Pentesting - Réaliser des tests d'intrusion

Durée: 5 Jours **Réf de cours: GKPENTEST** **Version: 1.0** **Méthodes d'apprentissage: Classe à distance**

Résumé:

La formation "Pentesting – Réaliser des tests d'intrusion" vise à former des professionnels capables de simuler des attaques informatiques pour identifier les failles de sécurité d'un système, d'un réseau ou d'une application.
Elle couvre les aspects théoriques et pratiques, de la planification à la rédaction de rapports, en passant par l'exploitation des vulnérabilités et la recommandation de mesures correctives.

Mise à jour : 16.12.2025

Public visé:

RSSI, Techniciens, Auditeurs amens & faire du pentest, Administrateurs systmes et rseaux.

Objectifs pédagogiques:

- A l'issue de la formation les participants seront capables de :
- Comprendre les fondamentaux et le cadre juridique du pentesting
- Connaître les différentes phases d'un test d'intrusion
- Utiliser les outils et techniques d'analyse de pentesting
- Simuler des attaques

Pré-requis:

Prérequis :

- Connaissance de base en informatique, notions en analyse de données et de rédaction.

Test et certification

Contenu:

Journée 1 – Introduction et cadre d'un pentest :

Démarrage de la formation

- Présentation des enjeux, tour de table des participants, identification des attentes, présentation du déroulé pédagogique et des modalités d'évaluation.

Module 1 : Présentation générale, méthodologie et cadre réglementaire

- Définitions : audit vs test d'intrusion vs Red Team
- Phases d'un pentest (PTES / OSSTMM)
- Typologies d'audits : boîte noire, blanche, grise
- Typologie d'attaquants (script kiddie, hacktivistes, APT, etc.)
- Contraintes légales (CNIL, RGPD, LPM) et aspects déontologiques

LAB 1 : QCM de validation des connaissances initiales

Journée 2 – Collecte d'information (OSINT ; reconnaissance) :

Module 2 : Collecte d'informations

- Techniques d'OSINT et outils (theHarvester, Shodan, Maltego…)
- Reconnaissance passive et active
- Énumération de services : ports, bannières, DNS, AD
- Analyse Whois, DNSdumpster, Netcraft, etc.

LAB 2 : Collecte d'informations sur une cible simulée + exploration avec outils open source

Journée 3 – Analyse de vulnérabilités et ingénierie sociale :

Module 3 : Analyse de vulnérabilités

- Scan avec Nmap, Nessus, Nikto, OpenVAS
- Identification de CVE, Matching IOC
- Introduction au framework MITRE ATT;CK
- Notions d'ingénierie sociale et exploitation humaine

LAB 3 : Réalisation d'un scan complet sur un environnement vulnérable + exploitation de scénarios MITRE

Journée 4 – Exploitation offensive (Red Teaming) :

Module 4 : Exploitation

- Techniques d'exploitation selon le type de service : Web, réseau, OS, AD
- Recherche d'exploits : exploit-db, searchsploit
- Introduction à

Metasploit Framework (modules, payloads, exploit)

- Exploits classiques : Buffer overflow, injection, mauvaise configuration

LAB 4 :

- Lancement de plusieurs exploits sur des services ciblés
- Usage de Metasploit pour prise de contrôle
- Exploitation manuelle vs automatisée
- Exploits personnalisés dans un scénario simulé

Journée 5 – Post-Exploitation ; Reporting :

Module 5 : Post-Exploitation

- Enumération post-compromission : credentials, utilisateurs, chemins d'accès
- Élévation de privilèges (Linux/Windows)
- Techniques d'exfiltration (exfiltration de fichiers, mails…)
- Persistance, mouvements latéraux
- Évitement de détection : effacement des logs, outils LOLBAS

LAB 5 :

- Simulation complète : post-exploitation + rebond latéral sur un second système
- Objectif : compromettre l'AD et récupérer les données sensibles

Module 6 : Reporting professionnel

- Structure d'un rapport technique : vulnérabilités, preuves, scoring
- Rédaction de la synthèse exécutive (non technique)
- Recommandations correctives
- Atelier : étude critique de rapports types

LAB 6 : Rédaction d'un rapport complet basé sur le lab de pentest réalisé

- Présentation orale des rapports en binôme
- Feedback croisé entre participants
- Clôture de la formation

Méthodes pédagogiques :

Démarche pédagogique
-Alternance théorie/démonstrations/pratique encadrée
-Études de cas et mise en situation complète sur VM vulnérables
-Déroulé de scénarios offensifs de bout en bout
-Accompagnement à la rédaction de livrables (rapport technique et synthèse)
-Support PDF et ressources complémentaires accessibles après la formation

Répartition théorie / pratique

40 % Théorie
60 % Pratique (labs et simulations)

Accès à un espace de partage sécurisé contenant :
-Le support de cours officiel au format électronique
-Les QCM d'entraînement
-Les fichiers d'exercices et corrigés
-Les modèles de documents utilisés dans les travaux pratiques

Suivi qualité et évaluation
-Avant la formation : Questionnaire de positionnement / diagnostic envoyé aux participants afin de recueillir les attentes, le niveau initial et détecter d'éventuels besoins spécifiques (techniques, pédagogiques ou liés à l'accessibilité)
-Pendant la formation : Évaluation à chaud en fin de première journée pour recueillir les ressentis immédiats et ajuster l'animation pédagogique si besoin ,Quiz, exercices, cas pratiques, Mises en situation, Échanges pédagogiques avec le formateur
-À l'issue de la formation : Questionnaire de satisfaction à chaud (participant + formateur), Une attestation de suivi de fin de formation sera délivrée à chaque participant

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement