EduGroupe
Accompagner pour réussir

Hacking et sécurité - Niveau avancé

Référence : **SECHACKA** Durée : **5 jours (35 heures)** Certification : **Aucune**

Opcommerce

CONNAISSANCES PRÉALABLE

- Disposer d'une première expérience du hacking éthique
- Connaissances de TCP/IP
- La maîtrise de Linux en ligne de commande est un plus

PROFIL DES STAGIAIRES

- Ingénieurs / Techniciens
- Administrateurs systèmes / réseaux
- Développeurs

OBJECTIFS

- Comprendre comment organiser une veille sur la sécurité et savoir où rechercher des informations fiables
- Identifier les "faiblesses" des éléments constitutifs du SI par des prises d'empreintes
- Disposer des compétences techniques nécessaires pour réaliser différentes attaques et ainsi en comprendre les subtilités

CERTIFICATION PRÉPARÉE

- Aucune

MÉTHODES PÉDAGOGIQUES

- Pédagogie active et ancrée dans le réel : Alternance d'apports théoriques courts et d'ateliers pratiques ; Apprentissage par l'action et la simulation ; Études de cas issues du terrain ; Évaluation continue
- Formats et adaptation selon le contexte : Présentiel (format privilégié) ; Distanciel synchrone (classe virtuelle) ; Distanciel asynchrone
- Dimension innovante : CTF (Capture The Flag) gamifié ; Scénarios dynamiques ; Suivi analytique personnalisé ; Intégration IA et automatisation ; Post-formation
- Moyens pédagogiques et techniques mobilisés : Laboratoire de cybersécurité isolé ; Plateforme en ligne pour héberger supports, exercices, quiz et ressources techniques ; Supports pédagogiques numériques ;

FORMATEUR

- Consultant-formateur expert en cybersécurité offensive

MÉTHODES D'ÉVALUATION DES ACQUIS

- Avant la formation : test de positionnement ou de validation des prérequis
- Pendant la formation : évaluations formatives sous diverses formes (exercices, quiz...)
- Fin de formation : évaluation sommative sous forme de quiz général ou étude de cas ; évaluation satisfaction
- Après la formation : Evaluation à froid, un mois après la session de formation
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

1. Jour 1 - Introduction et veille (7 h)

2. Matin - Accueil, cadre et méthodologie (3 h)

- Cadre juridique du pentest, règles d'engagement, méthodologie (OSINT ? scan ? exploitation ? post-exploitation ? rapport)
- 💡 *Icebreaker + quiz de positionnement (10 questions rapides) pour homogénéiser le niveau*
- 💡 *Mini-conférence interactive (25 min) : cadre légal + échanges (brainstorming : risques rencontrés en entreprise)*
- 💡 *Étude de cas (30 min) : lecture d'un brief d'intervention (scénario client) ? discussion en petits groupes sur le périmètre et règles d'engagement*
- Debrief (15 min) : synthèse et checklist d'ouverture de mission

3. Après-midi - Introduction à la veille (4 h)

- Sources (CVE, CERTs, listes, MISP), agrégation, automatisation (feeds, scripts)
- 💡 *Démonstration live : config d'un flux MISP / agrégation RSS + alertes*
- 💡 *Atelier pratique (binômes) : créer un mini-dashboard de veille (fiches sources, alertes CVE) — 60 min*
- 💡 *Exercice / Scénario : recevoir une alerte CVE ? établir l'impact potentiel sur un SI fictif (30 min) puis restitution*
- 💡 *Quiz synthèse (10 Q) + plan d'action individuel pour la veille*

4. Jour 2 - Prise d'informations et OSINT (7 h)

5. Matin - OSINT avancé (3.5 h)

- Whois, DNS (zone transfer, DNS history), archives web, métadonnées, abuse DB, foot-printing
- 💡 *Démonstration : chaines d'outils OSINT (theHarvester, Shodan, Censys, recon-ng)*
- 💡 *Atelier guidé (individuel) : mission OSINT sur une cible lab (collecte, enrichment, classement preuves) — 90 min*
- 💡 *Peer review : échange entre participants sur les trouvailles (20 min)*

6. Après-midi - Automatisation et tri (3.5 h)

- Scripts Python simples, normalisation, enrichissement IA basique (ex. tagging)
- 💡 *Coding sprint (pairs) : écrire un script qui interroge Shodan + filtre par version vulnérable (1 h)*
- 💡 *Étude de cas : analyser jeu de données OSINT fourni ? produire une cartographie d'acteurs/infrastructures (60 min)*
- 💡 *Quiz/retour et liste de sources fiables à conserver*

7. Jour 3 - Scan et prise d'empreinte (7 h)

8. Matin - Discovery et fingerprinting (3.5 h)

- Nmap avancé (scripting NSE), techniques passives (Wireshark, p0f), identification versions services
- 💡 *Workshop Nmap : exercices pratiques (scans furtifs, timing, NSE) — 60 min*
- 💡 *Challenge : trouver 5 informations clés à partir d'un réseau cible isolé (30 min) — restitution*
- 💡 *Brainstorming : priorisation des vecteurs d'attaque selon la surface découverte*

9. Après-midi - Scan applicatif et cartographie (3.5 h)

- Nikto, Nuclei, Burp Suite basics, fuzzing léger
- 💡 *Lab Burp Suite : reconnaissance d'une application web vulnérable (OWASP Juice Shop) — 90 min*
- 💡 *Exercice pratique : écrire des templates Nuclei simples pour détection (45 min)*
- 💡 *Débrief & checklist : comment transformer la cartographie en priorités d'audit*

10. Jour 4 - Vulnérabilités et exploitation (7 h)

11. Matin - Vulnérabilités courantes (3.5 h)

- Anatomie d'une exploitation, PoC, risques business
- Mini-cours interactif (45 min) : présentation + démos
- 💡 *Atelier d'exploitation guidée : SQLi sur lab ? extraction contrôlée (60–75 min)*
- 💡 *Quiz technique (mix QCM et questions ouvertes) pour vérifier compréhension*

12. Après-midi - Exploitation et post-exploitation (3.5 h)

- Metasploit (usage avancé), exploitation manuelle, persistence, pivoting, collecte de preuves
- 💡 *Scenario exploit (petits groupes) : usage de Metasploit puis exploitation manuelle pour comparer approches (90 min)*
- 💡 *Exercice élévation : trouver vecteurs d'élévation locaux (45 min)*
- 💡 *Debrief red/blue léger : quelles mesures défensives auraient bloqué l'attaque ?*

13. Jour 5 - Atelier pratique final et contre-mesures (7 h)

14. Matin - Scénario complet (4 h)

- 💡 *Application des techniques apprises dans un lab isolé*
- 💡 *Exercice final (incarnation d'un petit pentest) : groupes de 3–4 ; livrables attendus : log d'actions, captures d'écran, preuves, mini-rapport technique. Temps: 3 h*
- Le formateur joue un rôle d'ordonnanceur/observateur, injection de contraintes (ex. temps limité, cible mouvante) pour complexifier

15. Après-midi - Restitution, remédiation et évaluation (3 h)

- Structure d’un rapport, priorisation des corrections, playbooks de remédiation
- 💡 *Restitutions orales : chaque groupe présente 10–15 min + Q/A (80–90 min)*
- 💡 *Atelier rédaction : correction croisée de rapports (peer review) ? amélioration (30 min)*
- Évaluation finale par le formateur : notation exercice + quiz final synthèse
- Fermeture : remise d’attestations et livrables (checklists, templates de rapport)

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour vos éventuels besoins d’aménagements, afin de vous offrir la meilleure expérience possible .