Hacking et sécurité : les fondamentaux

Référence : **SECHSB** Durée : **2 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• 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. • Corriger les vulnérabilités. • Exploiter et définir l'impact et la portée d'une vulnérabilité. • Sécuriser un réseau et intégrer les outils de sécurité de base.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité offensive

METHODE D'EVALUATION DES ACQUIS

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

CONTENU DU COURS

JOUR 1

Introduction

- Définitions
- Objectifs
- Vocabulaire
- Méthodologie de test

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

Réseau

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

JOUR 2

Attaques locales

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

Ingénierie sociale

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

Attaques à distance

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

Se sécuriser

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