Tests d'intrusion

Référence : **SECPNT1** Durée : **5 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• 1-Des notions en IT et/ou SSI. • 2-Des notions d'utilisation d'une distribution Linux est un plus.

PROFIL DES STAGIAIRES

• 1-Pentesters. • 2-Consultants SSI. • 3-RSSI. • 4-Architectes.

OBJECTIFS

• Préparer un test d'intrusion réussi. • Maîtriser toutes les phases d'un test d'intrusion (de la découverte à la post exploitation) : Découvrir facilement et rapidement le réseau cible ; Exploiter en toute sécurité les vulnérabilités identifiées ; Élever ses privilèges pour piller les ressources critiques ; Rebondir sur le réseau compromis. • Comprendre les vulnérabilités exposées par les réseaux externes et internes. • Utiliser efficacement la trousse à outils du pentester.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité offensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Introduction aux tests d'intrusion

- Équipement et outils
- Organisation de l'audit
- Méthodologie des tests d'intrusion
- Gestion des informations et des notes
- Exemple de bon rapport d'audit
- Les meilleurs pratiques : PASSI

Rappels et bases

- Les shells Unix *sh
- Les shells Windows cmd & powershell
- Rappels sur les réseaux tcp/ip
- Rappels du protocole HTTP
- Introduction à Metasploit : Exploits et Payloads ; Fonctionnalités utiles ; Base de données ; Modules ; Customisation
- Mises en pratique

Découverte d'information

- Reconnaissance de la cible : Open Source Intelligence
- Découverte passive du SI : Écoute réseau
- Scans réseau : Cartographie du réseau ; Découverte de services ; Identification des Systèmes d'exploitation
- Scanners de vulnérabilités : Scanner Open Source Openvas
- Mises en pratique

Mots de passe

- Attaques en ligne : Brute force en ligne ; Outils Open Source
- Attaques hors ligne : Analyse d'empreintes ; Méthodologies de cassage ; Les Raibow Tables
- Outils Open Source
- Mises en pratique

Exploitation

- Identification des vulnérabilités : Contexte des vulnérabilités ; Étude de divers types de vulnérabilités
- Méthodologie d'exploitation : Identifier le bon exploit ou le bon outil : Éviter les problèmes ; Configurer son exploit
- Exploitations à distance
- Exploitations des clients
- Mises en pratique

Post-exploitation

- Le shell Meterpreter et ses addons
- Élévation de privilèges
- Fiabiliser l'accès
- Pillage : Vol de données ; Vol d'identifiants
- Rebond : Pivoter sur le réseau ; Découvrir et exploiter de nouvelles cibles
- Mises en pratique

Intrusion web

- Méthodologie d'intrusion WEB
- Utilisation d'un proxy WEB : Proxy Open Source ZAP
- Usurpation de privilèges : CSRF
- Les injections de code : Côté client : XSS ; Côté serveur : SQL
- Compromission des bases de données
- Autres types d'injections
- Les inclusions de fichiers : Locales ; A distance
- Les webshells : Précautions d'emploi
- Mises en pratique

Intrusion Windows

- Méthodologie d'intrusion Windows
- Découverte d'informations : Identification de vulnérabilités ; Techniques de vols d'identifiants
- Réutilisation des empreintes : Technique de "Pass The Hash"
- Élévation de privilèges : Locaux ; Sur le domaine : BloodHound
- Échapper aux anti-virus : Techniques diverses ; Outil Open Source Veil
- Outillage powershell : Framework Open Source PowerShell Empire
- Mises en pratique

Intrusion Unix/Linux

- Méthodologie d'intrusion Linux : Rappels sur la sécurité Unix
- Découverte d'informations : Identifications de vulnérabilités
- Élévation de privilèges : Abus de privilèges ; Exploitation de vulnérabilités complexes
- Mises en pratique