+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 CRTM©

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

La formation Certified Red Team Master (CRTM) vous offre une opportunité unique d'acquérir des compétences de pointe pour compromettre et prendre le contrôle d'infrastructures Windows complexes, réparties sur plusieurs forêts et domaines.

Ce programme de formation vous plongera dans des scénarios avancés où vous devrez abuser des mécanismes de sécurité Windows, contourner les défenses les plus sophistiquées, et exploiter les relations de confiance inter-forêts.

Vous apprendrez à manipuler des tickets Kerberos, à exécuter des escalades de privilèges multi-niveaux, et à réaliser des mouvements latéraux dans des environnements hautement sécurisés.

Grâce à cette formation, vous développerez une expertise approfondie dans les attaques inter-forêts, l'extraction de credentials, l'abus des délégations et l'exploitation des serveurs virtuels.

Vous maîtriserez des techniques comme le bypass d'anti-virus et la manipulation des ACL (Access Control Lists), tout en apprenant à compromettre des environnements qui sont isolés ou restreints.

En vous formant au CRTM, vous serez capable de simuler des attaques Red Team de grande envergure, de naviguer à travers des environnements complexes tout en contournant les défenses avancées, et de fournir des recommandations concrètes pour améliorer la sécurité des infrastructures critiques.

Objectifs

- Mener des attaques à grande échelle sur des environnements multi-forêts et multi-domaines
- Maîtriser les techniques avancées de mouvement latéral et d'escalade de privilèges
- Exploiter des vulnérabilités dans les systèmes de gestion des privilèges et des tickets Kerberos
- Comprendre et manipuler des outils de Red Team pour compromettre des environnements isolés
- Se préparer efficacement à la certification Certified Red Team Master (CRTM)

Public visé

- Hackers éthiques
- Red teamers expérimentés
- Pentesteurs spécialisés en environnement Windows
- Auditeurs en sécurité offensive
- Consultants en cybersécurité avancée

Pré-requis

- Connaissance solide des réseaux informatiques et des protocoles utilisés dans les environnements Windows
- Maîtrise des environnements Active Directory et des serveurs Windows
- Expérience en sécurité offensive et tests d’intrusion dans des environnements complexes
- Familiarité avec des outils comme Bloodhound, Mimikatz, et les scripts PowerShell serait un plus

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

Programme de la formation CRTM©

Exploration des domaines et abus des mécanismes de défense

- Énumération des forêts et sous-domaines
- Analyse des mécanismes de gestion des secrets
- Exploitation des faiblesses dans la gestion des privilèges
- Escalade locale de privilèges
- Extraction de secrets sans utiliser d'outils connus
- Contournement des restrictions locales sur les machines cibles

Pivotement inter-forêts et exploitation des identifiants

- Pivotement à travers des frontières forestières
- Résolution des problèmes Kerberos double-hop
- Rejeu des identifiants inter-forêts
- Extraction des credentials en texte clair
- Utilisation des outils d'administration pour l'élévation des privilèges
- Sécurisation des mouvements latéraux dans les environnements segmentés

Exploitation des délégations et escalade de privilèges

- Analyse des délégations de privilèges
- Exploitation des applications d'entreprise
- Mouvement latéral via des délégations compromis
- Utilisation d'outils internes
- Escalade de privilèges grâce à la modification des ACL (Access Control Lists)
- Extraction des credentials d’applications sur des serveurs distants

Abus des mécanismes de sécurité avancés et traversée de frontières forestières

- Contournement des solutions antivirus (AV)
- Exploitation des tickets Kerberos pour le mouvement latéral
- Gestion et résolution des problèmes Kerberos double-hop
- Escalade de privilèges dans une forêt enfant
- Exploitation des délégations pour élever les privilèges jusqu’à l'administrateur de domaine
- Pivotement entre les domaines pour accéder aux privilèges d’administration d'entreprise

Abus des points d’accès à distance et modifications des permissions

- Abus des points d'accès PowerShell Remoting
- Modification des ACL pour l’escalade des privilèges
- Énumération des restrictions d’application et leur contournement
- Exploitation des failles dans les délégations
- Analyse des données et accès aux documents confidentiels
- Utilisation des permissions d’administration

Simulation d'utilisateurs, création de payloads et contournement des restrictions

- Création de payloads pour contourner les antivirus
- Simulation d'utilisateur pour obtenir un point d'accès
- Contournement des restrictions d’accès aux privilèges sur les machines cibles
- Exploitation des permissions MS Exchange
- Usurpation d'identité et mouvements inter-domaines
- Manipulation des ACL

Compromission des serveurs virtuels et exfiltration finale

- Abus des serveurs virtuels et des contrôleurs de domaine hors ligne
- Extraction de secrets à partir des dumps de mémoire
- Contournement des restrictions Windows Defender Application Guard (WDAG)
- Abus des mécanismes de virtualisation
- Utilisation de NTLM pour accéder aux machines jointes au domaine
- Initiation et exfiltration finale

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.