Audit de sécurité de sites Web

Code : SE05 **Durée** : 4 jours **Classe** : Présentiel / à distance

Public

- Administrateurs systèmes et réseaux souhaitant maîtriser la sécurité offensive
- Développeurs web désireux de sécuriser leurs applications
- Responsables sécurité (RSSI) et consultants en cybersécurité
- Tout professionnel souhaitant se former à l'audit de sécurité web

Prérequis

- Avoir des bases solides en réseaux TCP/IP et en administration système
- Connaître les fondamentaux du développement web (HTML, PHP, SQL)
- Une expérience en administration Linux est recommandée

Objectifs

- Maîtriser les techniques de collecte d'informations et de reconnaissance
- Réaliser des scans de ports et prises d'empreinte des systèmes
- Identifier et exploiter les vulnérabilités réseau et système
- Détecter et corriger les principales failles web : SQL, XSS, CSRF, PHP

Programme détaillé

1- Introduction aux réseaux

- Rappels TCP/IP et modèle OSI
- Architecture réseau et matériel
- Protocoles réseau et adressage IP

2- Introduction à la veille

- Vocabulaire de la sécurité informatique
- Bases de données de vulnérabilités et d'exploits (CVE, NVD, Exploit-DB)
- Sources d'informations générales sur les menaces

3- Prise d'information

- Collecte d'informations publiques (OSINT)
- Utilisation des moteurs de recherche pour la reconnaissance
- Prise d'information active sur les systèmes cibles

4- Scan et prise d'empreinte

- Énumération des machines sur le réseau
- Scan de ports avec Nmap
- Prise d'empreinte du système d'exploitation (OS Fingerprinting)
- Prise d'empreinte des services et versions

5- Attaques réseau

- Idle Host Scanning
- Sniffing réseau avec Wireshark
- Spoofing réseau (ARP, IP)
- Hijacking de sessions
- Attaques des protocoles sécurisés (SSL/TLS)
- Dénis de service (DoS/DDoS)

6- Attaques système

- Scanner de vulnérabilités (Nessus, OpenVAS)
- Exploitation d'un service vulnérable distant
- Élévation de privilèges
- Espionnage du système
- Génération d'un malware avec Metasploit
- Encodage de payloads et méthodes de détection

Audit de sécurité de sites Web

Code : SE05 **Durée** : 4 jours **Classe** : Présentiel / à distance

7- Attaques web

- Cartographie du site et identification des fuites d'information
- Failles PHP : include, fopen, upload non sécurisé
- Injections SQL : détection, exploitation et prévention
- Cross-Site Scripting (XSS) : réfléchi, stocké et DOM
- Cross-Site Request Forgery (CSRF)
- Bonnes pratiques de sécurisation des applications web

8- Attaques applicatives

- Architecture Intel x86 et registres
- La pile et son fonctionnement
- Écrasement de variables et contrôle du registre EIP
- Exécution d'un shellcode
- Prise de contrôle du système en tant que root

9- Challenge final

- Mise en pratique globale de toutes les techniques apprises
- Audit complet d'un système cible en conditions réelles
- Identification, exploitation et rapport des vulnérabilités détectées