Hacking et sécurité : avancé

Référence : **SECHSA** Durée : **5 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Administration Windows/Linux. • TCP/IP. • Utilisation de Linux en ligne de commande.

PROFIL DES STAGIAIRES

• Administrateurs systèmes / réseaux. • Consultants en sécurité. • Développeurs. • Ingénieurs / techniciens. • RSSI, DSI.

OBJECTIFS

• Comprendre et détecter les attaques sur un SI. • Corriger les vulnérabilités. • Définir l'impact et la portée d'une vulnérabilité. • Réaliser un test de pénétration. • Sécuriser un réseau et intégrer des outils de sécurité adéquats.

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

Introduction
- Rappel TCP/IP / Réseau Matériel
- Protos / OSI - Adressage IP

Introduction à la veille
- Vocabulaire
- BDD de Vulnérabilités et Exploits
- Informations générales

Prise d'informations
- Informations publiques
- Moteur de recherche
- Prise d'information active

Scan et prise d'empreinte
- Enumération des machines
- Scan de ports
- Prise d'empreinte du système d'exploitation
- Prise d'empreinte des services

Attaques réseau
- Idle Host Scanning
- Sniffing réseau
- Spoofing réseau
- Hijacking
- Attaques des protocoles sécurisés
- Dénis de service

Attaques système
- Scanner de vulnérabilités
- Exploitation d'un service vulnérable distant
- Elévation de privilèges
- Espionnage du système
- Attaques via un malware : Génération d'un malware avec Metasploit - Encodage de payloads
- Méthode de détection

Attaques Web

- Cartographie du site et identification des fuites d'informations
- Failles PHP (include, fopen, Upload,etc)
- Injections SQL
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Bonnes pratiques

Attaques applicatives

- Escape shell
- Buffer overflow sous Linux : L'architecture Intel x86 - Les registres - La pile et son fonctionnement - Présentation des méthodes d'attaque standards (Ecrasement de variables - Contrôler EIP - Exécuter un shellcode - Prendre le contrôle du système en tant qu'utilisateur root)

Challenge final

- Mise en pratique des connaissances acquises durant la semaine sur un TP final