EduGroupe
Accompagner pour réussir

Pentesting - Réaliser des tests d'intrusion

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

Connaissances préalables

- Des notions en informatique et sécurité des systèmes d'information

Profil des stagiaires

- RSSI, SOC Manager, Analystes SOC, Consultant en cybersécurité ou toute personne en charge de la sécurité d'un système d'information d'entreprise

Objectifs

- 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
- Rédiger un rapport d'audit professionnel

Certification préparée

- Aucune

Méthodes pédagogiques

- Groupes de 4 à 12 personnes
- Apports théoriques illustrés d'exemples concrets
- Exercices pratiques
- Étude de cas fil rouge
- Accès à une documentation pédagogique numérique
- Utilisation d'outils collaboratifs (Miro, Wooclap) pour la co-construction
- Signature d'une feuille d'émargement pour attester de la présence à chaque demi-journée de formation

Formateur

- Consultant-formateur expert Pentest

Méthodes d'évaluation des acquis

- Participation et réalisation d'exercices tout au long de la formation
- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestations des compétences acquises et de fin de stage adressée à chaque participant

Contenu du cours

1. JOUR 1 - Fondamentaux et cadre du pentesting (7h)

2. Introduction et cadre légal (3h30)

- Définitions : test d'intrusion, audit de sécurité, Red Team
- Typologies : boîte noire, grise, blanche
- Règlementations (CNIL, RGPD, ePrivacy)
- Cadre légal et éthique : charte d'engagement, périmètre contractuel, responsabilité du pentester
- 💡 *Quiz d'introduction*
- 💡 *Étude de cas : contrat de pentest (analyse des clauses légales)*
- 💡 *Débat : éthique vs légalité*

3. Méthodologie et phases d'un pentest (3h30)

- Présentation des référentiels méthodologiques (PTES, OSSTMM, NIST)
- Les 6 phases : planification, reconnaissance, scanning, exploitation, post-exploitation, reporting
- Organisation d'un test d'intrusion en entreprise
- Présentation de l'environnement de lab (Kali Linux, VM vulnérables)
- 💡 *Schéma collaboratif des phases du pentest*
- 💡 *Quiz rapide (QCM)*
- 💡 *TP : installation et configuration de l'environnement de test*

4. JOUR 2 - Collecte d'informations et reconnaissance (7h)

5. OSINT et reconnaissance passive (3h30)

- Techniques de reconnaissance passive
- Outils : WHOIS, DNS, Shodan, Censys, Google Dorking
- Fingerprinting applicatif et technologique
- Risques liés à l'exposition d'informations publiques
- Démo d'outils OSINT
- 💡 *TP : cartographie de surface d'attaque*
- Étude de cas : cyberattaque médiatisée via infos publiques

6. Reconnaissance active et scan de vulnérabilités (3h30)

- Scan réseau : découverte d'hôtes et services (Nmap, Masscan)
- Détection de versions et fingerprinting
- Identification de vulnérabilités (Nessus, OpenVAS)
- Interprétation et priorisation des résultats
- 💡 *TP guidé avec Nmap*
- 💡 *TP semi-guidé avec Nessus/OpenVAS*
- Restitution collective : priorisation des failles trouvées

7. JOUR 3 - Exploitation des vulnérabilités (7h)

8. Techniques d’exploitation (3h30)

- Vulnérabilités courantes (OWASP Top 10) : injections SQL, XSS, CSRF, LFI/RFI
- Outils : Metasploit, SQLmap, Burp Suite
- Exploitation contrôlée dans un environnement lab
- Démo guidée : SQL Injection avec SQLmap
- 💡 *TP : exploitation OWASP Top 10 via Burp Suite*
- 💡 *Quiz : reconnaissance de failles sur scénarios réels*

9. Post-exploitation et élévation de privilèges (3h30)

- Objectifs de la post-exploitation : persistance, exfiltration, mouvement latéral
- Techniques d’élévation de privilèges (Linux & Windows)
- Exemples d’attaques réelles de type post-exploitation
- 💡 *TP : exploitation via Metasploit (session shell)*
- 💡 *TP : élévation de privilèges sur Linux & Windows*
- 💡 *Étude de cas : incident analysé (mouvement latéral)*

10. JOUR 4 - Simulations d’attaques et exercices pratiques (7h)

11. Attaques sur applications et systèmes (3h30)

- Attaques web : SQLi, XSS, upload malveillant, auth bypass
- Attaques réseau : brute force, MITM, exploitation SMB/RDP
- Sécurité des API et applications mobiles (introduction)
- 💡 *TP : exploitation d’une appli vulnérable*
- 💡 *TP : brute force avec Hydra*
- 💡 *Étude de cas : lien entre faille technique et risque métier*

12. Red Teaming & exercices pratiques (3h30)

- Différence pentest / Red Teaming
- Étapes d’une campagne Red Team simplifiée
- Organisation d’un CTF comme exercice de synthèse
- 💡 *Capture The Flag (individuel ou binômes)*
- Débrief collectif sur les stratégies employées
- 💡 *Discussion : rôle du Red Teaming dans la cybersécurité offensive*

13. JOUR 5 - Restitution et rapport d’audit (7h)

14. Structuration et communication des résultats (3h30)

- Structuration des résultats : preuves, captures, logs
- Méthodes de scoring (CVSS v3, impact métier)
- Bonnes pratiques de reporting (langage adapté, clarté, hiérarchisation)
- 💡 *Atelier : scoring CVSS d’une vulnérabilité*
- 💡 *Étude de cas : critique d’un rapport réel*
- 💡 *Quiz : bonnes pratiques de reporting*

15. Restitution finale et bilan (3h30)

- Méthodologie de rédaction d'un rapport professionnel
- Restitution orale : adapter son discours au public (technique / non-technique)
- Modèle de rapport et recommandations opérationnelles
- *TP final : rédaction d'un mini-rapport basé sur le CTF*
- *Restitution orale en groupe (jeu de rôle : consultants vs client)*
- Bilan de formation, remise des attestations et ressources

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