EduGroupe
Accompagner pour réussir

Hacking et sécurité : expert

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

Connaissances préalables

- Avoir suivi le cours SECHSA - Hacking & Sécurité : Avancé ou posséder les connaissances et compétences équivalentes
- Connaissance fondamentale des protocoles réseau (TCP/IP, routage)
- Développement occasionnel dans au moins un langage de programmation: Python, PHP, C
- Être à l'aise dans l'utilisation des outils classiques du pentest (Kali)
- Maîtrise de l'administration Linux (shell) et Windows
- Maîtrise des technologies de virtualisation (VirtualBox)
- Notions avancées sur les principales techniques de hacking (buffer overflows inclus)

Profil des stagiaires

- Administrateurs systèmes / réseaux
- Consultants en sécurité
- Développeurs
- Ingénieurs / Techniciens

Objectifs

- Acquérir un niveau d'expertise élevé dans le domaine de la sécurité en réalisant différents scénarios complexes d'attaques
- En déduire des solutions de sécurité avancées

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

EduGroupe
Accompagner pour réussir

Contenu du cours

1. JOURS 1 et 2

- Techniques de scan : Différents types de scans - Personnalisation des flags - Packet-trace - Utilisation des NSE Scripts
- Détection de filtrage : Messages d'erreur / Traceroute - Sorties nmap - Firewalking avec le NSE Firewalk
- Plan d'infrastructure : Problématiques / Erreurs à ne pas faire - Eléments de défense - Sécurité physique
- Forger les paquets : Commandes de base - Lire des paquets à partir d'un pcap
- Sniffer les paquets : Exporter au format pcap - Exporter au format PDF - Filtrage des paquets avec le filtre - filter - Modifier des paquets via scapy - Les outils de fuzzing de scapy
- Détournement de communication
- Layer 2 vlan (Trunk, vlan hopping)

2. Réseau

- Techniques de scan : Différents types de scans - Personnalisation des flags - Packet-trace - Utilisation des NSE Scripts
- Détection de filtrage : Messages d'erreur / Traceroute - Sorties nmap - Firewalking avec le NSE Firewalk
- Plan d'infrastructure : Problématiques / Erreurs à ne pas faire - Eléments de défense
- Forger les paquets : Commandes de base - Lire des paquets à partir d'un pcap - Créer et envoyer des paquets
- Sniffer les paquets : Exporter au format pcap - Exporter au format PDF - Filtrage des paquets avec le filtre - filter - Modifier des paquets via scapy - Les outils de fuzzing de scapy - Création d'outils utilisant scapy
- Détournement de communications

3. Jour 2 (suite)

- Découverte de l'infrastructure et des technologies associées
- Recherche des vulnérabilités : Côté serveur (recherche d'identifiant, vecteur d'injection, SQL injection) - Injection de fichiers - Problématique des sessions - Web Service - Ajax - Côté client (Clickjacking, Xss, XSRF, Flash, Java)

4. Système

- Metasploit
- Attaques d'un service à distance
- Attaque d'un client et bypass d'antivirus : Attaque visant Internet Explorer, Firefox - Attaque visant la suite Microsoft Office - Génération de binaire Meterpreter - Bypass AV (killav.rb, chiffrement, padding etc.)
- Utilisation du Meterpreter : Utilisation du cmd/Escalade de privilège - MultiCMD, attaque 5 sessions et plus - Manipulation du filesystem - Sniffing / Pivoting / Port Forwarding
- Attaque d'un réseau Microsoft : Architecture / PassTheHash - Vol de token (impersonate token)
- Rootkit

5. JOUR 3

-

6. Web

- Découverte de l'infrastructure et des technologies associées
- Recherche des vulnérabilités : Côté serveur (recherche d'identifiant, vecteur d'injection, SQL injection) - Injection de fichiers - Problématique des sessions - Web Service - Côté client (Clickjacking, XSS, CSRF)

7. JOUR 4

-

8. Applicatif

- Shellcoding Linux : Du C à l'assembleur - Suppression des NULL bytes - Exécution d'un shell
- Buffer Overflow avancés sous Linux : Présentation des méthodes standards (Ecrasement de variables - Contrôler EIP - Exécuter un shellcode) - Présentation du ROP et des techniques de bypass des dernières protections (ASLR / NX/ PIE / RELRO)

9. JOUR 5

-

10. TP 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.