SQLI INSTITUT

400 FORMATIONS
POUR FAIRE LA DIFFÉRENCE

# HACKING & SÉCURITÉ AVANCÉ

## CODE STAGE : S0002

### OBJECTIFS

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

### DURÉE

5 jours

### PUBLIC

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

### PRÉ-REQUIS

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

### PROGRAMME

Module 1 : Introduction
Rappel TCP/IP / Réseau Matériel
Protos / OSI – Adressage IP

Module 2 : Introduction à la veille
Vocabulaire
BDD de Vulnérabilités et Exploits
Informations générales

Module 3 : Prise d'informations
Informations publiques
Moteur de recherche
Prise d'information active

Module 4 : Scan et prise d'empreinte
Enumération des machines
Scan de ports
Prise d'empreinte du système d'exploitation
Prise d'empreinte des services

Module 5 : Attaques réseau
Idle Host Scanning
Sniffing réseau
Spoofing réseau
Hijacking
Attaques des protocoles sécurisés
Dénis de service

Module 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

Module 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

Module 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)

Module 9 : Challenge final

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