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

Mis à jour le 23/02/2024

S'inscrire

Formation Mandiant Red Team Ethical Hacker

4 jours (28 heures)

Présentation

Notre formation Red Team Ethical Hacker vous apprendra toutes les techniques et méthodes de pentesting afin de devenir un véritable expert Red Team. Vous serez, à l'issue de cette formation, capable de mener à bien de véritables attaques grandeur nature afin de découvrir et de corriger des vulnérabilités au sein des infrastructures de votre organisation.

Notre programme, inspiré des plus grands experts du domaine comme OffSec et Mandiant, aborde toutes les compétences nécessaires à la mise en place d'opérations de pentesting. Vous y apprendrez les concepts d'infrastructure et command control ainsi que de la reconnaissance et compromission initiale.

Notre formation ne vous apprendra pas seulement à réaliser des attaques sur des infrastructures, mais également à réaliser des rapports détaillés qui serviront à améliorer les stratégies de cybersécurités mises en place et en adopter d'autres, plus efficaces.

Vous aurez aussi l'occasion de tester les compétences acquises au cours de notre formation avec un atelier pratique de type Capture the Flag.

Objectifs

- Identifier et compromettre une cible
- Déployer des tactiques pour conserver l'accès à une cible compromise
- Exfiltrer des données sécurisées sans se faire détecter
- Écrire des rapports détaillés sur les vulnérabilités afin de les corriger

Public visé

- Ethical Hacker
- Experts en Cybersécurité

- Pentester

Pré-requis

- Expérience en Cybersécurité/pentesting
- Connaissance d'active directory
- Familiarité avec les scripts PowerShell

Programme de notre formation Red Team Ethical Hacker

INTRODUCTION AU RED TEAMING

- Qu'est-ce que le Red Teaming ?
- Différences avec le pentesting traditionnel
- Objectifs et bénéfices
- Règles d'engagement et aspects légaux
- Présentation des outils et méthodologie
- Différence entre les attaquants éthiques et les cybercriminels

INFRASTRUCTURE ET COMMAND & CONTROL (C2)

- Acquisition de domaines pour les opérations
- Configuration de l'infrastructure nécessaire
- Mise en place et sécurisation des serveurs C2
- Domain Fronting
- Redirecteurs HTTPS et DNS

RECONNAISSANCE INITIALE

- Reconnaissance passive : Whois, DNS et réseaux sociaux
- Reconnaissance active : Scanning de réseau et découverte de services
- Google Dorks et collecte d'informations
- Énumération des e-mails
- Analyse des données organisationnelles
- Les meilleures pratiques pour rester discret

COMPROMISSION INITIALE

- Techniques de compromission : Web Shells, injections SQL, Password Spraying
- Préparation et utilisation d'attaques d'ingénierie sociale
- Création de charges utiles malveillantes
- Distribution via e-mail ou sites web clonés
- personnalisation des vecteurs d'attaque
- Simulation d'attaques réelles

ÉTABLISSEMENT D'UNE TÊTE DE PONT

- Techniques d'obfuscation
- Évasion des antivirus
- Utilisation de frameworks comme .NET et PowerShell pour exécuter du code malveillant
- Exécution de commandes
- Scripts sans détection
- Opération post-exploitation et collecte de renseignements
- Stratégies pour maintenir l'accès et éviter la détection

ATTAQUES CONTRE ACTIVE DIRECTORY ET MOUVEMENT LATÉRAL

- Énumération et escalade de privilèges dans Active Directory
- Cartographier les relations AD
- Mouvement latéral et propagation dans un réseau
- Importance de l'opsec
- Simulation d'attaques

OBTENTION DE L'OBJECTIF ET RAPPORT

- Stratégies d'attaque de base de données
- Techniques pour l'exfiltration de données sensibles
- Préparation d'un rapport détaillé des vulnérabilités
- Retest et validation des mesures correctives
- Analyse de l'efficacité des actions et mesure de l'impact

CADRES ET MÉTHODOLOGIES

- Introduction aux cadres comme MITRE ATT&CK™ et Kill Chain
- Compréhension et utilisation de l'intelligence des menaces
- Planification et exécution d'émulations d'adversaires
- Analyse des indicateurs de compromission (IoC)
- Veille technologique et adaptation des stratégies

INFRASTRUCTURE D'ATTAQUE ET SÉCURITÉ OPÉRATIONNELLE

- Configuration et gestion des outils Red Team
- Sécurisation de l'infrastructure d'attaque
- Mise en place de redirecteurs
- Maintien de l'accès et la persistance
- Gestion des risques
- Réduction de l'empreinte de l'attaque

ANALYSE DE MALWARE ET INGÉNIERIE INVERSE

- Outils d'analyse de malware (Ghidra et IDA Pro)
- Ingénierie inverse de logiciels malveillants
- Formats de fichiers exécutables et structure interne
- Tactiques utilisées par les malwares
- Importance de l'analyse de malware

CAPTURE DU DRAPEAU EN ÉQUIPE ROUGE

- Organisation d'un exercice pratique de type Capture The Flag (CTF)
- Simulation d'une attaque complète sur une infrastructure prédéfinie
- Analyse en équipe des stratégies utilisées et des résultats obtenus
- Importance de la collaboration et de la communication au sein de l'équipe Red Team
- Retour d'expérience et identification des points d'amélioration

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.