Reconnaissance Active Directory

Documentation rédigée par : GADONNAUD Ewen

Formation : BTS SIO 1ère année - Option SISR

Établissement : Lycée Paul-Louis Courier, Tours

Date : Mars 2026

Les techniques présentées ici sont à des fins éducatives et de formation. Leur utilisation n'est légale que sur des environnements dont vous êtes propriétaire ou pour lesquels vous disposez d'une autorisation écrite explicite.

1. Qu'est-ce que l'Active Directory ?

L'Active Directory (AD) est le service d'annuaire de Microsoft, déployé dans la quasi-totalité des entreprises. Il centralise la gestion des identités, des accès et des politiques de sécurité d'un réseau Windows.

Composants clés à connaître :

Terme	Définition
Domain	Unité d'organisation principale (ex: `lab.local`)
Domain Controller (DC)	Serveur qui héberge et gère l'AD. Cible prioritaire en pentest
Forest	Ensemble de domaines partageant un schéma AD commun
OU (Organizational Unit)	Conteneur logique pour organiser utilisateurs, groupes, machines
GPO (Group Policy Object)	Politiques appliquées automatiquement aux objets de l'AD
SPN (Service Principal Name)	Identifiant unique d'un service (utile pour Kerberoasting)
LDAP	Protocole utilisé pour interroger l'annuaire AD
Kerberos	Protocole d'authentification principal de l'AD
NTLM	Protocole d'authentification legacy, encore présent et exploitable

Pourquoi l'AD est une cible privilégiée ? Compromettre le Domain Controller = compromettre l'intégralité du réseau. Un attaquant qui obtient les droits `Domain Admin` contrôle tous les comptes, toutes les machines, et toutes les politiques du domaine.

2. Méthodologie de reconnaissance

La reconnaissance AD suit une progression logique :

```
1. Découverte réseau       → Trouver les machines, identifier le DC
2. Enumération LDAP        → Lister utilisateurs, groupes, machines, GPO
3. Enumération des droits  → Identifier les chemins de privilège
4. Identification des cibles → Comptes privilégiés, services exposés,
mauvaises configs
```

On distingue deux types de reconnaissance :

Type	Description	Outils
Passive	Sans authentification, sans interagir avec le DC	nmap, ldapsearch anonyme
Authentifiée	Avec un compte du domaine (même bas privilège)	BloodHound, ldapdomaindump, enum4linux-ng

En situation réelle, un simple compte utilisateur du domaine suffit pour énumérer l'intégralité de l'AD. C'est une faiblesse fondamentale de l'Active Directory par défaut.

3. Environnement de Laboratoire (Maquette)

```
Attaquant (Kali Linux)
Mode réseau : Bridge

Cible : Domain Controller (Windows Server 2025)
IP : 192.168.1.229
Domaine : lab.local
```

Comptes configurés pour le TP :

- `jdupont` / `Password123` : Utilisateur standard (Membre du groupe Users, UO Utilisateurs_Lab).
- `amartin` / `Summer2024!` : Administrateur (Membre du groupe Admins IT → Domain Admins). Possède un SPN enregistré (`HTTP/webserver.lab.local`).
- `svcbackup` / `Backup2024` : Compte de service (Membre du groupe Users). La pré-authentification Kerberos a été volontairement désactivée (vulnérable à l'AS-REP Roasting).
- `admin` / `P@ssw0rd` : Domain Admin par défaut.

Sur Windows Server 2025, le pare-feu bloque les requêtes ICMP entrantes par défaut. Pour permettre le ping depuis la machine attaquante, la règle suivante a été ajoutée en PowerShell : `netsh advfirewall firewall add rule name="ICMP Allow" protocol=icmpv4:8,any dir=in action=allow`

4. Découverte réseau

Identifier les hôtes actifs et le contrôleur de domaine

```
nmap -sn 192.168.1.0/24                    # Ping scan pour identifier les machines sur le sous-réseau
nmap -sV -p 88,389,445,3268 192.168.1.229  # Vérification des ports caractéristiques de l'AD sur la cible
```

Ports caractéristiques d'un Domain Controller :

Port	Service	Intérêt
88	Kerberos	Confirme la présence d'un DC
389	LDAP	Interrogation de l'annuaire
445	SMB	Partages, authentification NTLM
636	LDAPS	LDAP chiffré
3268	Global Catalog	Recherche multi-domaines

5. Enumération LDAP

Avec un compte du domaine

```
ldapsearch -x -H ldap://192.168.1.229 \
  -D "jdupont@lab.local" \
  -w "Password123" \
  -b "DC=lab,DC=local" \
  "(objectClass=user)" cn sAMAccountName
```

Avec ldapdomaindump (résultats en HTML/JSON)

```
ldapdomaindump -u "lab.local\jdupont" -p "Password123" 192.168.1.229
```

Spécificité de sécurité liée à Windows Server 2025 Par défaut, Windows Server 2025 impose l'intégrité et la signature des requêtes LDAP (`LDAP server signing requirements Enforcement`). Les requêtes non chiffrées en “Simple Bind” (comme celles effectuées par défaut par `ldapsearch` ou `ldapdomaindump`) sont rejetées avec une erreur exigeant le SSL/TLS. Pour reproduire un environnement de CTF classique et permettre l'énumération non chiffrée, il est nécessaire de modifier la GPO `Default Domain Controllers Policy` :

- Chemin : `Paramètres de sécurité → Stratégies locales → Options de sécurité`
- Paramètre : `Contrôleur de domaine : conditions requises pour la signature de serveur LDAP` défini sur **Aucun**.

Appliquer ensuite avec `gpupdate /force`.

6. Suite de l'énumération (En cours d'élaboration...)

(Les sections sur l'énumération SMB, BloodHound, et l'exploitation des vulnérabilités Kerberos seront ajoutées au fur et à mesure du laboratoire)

— Ewen 2026/03/11