Sécurité informatique
Hacking et sécurité avancée

Publics

Administrateur systèmes, techniciens, responsables sécurité

Pré-requis

Connaissance de base sur les systèmes et les réseaux

Objectifs pédagogiques

Etre capable de :

- Maitriser les compétences techniques nécessaires pour comprendre les techniques d'attaques et mieux protéger le système d'information

Moyens pédagogiques et techniques

Explications théoriques et exercices pratiques pour mise en situation rapide

1 vidéoprojecteur par salle

1 ordinateur par stagiaire

1 support de cours par stagiaire

Évaluation et documents fournis

- Document d'évaluation de satisfaction
- Attestation de présence
- Exercices pratiques de validation des acquis sous contrôle du formateur

Lieu : • Centre de formation Activ'Académie
• Site client (nous consulter)

Durée totale : 3 jours (21 heures)

Nombre de participants : 4 maximum

Programme

Introduction

- Présentation de l'environnement de Hacking : Lutter contre quels risques
- Le processus de sécurité

Scan et prises d'empreintes

- Reconnaissance de la cible : Les bases de données Whois / Recherche sur Internet
- Cartographie de la cible
- System Fingerprinting : La prise d'empreinte du système
- Énumération des vulnérabilités : Scan de vulnérabilités

Vulnérabilités Réseaux

- Interception de trafic et analyse : Approche théorique
- Environnements réseaux : Facilités et limites du Sniffing
- Utilisation d'un Sniffer
- Contourner les protections d'infrastructures réseaux : IP Spoofing
- Contourner le Firewall
- Attaque de protocoles sécurisés
- IDLE Host Scanning
- Hijacking

Vulnérabilités Client

- Modes et signes d'infection
- Introduction à Metasploit
- Conception de Malware

Vulnérabilités Web

- Failles PHP (inclusion, f open...)
- Attaques des bases de données : SQL INJECTION
- XSS : Piratage de sessions & usurpation d'identité : Usurpation d'identité / Piratage de session
- Cross-Site Resquest Forgery (C.S.R.F.)

Vulnérabilités Applicatives

- Escape Shell
- Buffer Overflow
- Étude de méthodologies d'attaques avancées en local et prise de contrôle du statut Administrateur

Vulnérabilités système

- Élévation des privilèges
- Brute force d'authentification
- Le fichier PASSWD d'Unix
- Espionnage du système
- Backdoor et Rootkits
- Systèmes de détection d'intrusion

Contre-mesures

- Contre-mesures classiques
- Filtrage des entrées utilisateur
- Séparation des droits
- Limitation des accès réseau
- Firewall et VPN
- Détection des intrusions

Mise à jour : Octobre 2024

Tarifs Inter : 650€ HT/jour/pers.
Tarifs Intra / sur mesure : nous consulter
Délais : nous consulter
Moyens d'encadrement :
formateur spécialiste du domaine
Référence : SRS

Activ' académie