Labo Reconnaissance Active Directory (Windows Server 2025)

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)
  IP : 192.168.1.206
  Mode réseau : Bridge

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

Comptes configurés pour le TP :

Compte	Mot de passe	Rôle	Particularité
`jdupont`	`Password123`	Utilisateur standard	Membre du groupe Users
`amartin`	`Summer2024!`	Administrateur	Membre Admins IT → Domain Admins. SPN : `HTTP/webserver.lab.local`
`svcbackup`	`Backup2024`	Compte de service	Pré-authentification Kerberos désactivée (AS-REP Roastable)
`admin`	`P@ssw0rd`	Domain Admin	Compte administrateur 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 sur le DC :

```
netsh advfirewall firewall add rule name="ICMP Allow" protocol=icmpv4:8,any
dir=in action=allow
```

4. Découverte réseau

Ping scan — identification des hôtes actifs

```
nmap -sn 192.168.1.0/24
```

Résultat obtenu :

```
Starting Nmap 7.95 at 2026-03-11 21:49 CET
Host is up (0.012s latency).
MAC Address: 08:00:27:E1:70:82 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Nmap done: 256 IP addresses (1 host up) scanned in 1.99 seconds
```

L'adresse MAC `08:00:27:E1:70:82` identifie la machine comme une VM VirtualBox — c'est notre DC à l'adresse `192.168.1.229`.

Scan des ports caractéristiques d'un DC

```
nmap -sV -p 88,389,445,3268 192.168.1.229
```

Résultat obtenu :

```
PORT     STATE    SERVICE       VERSION
80/tcp   filtered http
389/tcp  open     ldap          Microsoft Windows Active Directory LDAP
                                (Domain: lab.local0., Site: Default-First-
Site-Name)
445/tcp  open     microsoft-ds?
3268/tcp open     ldap          Microsoft Windows Active Directory LDAP
                                (Domain: lab.local0., Site: Default-First-
Site-Name)
MAC Address: 08:00:27:E1:70:82 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Service Info: Host: WIN-U64MI2E97RF; OS: Windows; CPE:
cpe:/o:microsoft:windows
```

Les ports 389 (LDAP) et 3268 (Global Catalog) sont ouverts et confirment la présence d'un DC. Nmap a automatiquement récupéré le nom de domaine `lab.local` et le hostname `WIN-U64MI2E97RF`.

Port	État	Interprétation
80	filtered	Pare-feu Windows bloque HTTP — normal

Port	État	Interprétation
389	open	LDAP disponible — annuaire interrogeable
445	open	SMB disponible — énumération des partages possible
3268	open	Global Catalog — confirme le rôle DC

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
```

Détail de la commande :

- `-x` — authentification simple (login/mot de passe)
- `-H ldap://192.168.1.229` — adresse du serveur LDAP
- `-D “jdupont@lab.local”` — compte utilisé pour s'authentifier
- `-w “Password123”` — mot de passe associé
- `-b “DC=lab,DC=local”` — point de départ de la recherche (racine du domaine)
- `“(objectClass=user)”` — filtre : uniquement les objets de type utilisateur
- `cn sAMAccountName` — attributs à récupérer : nom complet et login Windows

Spécificité Windows Server 2025 — LDAP Signing

Par défaut, Windows Server 2025 impose la signature des requêtes LDAP. Les requêtes non chiffrées sont rejetées avec l'erreur suivante :

```
ldap_bind: Strong(er) authentication required (8)
additional info: 00002028: LdapErr: DSID-0C09035C, comment: The server
requires binds to turn on integrity checking if SSL\TLS are not already
active on the connection, data 0, v65f4
```

Pour reproduire un environnement de lab classique, désactiver cette exigence via 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` → **Aucun**

Appliquer ensuite sur le DC :

```
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)