EduGroupe
Accompagner pour réussir

Tests d'intrusion

Référence : **SECPNT1** Durée : **5 jours (35 heures)** Certification : **Aucune**

Connaissances préalables

- 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
- Comprendre les vulnérabilités exposées par les réseaux externes et internes
- Utiliser efficacement la trousse à outils du pentester

Certification préparée

- Aucune

Méthodes pédagogiques

- 6 à 12 personnes maximum par cours, 1 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 et de réflexions

Formateur·rice

- 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

Contenu du cours

1. 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

2. 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
- Mises en pratique

3. Découverte d'information

- Reconnaissance de la cible : Open Source Intelligence
- Découverte passive du SI : Écoute réseau
- Scans réseau : Cartographie du réseau
- Scanners de vulnérabilités : Scanner Open Source Openvas
- Mises en pratique

4. Mots de passe

- Attaques en ligne : Brute force en ligne
- Attaques hors ligne : Analyse d'empreintes
- Outils Open Source
- Mises en pratique

5. Exploitation

- Identification des vulnérabilités : Contexte des vulnérabilités
- Méthodologie d'exploitation : Identifier le bon exploit ou le bon outil : Éviter les problèmes
- Exploitations à distance
- Exploitations des clients
- Mises en pratique

6. Post-exploitation

- Le shell Meterpreter et ses addons
- Élévation de privilèges
- Fiabiliser l'accès
- Pillage : Vol de données
- Rebond : Pivoter sur le réseau
- Mises en pratique

7. 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
- Compromission des bases de données
- Autres types d'injections
- Les inclusions de fichiers : Locales
- Les webshells : Précautions d'emploi
- Mises en pratique

8. Intrusion Windows

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

9. Intrusion Unix/Linux

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

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.