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

Mis à jour le 30/09/2024

S'inscrire

Formation Préparation à la certification CRTP©

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

2 jours (14 heures)

Présentation

La formation Certified Red Team Professional (CRTP) vous permettra d'acquérir les compétences indispensables pour comprendre et simuler des attaques avancées sur des environnements Active Directory.

À travers cet enseignement pratique, vous deviendrez experts dans l'identification des failles de sécurité, la simulation d'attaques réelles et l'exploitation de vulnérabilités dans un environnement Windows.

Vous apprendrez à pénétrer des infrastructures complexes en utilisant les techniques les plus sophistiquées, tout en développant une compréhension approfondie des mouvements latéraux, de l'escalade de privilèges et des mécanismes de persistance.

Grâce à la certification CRTP, vous serez en mesure de renforcer vos compétences en matière de sécurité offensive et de participer activement à la défense proactive des organisations contre les menaces persistantes avancées (APT).

Cette formation vous aidera à maîtriser les outils et techniques utilisés par les attaquants dans le cadre de simulations red team, pour démontrer les risques présents dans les systèmes Active Directory de votre entreprise.

Objectifs

- Savoir exécuter des attaques complexes sur Active Directory.
- Comprendre et utiliser les techniques de lateral movement et d'escalade de privilèges
- Manipuler les outils de red teaming et les utiliser
- Apprendre à maintenir un accès persistant et à échapper aux solutions de détection
- Être prêt à passer la certification Certified Red Team Professional (CRTP)

Public visé

- Hackers éthiques
- Red teamers
- Pentesteurs
- Auditeurs en sécurité offensive
- Consultants en cybersécurité

Pré-requis

- Une bonne compréhension des réseaux informatiques
- Connaissance des systèmes Windows et des environnements Active Directory
- Connaissance de base en sécurité informatique (tests d'intrusion, exploitation de vulnérabilités)

Note : Ambient IT n’est pas propriétaire de CRTP©, cette certification appartient à AlteredSecurity ©.

Programme de la formation CRTP©

Introduction au Red Teaming

- Définition du Red Teaming
- Objectifs stratégiques
- Cycle d'une attaque : Planification, reconnaissance, exploitation, escalade de privilèges, et persistance
- Types d’attaques simulées :
  - Attaques persistantes avancées (APT), attaques ciblées sur l'AD
- Cadre légal et éthique

Reconnaissance Active Directory

- Vue d'ensemble d'Active Directory : Structures essentielles
  - Unités Organisationnelles, Groupes de sécurité, Politiques de groupe
- Méthodes de découverte d'AD (BloodHound, PowerView, SharpHound)
- Identifier les comptes sensibles (Domain Admins, Enterprise Admins)
- Collecte d’informations à partir d’outils standards : Commandes Windows natives (net user, net group)
- Techniques de reconnaissance passives : Exploitation des partages réseaux, recherches DNS, et LDAP

Escalade de Privilèges

- Exploitation des GPO (Group Policy Objects)
- Escalade via les comptes de service
- Techniques de bypass UAC (User Access Control)
- Exploitation des failles logicielles
- Analyse des erreurs de configuration

Persistance dans un Environnement Compromis

- Création de Scheduled Tasks
- Abus des services Windows
- Utilisation de backdoors dans AD
- Techniques de persistance avancées

Exfiltration de Données

- Tunneling des données
- Compresser et masquer les données
- Utilisation de canaux de communication alternatifs
- Extraction silencieuse via PowerShell
- Utilisation des comptes compromis

Simulation d’Attaque d’Environnement Windows

- Simulation d’un scénario d’attaque complet
- Exercices pratiques sur le lateral movement
- Escalade de privilèges
- Atelier de persistance
- Exfiltration simulée

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format

numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.