JAVA

Audit de sécurité de sites Web

3 jours (21h00) | JAV0012 | Num form : form-182 | Perfectionnement / Avancé

INFORMATIQUE / DÉVELOPPEMENT / JAVA

À l'issue de ce stage vous serez capable de :

- Connaître les différents types de vulnérabilités des sites web et comprendre comment elles peuvent être exploitées
- Comprendre comment augmenter le champ d'exploitation des vulnérabilités pour un test d'intrusion
- Disposer de l'ensemble des connaissances et compétences nécessaires à la réalisation d'un audit de sécurité

Niveau requis :

- Avoir suivi la formation "Hacking et Sécurité - Niveau avancé" ou connaissances équivalentes
- Maîtrise des outils Linux
- Connaissance des langages de développement Web

Public concerné :

- Consultants en sécurité
- Développeurs
- Ingénieurs / Techniciens

Programme :

INTRODUCTION

- Rappel TCP/IP / Réseau Matériel

- Protos / OSI - Adressage IP

INTRODUCTION À LA VEILLE

- Vocabulaire
- BDD de Vulnérabilités et Exploits
- Informations générales

PRISE D'INFORMATION

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

SCAN ET PRISE D'EMPREINTE

- Énumération 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
- Élévation 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'information
- 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'attaques standards (écrasement 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 sur un TP final