EduGroupe
Accompagner pour réussir

Hacking et sécurité : avancé

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

Connaissances préalables

- 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
- Définir l'impact et la portée d'une vulnérabilité
- Réaliser un test de pénétration
- Corriger les vulnérabilités
- Sécuriser un réseau et intégrer des outils de sécurité adéquats

Certification préparée

- Aucune

Méthodes pédagogiques

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

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. Introduction

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

2. Introduction à la veille

- Vocabulaire
- BDD de Vulnérabilités et Exploits
- Informations générales

3. Prise d'informations

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

4. Scan et prise d'empreinte

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

5. Attaques réseau

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

6. 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

7. 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

8. 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)

9. Challenge final

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

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.