EduGroupe
Accompagner pour réussir

Hacking et sécurité - Les fondamentaux

Référence : **SECHACKF** Durée : **4 jours (28 heures)** Certification : **Aucune**

Opcommerce

CONNAISSANCES PRÉALABLE

- Aucun prérequis

PROFIL DES STAGIAIRES

- Ingénieurs / Techniciens
- Administrateurs systèmes / réseaux
- Toute personne intéressée par la pratique de la sécurité

OBJECTIFS

- Comprendre comment il est possible de s'introduire frauduleusement sur un système distant
- Savoir quels sont les mécanismes en jeu dans le cas d'attaques système
- Acquérir les compétences nécessaires pour mettre en place un dispositif global garantissant la sécurité des systèmes

CERTIFICATION PRÉPARÉE

- Aucune

MÉTHODES PÉDAGOGIQUES

- Pédagogie active et participative : Alternance d'apports théoriques, de démonstrations et d'ateliers pratiques ; Approche learning by doing ; Études de cas réels issus d'incidents récents ; Fil rouge pédagogique ; Évaluations formatives
- Formats et adaptation selon le contexte : Présentiel (inter Paris, Lyon, Nantes, Rennes, Toulouse, Pau/ intra partout en France) ; Distanciel synchrone ; Distanciel asynchrone(en option)
- Dmension innovante et immersive : Cyber Range virtuel ; Scénario fil rouge évolutif ; Simulations d'attaques en binôme attaquant / défenseur ; Outil d'auto-diagnostic de maturité sécurité ; Suivi post-formation
- Moyens pédagogiques et techniques mobilisés : Plateforme Internet dédiée ; Environnements de lab sécurisés ; Supports pédagogiques numériques

FORMATEUR

- Consultant-formateur expert en cybersécurité offensive et défensive, certifié (CEH, OSCP, ISO 27001 Lead Implementer)

MÉTHODES D'ÉVALUATION DES ACQUIS

- Avant la formation : test de positionnement ou de validation des prérequis
- Pendant la formation : évaluations formatives sous plusieurs formes (exercices, quiz)
- À la fin de la formation : évaluation sommative sous forme de quiz général ou étude de cas ; évaluation satisfaction
- Après la formation : évaluation 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 à la sécurité des réseaux (7h)

2. Matin (3h30) : Les fondamentaux des réseaux et de leur sécurité

- Rappels sur les protocoles réseau (TCP/IP, UDP, DNS, HTTP, HTTPS)
- Fonctionnement des architectures client-serveur et des modèles OSI / TCP-IP
- Identification des zones sensibles : périmètre, DMZ, flux inter-serveurs, segmentation
- Notions de pare-feu, NAT, VPN, proxy, IDS / IPS
- 💡 *Démonstration : capture et analyse de paquets (Wireshark)*

3. Après-midi (3h30) : Les bases de la sécurité réseau

- Vulnérabilités courantes dans les infrastructures (exposition de ports, configuration par défaut)
- Attaques sur les protocoles (ARP spoofing, DNS poisoning, sniffing, DoS/DDoS)
- Cartographie et reconnaissance réseau : scan de ports, découverte d'hôtes, fingerprinting
- 💡 *Atelier pratique (environnement simulé) : analyse d'un scan réseau et détection d'anomalies*

4. Jour 2 – Attaques à distance : comprendre et expérimenter (7h)

5. Matin (3h30) : Les vecteurs d'attaque à distance

- Étapes d'une attaque : reconnaissance, exploitation, élévation de privilèges, maintien de l'accès
- Exploitation de vulnérabilités connues (CVE, Metasploit)
- Phishing, brute force, exploitation RDP / SSH / SMB
- Introduction aux attaques web (XSS, SQLi, CSRF)
- 💡 *Démonstration : exploitation d'une faille sur un service distant simulé*

6. Après-midi (3h30) : Comprendre la compromission

- Injection de code, exploitation de buffer overflow, exécution de commande à distance
- Mécanismes de persistance et d'évasion (rootkits, obfuscation, tunneling)
- 💡 *Atelier guidé (sandbox) : observation d'un scénario de compromission et identification des traces dans les logs*
- Analyse de l'impact d'une intrusion sur le SI

7. Jour 3 – Attaques systèmes et compromission des environnements (7h)

8. Matin (3h30) : Vulnérabilités et attaques sur les systèmes

- Spécificités Windows et Linux : droits, services, mises à jour, partages, comptes
- Exploitation locale : élévation de privilèges, contournement de politiques de sécurité
- Outils d'exploitation (Mimikatz, PowerShell Empire, Linux PrivEsc)
- 💡 *Exercice pratique : détection d'une élévation de privilèges sur un poste compromis*

9. Après-midi (3h30) : Analyse post-attaque et forensic de premier niveau

- Méthodologie d'analyse d'un poste infecté
- Identification des artefacts et des journaux pertinents (logs, clés de registre, tâches planifiées)
- Premières actions de confinement et de remédiation
- 💡 *Étude de cas : analyse d'un poste compromis et reconstitution du scénario d'attaque*

10. Jour 4 – Sécuriser le système et construire une défense en profondeur (7h)

11. Matin (3h30) : Mise en place d'un dispositif global de sécurité

- Principes de la sécurité en couches : périmètre, réseau, poste, application, utilisateur
- Bonnes pratiques : durcissement (hardening) Windows / Linux, gestion des correctifs, supervision
- Gestion des identités et des accès (MFA, segmentation, PAM)
- Sauvegardes, chiffrement et PRA/PCA
- 💡 *Atelier pratique : élaboration d'un plan de sécurisation système global*

12. Après-midi (3h30) : Sécurité opérationnelle et amélioration continue

- Outils et solutions de supervision (EDR, SIEM, SOC)
- Gestion des vulnérabilités et des mises à jour (scans réguliers, scoring CVSS/EPSS)
- Surveillance et réaction : principes de la détection d'incidents
- Sensibilisation et politique de sécurité
- 💡 *Exercice final : simulation de mise en place d'une architecture sécurisée avant / après*
- 💡 *Quiz final + restitution orale du plan de sécurité*

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 .