MAJ 27/10/2025

Formation « Tests d'intrusion Active Directory »

Réf: PENTESTAD

Active Directory est le coeur battant des infrastructures Microsoft, et la cible privilégiée des attaques cyber. Réaliser des tests d'intrusions sur cet environnement est une méthode efficace et pragmatique pour mettre en évidence les vulnérabilités qui seront exploitées par vos adversaires.

Découvrez ces vulnérabilités par vous-même avant que celles-ci soient exploitées par d'autres !

Objectifs

- Maîtriser toutes les phases d'un test d'intrusion (de la reconnaissance à la post exploitation)
  - Reconnaissance de l'environnement AD avec et sans authentification
  - Exploitation des vulnérabilités identifiées en toute sécurité
  - Élévation des privilèges pour piller les ressources critiques
  - Rebond vers d'autres systèmes ou vers/depuis Entra ID
- Comprendre les vulnérabilités Active Directory / Entra ID
- Utiliser efficacement la trousse à outils du pentester

Durée & horaires

- 5 jours soit 35 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Pentesters
- Consultants SSI
- Architectes
- RSSI (avec background technique)

Pré-requis

- Connaître les attaques et outils rudimentaires des tests d'intrusion (nmap, responder/ntlmrelayx, metasploit, nxc...)
- et/ou disposer d'une certification Pentest1 HS2 (ou équivalent ex : OSCP)

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs
- Les concepts essentiels développés dans la formation sont illustrés au travers de mises en pratique sur PC permettant d'acquérir des compétences concrètes applicables en test d'intrusion
- Un SI (Active Directory) vulnérable fidèle à la réalité sert de plateforme pour les tests
- Tous les outils utilisés sont issus du monde libre et peuvent être réutilisés lors des missions
- Utilisation de techniques et outils classiques ainsi que modernes tout au long de la formation

Supports

- Support de cours numérique en Français projeté
- Support de cours en Français imprimé
- Cahier d'exercices
- Cahier de corrections
- Ordinateur portable prêté pour la réalisation des exercices

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration
- Evaluation de pré-formation envoyée avant le début de la formation

- **Evaluation de mi-formation effectuée en session par le formateur au moyen de QCM et de travaux pratiques**
- **Examen final à la fin de la formation (cf certification)**

Ces évaluations ont pour but de valider les compétences acquises.

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification PENTESTAD par HS2.**

Programme

Notions essentielles

- Les différentes fonctionnalités de AD (Annuaire, PKI, configuration…)
- Forêt, Domaine, UO...
- Schéma et rôles FSMO
- Comptes utilisateurs/machines, groupes, GPO

Reconnaissance sans authentification

- Rappels Pentest1
  - Enumération des postes et serveurs
  - Enumération LDAP/SMB/RPC Nulle
  - Password spraying
- Bruteforce RID
- PXE

Reconnaissance avec authentification

- BloodHound
  - Introduction
  - Collecteurs
  - Recherche de chemins d'attaque
  - CQL avancé
- Enumération DNS
- adPeas

Mouvement latéral

- Coercition
  - Techniques de coercition via RPC
  - Fichiers sur les partages
    - LNK, SCF, URL
- Relais NTLM
  - Cross protocol
  - Protections signing/EPA
  - Reflected
  - Vers LDAP
    - WebDav
      - Webclient Service
      - Activation
      - Relais HTTP
    - Shadow Credentials
    - RBCD
  - MSSQL
- Pass the certificate
- DNS

- Kerberos
  - Attaques de roasting avancées (Kerberoasting via AS-RepRoasting)
  - Pass the ticket
  - Délégation Kerberos
    - Délégation sans contrainte
      - Compte machine
      - Compte utilisateur
    - Délégation contrainte
    - Délégation contrainte basée sur les ressources
  - Relais Kerberos
    - classique/reflected
- Pre2k
- WSUS
  - Wsuspendu
  - Wsuspect
- SCCM/MECM

Post-exploitation et persistance

- AdminSDHolder
- DC shadow
- DPAPI
- Forge de tickets
  - Sapphire
  - Diamond
- Relations d'approbation (domaines et forêts)
  - Directionnelles
  - SID History

Azure / Entra ID

- Introduction
  - Concepts clés d'Entra ID
  - Différences Active Directory / Entra ID
  - Rôle et privilèges sensibles
  - Mécanismes d'authentification (OAuth2, OIDC, SAML)
- Attaques sur l'infrastructure de synchronisation hybride
  - Compromission du compte de service Azure AD Connect
  - Extraction de secrets d'authentification depuis AAD Connect
    - Password Hash Synchronization (PHS)
    - Clé Seamless SSO
    - Pass-through Authentication (PTA)
- Pivots Active Directory vers Entra ID
  - Réutilisation de la clé Seamless SSO
  - Abus d'un IdP fédéré
    - Golden SAML
  - Abus d'un poste compromis
    - Dump de Primary Refresh Token (PRT)
    - Vol de refresh/access tokens locaux
    - Pass-the-Cookie
- Accès initial et escalade de privilèges dans Entra ID
  - Reconnaissance et accès initial
    - Enumeration des utilisateurs
    - Password spray & legacy auth
    - Consent phishing
  - Escalade de privilèges dans Entra ID

        - Activation de rôles PIM éligibles
        - Abus de règles de groupes dynamiques
        - Abus de permissions d'application
- Pivots Entra ID vers Active Directory
    - Pivot vers l'environnement on-prem
        - Hybrid Azure AD Join
        - Shadow Credentials (msDS-KeyCredentialLink)
        - Writeback d'attributs
        - Abus d'identités managées
            - Azure ARC
            - Azure Function App / Logic Apps