+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 CRTE©

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

La formation Certified Red Team Expert (CRTE) vous permettra d'acquérir des compétences avancées pour attaquer et compromettre des infrastructures Windows d'entreprise, multi-domaines et multi-forêts.

Vous apprendrez à identifier et à exploiter les failles de sécurité dans des environnements Windows modernes, comprenant des domaines complexes avec des relations de confiance inter-forêts.

Cette formation vous plongera dans des scénarios réalistes où vous devrez utiliser les techniques les plus sophistiquées pour mener des attaques, élever vos privilèges, et pivoter entre différentes machines tout en contournant les défenses mises en place.

Ce programme vous permettra de développer une expertise sur les attaques à grande échelle telles que l'abus des protocoles Kerberos, la persistance à long terme dans Active Directory via des tickets Golden et Silver, ainsi que les attaques inter-forêts complexes.

En maîtrisant ces techniques, vous serez capable de simuler des attaques de type Red Team sur des infrastructures critiques tout en fournissant des recommandations stratégiques pour améliorer la sécurité des environnements Windows.

Cette formation vous préparera non seulement à obtenir la certification CRTE, mais aussi à renforcer vos compétences en sécurité offensive et à jouer un rôle crucial dans la protection des entreprises contre les menaces sophistiquées.

Objectifs

- Savoir mener des attaques complexes sur des environnements Active Directory
- Maîtriser les techniques de mouvement latéral et d’escalade de privilèges
- Comprendre et utiliser des outils avancés de red teaming
- Apprendre à maintenir un accès persistant et à échapper aux solutions de détection
- Être capable de déjouer les mécanismes de sécurité
- Se préparer efficacement à la certification Certified Red Team Expert (CRTE)

Public visé

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

Pré-requis

- Bonne compréhension des réseaux informatiques et des protocoles utilisés dans les environnements Windows
- Connaissance approfondie des systèmes Windows Server et des environnements Active Directory
- Expérience préalable en sécurité offensive (tests d'intrusion, exploitation de vulnérabilités)
- Expérience avec des outils tels que Bloodhound, Mimikatz, et les scripts PowerShell serait un atout

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

Programme de la formation CRTE©

Active Directory & Enumeration Avancée

- Introduction à Active Directory (concepts, domaines, forêts)
- Techniques d'énumération avancée :
  - BloodHound
  - Powerview
  - ADRecon
- Énumération des relations de confiance entre domaines et forêts
- Identification des utilisateurs privilégiés et groupes sensibles
- [PRATIQUE] : Cartographier un environnement AD multi-domaines et multi-forêts

Domain Privilege Escalation & Exécution de Code

- Escalade de privilèges locaux :
  - Exploitation des failles Windows : Token Impersonation, UAC Bypass
  - Abus de SeImpersonatePrivilege

- Exécution de code via abus des fonctionnalités natives :
  - WMI, PowerShell, Scheduled Tasks, GPOs
- Rejeu d’identifiants : Pass-the-Hash et Pass-the-Ticket avec Mimikatz
- [PRATIQUE] Escalade de privilèges locaux et exécution de code avec des outils natifs

Domain Dominance & Persistence

- Techniques de contournement des antivirus, EDR et application whitelisting (AppLocker, Device Guard)
- Exploitation de techniques comme DLL Hijacking et binary padding
- Persistance à long terme dans le domaine :
  - Abus de Golden/Silver Tickets, AdminSDHolder, DSRM, DCSync
  - Techniques avancées comme le Skeleton Key et l'abus des ACLs
- [PRATIQUE] Bypass des contre-mesures et mise en place de méthodes de persistance

Mouvement Latéral & Pivotement

- Techniques de mouvement latéral : PSExec, RDP, WinRM
- Contournement des règles de pare-feu via pivotement sur des machines Windows
- Chasse aux secrets d'entreprise via les outils Windows intégrés
- [PRATIQUE]: Mouvement latéral et exfiltration de données sensibles

Cross Domain Attacks & Cross Forest Attacks

- Escalade des privilèges dans un domaine avec Kerberoast
- Exploitation des relations de confiance entre domaines et forêts
- Attaques cross-trust et abus des SID History
- Abus des trusts SQL Server pour escalader les privilèges
- [PRATIQUE] Escalade de privilèges dans un domaine et forêts, abus des trusts SQL

Defenses

- Groupes de privilèges, drapeaux de sécurité, et configurations des comptes privilégiés
- Utilisation des Privilege Administrative Workstations (PAW)
- Administration à durée limitée avec JIT (Just-in-Time) et JEA (Just Enough Administration)
- Compréhension du modèle en tiers et de l’environnement ESAE
- Exploitation des fonctionnalités de sécurité comme Credential Guard, WDAC, LAPS, et le groupe des Protected Users

Deception

- Techniques de déception dans un environnement Active Directory
- Utilisation de fausses informations, honeypots et autres outils de déception
- [**PRATIQUE**] Déploiement de mécanismes de déception dans un environnement AD

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.