EduGroupe
Accompagner pour réussir

Pentest Active Directory 1

Référence : **SECPNT002** Durée : **5 jours (35 heures)** Certification : **Aucune**

Connaissances préalables

- Avoir de bonnes connaissances réseau et Unix est recommandé
- Avoir des notions de sécurité offensive mais pas d'expérience préalable sur les environnements Active Directory

Profil des stagiaires

- Cette formation Pentest Active Directory 1 s'adresse principalement aux pentesteurs, administrateurs systèmes et architectes sécurité
- Elle s'adresses aussi à tout profil technique souhaitant enrichir son parcours professionnel avec une composante sécurité

Objectifs

- Acquérir les compétences nécessaires à la réalisation d'un test d'intrusion Active Directory approfondi

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. JOUR 1

-

2. Bases théoriques des mécanismes de sécurité

- Fonctionnement des mécanismes d'administration (RPC, SMB, WMI, RDP, WinRM)
- Gestion des identités et des accès, stockage des secrets, protocoles d'authentification réseau (NTLM, Kerberos)
- Hiérarchie et liens de confiance Active Directory

3. Techniques de reconnaissance et d'exploitation depuis un accès anonyme

- Enumération
- Empoisonnement de protocoles réseau
- Relaying

4. JOUR 2

-

5. Reconnaissance sur le domaine depuis un accès non privilégié

- Extraction des objets (utilisateurs, groupes, machines, GPO) et cartographie avec BloodHound

6. Élévation de privilèges locale

- Enumération et exploitation (services locaux, tâches planifiées, ACLs, vulnérabilités publiques)
- Techniques de contournement de l'UAC

7. JOUR 3

-

8. Élévation de privilèges au sein d'un domaine

- Extraction de secrets (registres, LSASS, DPAPI)
- Rejeu d'authentification
- Kerberoasting
- Abus de chemins de contrôle

9. Contournement de restrictions logicielles

- AppLocker
- Evasion de bureaux restreints (Citrix, Kiosque RDP)

10. JOUR 4

-

11. Étapes de post-exploitation depuis un accès privilégié sur le domaine

- Extraction de secrets (NTDS, DPAPI)
- Forge de tickets (silver et golden tickets)
- Manipulation d'ACL
- Persistance au sein de l'environnement et effacement des traces

12. Extension de la compromission

- Etudes des relations de confiance inter-domaines et inter-forêts
- Abus de délégation Kerberos

13. JOUR 5

-

14. Introduction à Azure

- Concepts fondamentaux (terminologie, gestion des identités et des accès)
- Intégration avec l'Active Directory (synchronisation des identités, mécanisme Single Sign-On)
- Etapes de reconnaissance et compromission depuis l'environnement on-premise

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.