTP certification training

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

2 days (14 hours)

Presentation

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

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

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 CARTP certification, you'll be able to enhance your offensive security skills, better protect cloud infrastructures and actively participate in organizations' proactive defense against persistent threats.

This course will help you master the tools and techniques used by attackers to simulate attacks on Azure and Azure Active Directory environments.

Objectives

- Execute complex attacks on Azure and AzureAD
- Understand and use lateral movement and privilege escalation techniques
- Learn how to maintain persistent access and evade detection solutions
- Understanding how to extract data from the Azure cloud
- Ready to take the Certified Azure Red Team Professional (CARTP) certification

Target audience

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

Prerequisites

- A good understanding of computer networks
- Knowledge of Azure systems, Azure AD and the Azure Cloud
- Basic knowledge of IT security (penetration testing, vulnerability exploitation)

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

CARTP© training program

Introduction to Azure and Azure ADirectory

- Understanding Azure and Azure AD
- understand their roles and the relationship between Azure AD and Azure
- Understanding **Azure Kill Chain**
- introduction to Azure architecture
- fine-tuning of various concepts
  - Subscription
  - ARM
  - The resources
  - Management Groups
  - Managed Identity

Recognition and discovery

- Understand the default permissions an Azure AD user has within a tenant.
- Find out how to validate an organization's e-mail credentials
- Using OSINT and unauthenticated enumeration techniques
- Gathering information on targets

Escalade de Privilèges

- Increasing privileges in Azure AD and Azure by abusing custom roles
- Understanding Dynamic Groups and abusing the membership rule to obtain dynamic group membership
- Understand how Abuse Custom Script Extension and RunCommand can be used to execute commands as SYSTEM

- Use of services
  - Automation accounts
  - Key Vaults
  - Storage Accounts
- Configuration error analysis

Persistence and defense

- abusive implementation of SSO using AZUREADSSOACC for persistence
- Azure AD Connect server criticality and how OS-level persistence can compromise on-premise and cloud infrastructure
- Deepen your knowledge of attacks such as Skeleton key in the cloud and Golden SAML attack
- Understanding continuous access evaluation and its impact on replay tokens
- review of the various MFA settings in Azure AD

Data Exfiltration

- Extraction of secrets from **Key vaults** by abusing managed identity
- Compressing and masking data
- Use of alternative communication channels
- Extraction of workstation passwords and tokens using Compromised Azure
- Extracting secrets from blob storage
- Extract secrets from deployment history

Lateral Movement in Azure and Azure AD

- Using Hybrid workers with runbooks to switch from Azure to local machines
- lateral movement from GitHub to Azure tenant
- Carry out attacks against applications using an application proxy to execute a lateral movement from the cloud to onprem
- Misuse of hybrid model to perform lateral movements on site to the cloud
- Using Intune to run commands on local machines

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 enrolment is finalized, the learner receives a self-assessment questionnaire enabling 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 with regard to the training to come, within the limits imposed by the format selected. This

The questionnaire also enables us to anticipate any connection or internal security problems (intra-company or virtual classroom) that 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.