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

Mis à jour le 01/03/2024

S'inscrire

Formation Préparation à la Certification GIAC GPEN©

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

Devenez pentesteur certifié avec la célèbre certification de GIAC : GPEN©. Notre formation GPEN© vous préparera étape par étape grâce à un programme complet couvrant toutes les compétences évaluées lors de l'examen.

En effet, nous commencerons ce cours en vous présentant les tests d'intrusion à travers divers aspects : la planification, le scoping, la reconnaissance et le scan. Vous apprendrez à maitriser les outils indispensables aux hackers éthiques : Nmap, Netcat, PowerShell ou encore Netgrok.

Nous vous enseignerons les méthodes d'intrusion présentes lors de l'épreuve comme les attaques par mot de passe, l'escalade des privilèges ou l'exploitation. Enfin, vous saurez rédiger des rapports de pentesting convaincant évaluant le risque commercial.

Par ailleurs, des stratégies et des méthodes vous seront divulguées pour que vous soyez préparés au passage de la certification GPEN©. Sachez également que nous préparons aussi la partie pratique : GX-PT©.

Objectifs

- Connaître les principales vulnérabilités et techniques d'intrusion système / web
- Être prêt pour le passage de la certification GPEN©

Public visé

- Pentesteur
- Hackers éthique
- Membre Red team
- Membre Blue team
- Auditeur
- Analyste en cybersécurité
- Consultant en cybersécurité

Pré-requis

- Expérience en protocole TCP/IP
- Maîtrise de l'anglais technique
- Connaissances de base en lignes de commande Linux et Windows

Pré-requis matériel

- Machine :
  - Au minimum, un processeur 64 bit Intel i5/i7 ou l'équivalent AMD avec 2 GHz ou plus
  - Un système d'exploitation récent et à jour
  - 8GB de RAM au minimum
  - 50GB d'espace de stockage libre ou plus
  - Une bonne connexion internet
  - Un droit d'administration local
- Logiciels :
  - Selon votre environnement, installer : VMware Workstation Pro, VMware Player, VMWare Fusion Pro ou VMware Fusion Player
  - Désactiver VM Ware Hyper V si vous êtes sur Windows
  - 7-Zip ou Keka installé
  - Les firewalls et les antivirus doivent être désactivés

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

Programme de la Préparation à la Certification GIAC GPEN©

Planification, scoping, reconnaissance et scan

- L'état d'esprit du pentesteur professionnel
- Mise en place d'une infrastructure de test d'intrusion de classe mondiale
- Créer des champs d'application et des règles d'engagement efficaces pour les tests d'intrusion
- Reconnaissance de l'organisation cible, de l'infrastructure et des utilisateurs
- Conseils pour un scan efficace
- Analyse des versions avec Nmap
- Réduction des faux positifs
- Netcat pour le pentester
- Tirer le meilleur parti de Nmap
- Scanner plus rapidement avec Masscan
- Empreinte du système d'exploitation, analyse des versions en profondeur
- EyeWitness

- Nmap en profondeur : Le moteur de script de Nmap

Accès initial, payloads et connaissance de la situation

- Obtenir un accès initial
- Deviner les mots de passe, les détruire et les remplir d'informations d'identification
- Exploitation et catégories d'exploitation
- Exploitation des services réseau et utilisation de Meterpreter
- Cadres de commande et de contrôle et choix de celui qui vous convient
- Utilisation de l'émulation adverse et du framework de la red team, Sliver
- Post-exploitation avec PowerShell Empire
- Génération de charges utiles dans Metasploit et Sliver
- Test d'intrusion présumée post-exploitation
- Connaissance de la situation sous Linux et Windows
- Extraire des informations utiles d'un hôte Windows compromis avec Seatbelt

Escalade des privilèges, persistance et attaques par mot de passe

- Méthodes et techniques d'escalade des privilèges sous Windows et Linux
- Identification des chemins d'attaque avec BloodHound
- Persistance et maintien de l'accès
- Conseils pour les attaques par mot de passe
- Récupération et manipulation de hachages sous Windows, Linux et d'autres systèmes
- Extraction de hachages et de mots de passe de la mémoire avec Mimikatz
- Craquage efficace de mots de passe avec John the Ripper et Hashcat
- Empoisonner la résolution de noms en multidiffusion avec Responder

Mouvements latéraux et rapport

- Mouvement latéral
- Exécution de commandes à distance
- Attaquer des protocoles réseau avec Impacket
- Anti-virus et contournement des outils de défense
- Contournement du contrôle des applications à l'aide des fonctions intégrées de Windows
- Mise en œuvre de relais de transfert de port via SSH pour des pivots sans Merciless
- Pivoter dans les environnements cibles avec C2
- Rapports efficaces et communication d'entreprise

Domination de domaine et annihilation d'Azure

- Protocole d'authentification Kerberos
- Kerberoasting pour l'escalade des privilèges de domaine et la compromission des informations d'identification
- Accès permanent au domaine administratif
- Évaluer et attaquer AD CS
- Obtention de NTDS.dit et extraction des hachages de domaine
- Attaques par ticket d'or et d'argent pour la persistance
- Autres attaques Kerberos, notamment Skeleton Key, Over-Pass-the-Hash et Pass-the-Ticket
- Escalade efficace des privilèges de domaine

- Reconnaissance d'Azure et d'Azure AD
- Attaques et destruction de mots de passe Azure
- Comprendre les permissions Azure
- Exécution de commandes sur des hôtes Azure
- Tunnels avec Ngrok
- Mouvement latéral dans Azure

Test d'intrusion et capture du drapeau

- Application des tests d'intrusion et des pratiques de piratage éthique
- Analyse détaillée de bout en bout pour trouver les vulnérabilités et les voies d'accès
- Exploitation pour prendre le contrôle des systèmes cibles
- Post-exploitation pour déterminer le risque commercial
- Merciless pivot
- Analyse des résultats pour comprendre le risque commercial et concevoir des mesures correctives

Stratégie et méthodes pour réussir l’examen

Module complémentaire (+1 jour) : Préparation à GX-PT©

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.