EduGroupe
Accompagner pour réussir

Hacking et sécurité : les fondamentaux

Référence : **SECHSB** Durée : **2 jours (14 heures)** Certification : **Aucune**

Connaissances préalables

- Connaissances de Windows

Profil des stagiaires

- Administrateur système / réseau
- Ingénieurs / Techniciens
- RSSI
- Toute personne s'intéressant à la sécurité

Objectifs

- Comprendre et détecter les attaques sur un SI
- Exploiter et définir l'impact et la portée d'une vulnérabilité
- Corriger les vulnérabilités
- Sécuriser un réseau et intégrer les outils de sécurité de base

Certification préparée

- Aucune

Méthodes pédagogiques

- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- Mise à disposition d'un poste de travail par participant

Formateur

- Consultant-Formateur expert Sécurité offensive

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. JOUR 1

-

2. Introduction

- Définitions
- Objectifs
- Vocabulaire
- Méthodologie de test

3. Prise d'information

- Objectifs
- Prise d’information passive (WHOIS, réseaux sociaux, Google Hacking, Shodan, etc.)
- Prise d’information active (traceroute, social engineering, etc.)
- Bases de vulnérabilités et d’exploits

4. Réseau

- Rappels modèles OSI et TCP/IP
- Vocabulaire
- Protocoles ARP, IP, TCP et UDP
- NAT
- Scan de ports
- Sniffing
- ARP Cache Poisoning
- DoS / DDoS

5. JOUR 2

-

6. Attaques locales

- Cassage de mots de passe
- Elévation de privilèges
- Attaque du GRUB

7. Ingénierie sociale

- Utilisation de faiblesses humaines afin de récupérer des informations sensibles et/ou compromettre des systèmes
- Phishing
- Outils de contrôle à distance

8. Attaques à distance

- Introduction à Metasploit Framework
- Scanner de vulnérabilités
- Attaques d'un poste client
- Attaque d'un serveur
- Introduction aux vulnérabilités Web

9. Se sécuriser

- Les mises à jour
- Configurations par défaut et bonnes pratiques
- Introduction à la cryptographie
- Présentation de la stéganographie
- Anonymat (TOR)

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.