RÉPUBLIQUE DU BÉNIN
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

**UNIVERSITÉ D'ABOMEY-CALAVI**

**INSTITUT DE FORMATION ET DE RECHERCHE EN INFORMATIQUE**

BP 526 Cotonou Tel : +229 21 14 19 88
https://www.ifri-uac.bj Courriel : contact@ifri.uac.bj

# MÉMOIRE

pour l'obtention du

**Diplôme de Licence en Informatique**

**Option :** Sécurité Informatique

**Présenté par** :
Omoladé Bignon Farel Eldred **ADELAKOUN**

# Active Directory : Vulnérabilités, Exploitation et Contres-mesures (Faiblesses du protocole SMB)

**Sous la supervision** :
Amadou Tidjani **SANDA MAHAMA**

**Membres du jury** :

| | | |
|---|---|---|
| Dr (MA) Vinasétan Ratheil HOUNDJI | IFRI | Président |
| Ing Rose GOHOUE | IFRI | Examinateur |
| Dr (MA) Tidjani SANDA | IMSP | Rapporteur |

Année Académique : **2023 - 2024**

# Sommaire


Dédicace ii

Remerciements iii

Résumé iv

Abstract v

List of Figures vi

Liste des acronymes vii

Introduction 1

1 Revue de littérature 3

2 Exploitations des failles et approches de solutions (Vulnérabilité du protocole SMB) 12

3 Résultats des implémentations et recommandations 19

Conclusion 24

Webographie 25

Table des matières 27

# Dédicace

A Tous mes proches, amis et mentors, qui ont partagé chaque étape de ce voyage, dans la douleur comme dans la joie. Vos encouragements et votre amour m'ont porté jusqu'ici.

# Remerciements

Je tiens à remercier :

- Mes parents pour le soutien morale et l'encouragement qu'ils m'ont donné durant ma formation et le déroulement de ce travail ;
- Le Directeur de l'Institut de Formation et de Recherche en Informatique (IFRI), Monsieur Eugène EZIN pour ses nombreux conseils ;
- Tout le corps professoral de l'IFRI pour la qualité des enseignements ;
- Monsieur Athanase ATCHOME pour ses conseils, son support et son assistance ;
- Monsieur Tidjani SANDA pour son assistance durant la réalisation de ce projet ;
- Mes amis et camarades de classe.

# Résumé

L'Active Directory (AD) est un système essentiel pour la gestion des identités et des accès au sein des entreprises, permettant de centraliser l'administration des utilisateurs, des ordinateurs et des ressources réseau. Grâce à ce système, l'authentification et l'autorisation des utilisateurs sont simplifiées, et des politiques de sécurité peuvent être appliquées de manière centralisée. Cependant, l'Active Directory n'est pas exempt de vulnérabilités, principalement dues à une configuration inadéquate, qui peuvent être exploitées par des attaquants pour compromettre l'intégrité et la sécurité du réseau. Par conséquent, il est primordial de mettre en œuvre des mesures de sécurité robustes pour protéger cet outil et donc les données contre les menaces potentielles.

Ce projet de mémoire se concentre sur l'étude approfondie des vulnérabilités de l'Active Directory et des meilleures pratiques de sécurisation. L'objectif est d'explorer les différents mécanismes de sécurité existants et de proposer des solutions concrètes pour minimiser les risques liés à ces vulnérabilités. Ce travail vise à fournir des recommandations pratiques pour renforcer la sécurité des infrastructures basées sur l'Active Directory et à aider les entreprises à protéger efficacement leurs ressources critiques contre les menaces potentielles.

**Mots clés** : Active Directory,Vulnérabilité,Protocole, protocole SMB

# Abstract

Active Directory (AD) is a critical system for identity and access management within companies, allowing centralized administration of users, computers, and network resources. With this system, user authentication and authorization are simplified, and security policies can be applied centrally. However, Active Directory is not free of vulnerabilities, mainly due to improper configuration, which can be exploited by attackers to compromise the integrity and security of the network. Therefore, it is essential to implement robust security measures to protect this tool and therefore the data from potential threats.

This thesis project focuses on the in-depth study of Active Directory vulnerabilities and best practices for securing them. The objective is to explore the different existing security mechanisms and to propose concrete solutions to minimize the risks related to these vulnerabilities. This work aims to provide practical recommendations to strengthen the security of Active Directory-based infrastructures and to help companies effectively protect their critical resources against potential threats.

**Key words**: Active Directory,Vulnerability,Protocol,SMB protocol

# List of Figures


1.1 Conteunarisation d'objets[4]. . . . . 4
1.2 Objets Active Directory [6] . . . . . 5
1.3 Forêt Active Directory [7] . . . . . 6
1.4 Arbre Active Directory [8] . . . . . 7

2.1 Infrastructure globale . . . . . 13
2.2 Présentation globale du Contrôleur de Domaine . . . . . 14
2.3 Identification de présence . . . . . 15
2.4 Hash de l'utilisateur capturé . . . . . 15
2.5 Mot de passe craqué de l'utilisateur . . . . . 16
2.6 Listing des dossiers partagés . . . . . 16
2.7 Obtention du flag . . . . . 16

3.1 Vérification de la présence du protocole SMB . . . . . 19
3.2 Restriction de NTLM et signature SMB . . . . . 20
3.3 Nouvelle tentative d'attaque . . . . . 20
3.4 Restrictions des accès . . . . . 21

# Liste des acronymes

**AD :**

Active Directory vi, 3

**DC :**

Domain Controller vi

**gMSA :**

Group Managed Service Account vi, 11

**GPO :**

Group Policy Object vi, 18

**LDAP :**

Lightweight Directory Access Protocol vi, 3

**LSASS :**

Local Security Authority Subsystem Service vi, 10

**MitM :**

Man-in-the-Middle vi, 8

**MSA :**

Managed Service Account vi, 11

**NTDS :**

NT Directory Services vi, 3

**NTLM :**

NT LAN Manager vi, 8

**OU :**

Organizational Unit vi

**Pth :**

Pass-the-Hash vi, 9

**SAM :**

Security Account Manager vi, 3

**SMB :**

Server Message Block vi, 8

**TGS :**

Ticket Granting Service vi, 10

# Introduction Générale

La dématérialisation croissante des processus et procédures des entreprises aujourd'hui, nécéssite une gestion efficace des ressources réseaux, la gestion des identités et des accès afin de garantir la disponibilité, l'intégrité et la disponiblité des systèmes et des données. Pour y répondre, divers outils, tels que l'Active Directory (AD), Microsoft Identity Manager (MIM), NetIQ Identity Manager, Okta, et bien d'autres, ont été mis en place afin de répondre aux exigences de gestion et de sécurité de ces infrastructures. Parmi ces outils, certains sont particulièrement privilégiés, comme en témoigne le choix de la Direction Générale des Impôts (DGI) pour l'Active Directory, un service d'annuaire développé par Microsoft pour les environnements Windows [1], et reconnu pour sa capacité à centraliser et sécuriser la gestion des identités et des ressources au sein des organisations.
Cependant, malgré ses atouts, l'Active Directory présente des vulnérabilités significatives. Celles-ci, si elles sont exploitées, peuvent compromettre des aspects de la sécurité tels que la confidentialité, l'intégrité et la disponibilité des systèmes et des données. Dans le cas d'une institution comme la DGI, cela pourrait mettre en péril la sécurité des données fiscales sensibles. Ainsi, il s'agit de répondre aux questions suivantes : Quelles sont les vulnérabilités présentes au sein de l'Active Directory ? Comment une faille du protocole SMB peut-elle être exploitée pour compromettre la sécurité des systèmes et des données, et quelles solutions peuvent être envisagées pour contrer de telles menaces ?

## 0.1 Objectifs

L'objectif général de ce mémoire est d'explorer les vulnérabilités de l'Active Directory, en particulier celles associées au protocole SMB, afin de proposer des solutions techniques efficaces pour sécuriser les infrastructures réseau et protéger les ressources critiques contre les menaces potentielles.

### 0.1.1 Objectifs spécifiques

- Étudier les vulnérabilités de l'Active Directory,
- Mettre en lumière et exploiter certaines de ces failles, comme celles associés au protocole SMB, pour illustrer les risques potentiels,
- Proposer des contre-mesures adaptées afin de sécuriser les ressources réseaux et de gérer les identitées et les accès par l'Active Directory.

## 0.2 Organisation du travail

Ce travail est structuré en trois chapitres. Le premier chapitre propose une revue de littérature sur l'Active Directory et ses vulnérabilités. Le second chapitre se concentre sur l'exploitation des vulnérabilités liées au protocole SMB et propose des solutions pour renforcer la sécurité de l'Active Directory. Enfin, le troisième chapitre présente les résultats de la mise en oeuvre des solutions et fournit des recommandations pour améliorer davantage la sécurité.

Chapitre 1

# Revue de littérature

## Généralités

À l'origine nommé NT Directory Services, ou «Services d'annuaire de NT» en français, l'Active Directory a été présenté pour la première fois en **1996** [2]. Il fut officiellement déployé avec **Windows 2000 Server** en **1999**, marquant un tournant dans la gestion des réseaux d'entreprise. Ce service a rapidement évolué, avec une première mise à jour dans **Windows Server 2003** pour étendre ses fonctionnalités et faciliter son administration. Depuis, chaque nouvelle version de Windows Server a apporté des améliorations pour répondre aux besoins croissants des entreprises en matière de sécurité et de gestion des ressources.
L'Active Directory est conçu pour centraliser la gestion des identités et des ressources réseau dans un environnement Windows. Il tire son origine de l'évolution de la base de données de comptes de données SAM, qui gérait auparavant les comptes d'utilisateurs de manière locale sur chaque machine. De plus avec l'intégration du protocole LDAP, l'AD est devenu un service d'annuaire centralisé, permettant aux organisations de gérer de manière plus efficace les accès aux ressources et les configurations réseau.
Ce service repose sur une technologie de stockage basée sur le régistre windows [3] où la base SAM continue de jouer un rôle fondamental. Ayant une structure hiérarchique, l'Active Directory est subdivisé en domaines, lui permettant une gestion centralisée des ressources telles que les utilisateurs, et les ordinateurs. Cette hiérarchisation permet de regrouper les objets en entités logiques, tout en facilitant leur administration, en les organisant en conteneurs qui peuvent eux-mêmes contenir d'autres objets, comme le montre la figure ci-dessous :

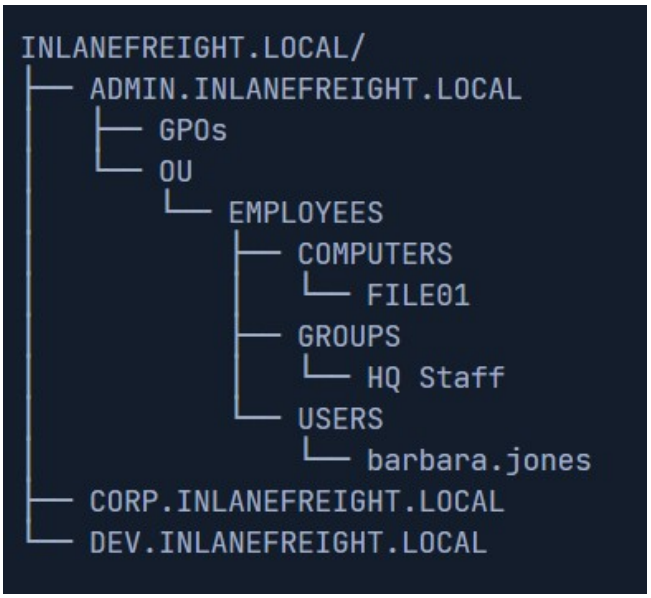



FIGURE 1.1 : Conteunarisation d'objets[4].

## 1.1 Objets

Un objet est une entité distincte qui possède un ensemble d'attributs spécifiques pouvant être utilisés dans plusieurs classes d'objets de schémas. Ceux-ci sont d'une grande importance, car leur modification, en passant par leur création, a un impact conséquent sur toute la structure de l'Active Directory. Parmi ces objets, on peut citer :

- **Unité d'organisation** : Permet la création d'une hiérarchie d'objets en regroupant des objets ayant les mêmes besoins administratifs.
- **Ordinateur et utilisateur** : Représentent les machines et les comptes d'utilisateur au sein du réseau Active Directory.

### 1.1.1 Groupe

Base de données et ensemble de services qui permettent de mettre en lien les utilisateurs avec les ressources réseaux dont ils ont besoin pour mener à bien leurs missions. Deux types de groupe sont à identifier : Groupe de sécurité et Groupe de distribution avec trois différents types d'étendues : Domaine local, Global et Universel[5] :

- **Groupe de sécurité** : Permet de gérer les autorisations au sein du domaine Active Directory, faisant de lui le groupe le plus utilisé.
- **Groupe de distribution** : Ils sont principalement utilisés par des applications de messagerie, comme Exchange pour créer des listes de diffusion.

#### 1.1.1.1 Étendus des groupes

On note :

- **Domaine Local** : Utilisé pour gérer les autorisations d'accès à des ressources dans le domaine où il a été créé. Un groupe à étendu local ne peut pas être utilisé dans un autre domaine.
- **Domaine global** : Utilisé pour gérer des autorisations dans le domaine où il a été créé ou dans un autre domaine approuvé. Il ne peut contenir que des objets du domaine où il a été créé.
- **Groupe Universel** : Ayant une portée maximale, il est accessible sur l'ensemble de la forêt. Ce type de groupe est répliqué sur les contrôleurs de domaine ayant un catalogue global (GC).

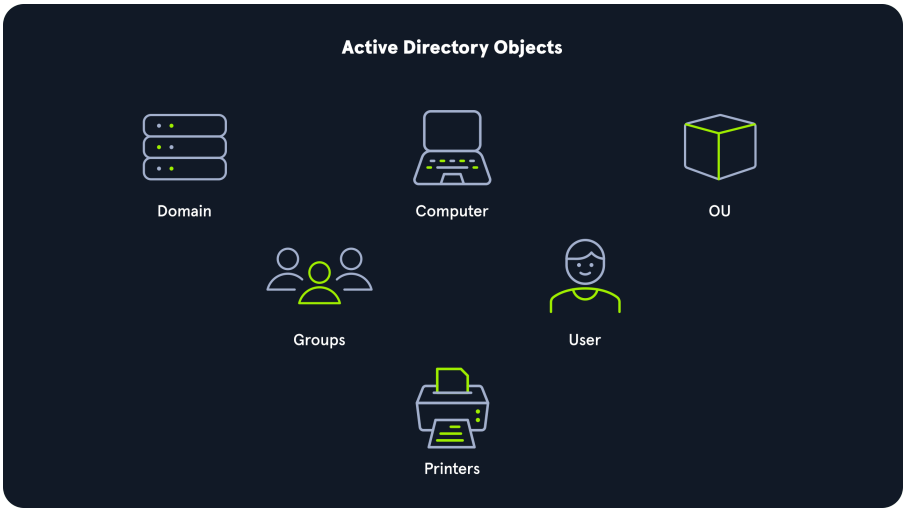



FIGURE 1.2 : Objets Active Directory [6]

#### 1.1.1.2 Stratégie de Groupe (GPO)

Ce sont des ensembles de règles et de configurations appliquées aux objets dans Active Directory, tels que les utilisateurs et les ordinateurs. Les GPO permettent aux administrateurs de gérer les configurations de sécurité, les paramètres logiciels et bien d'autres aspects de l'environnement utilisateur et ordinateur de manière centralisée. Elles peuvent être appliquées au niveau du site, du domaine ou de l'unité d'organisation ; elles héritent et combinent les paramètres en fonction de la hiérarchie de l'Active Directory.

## 1.2 Forêts Arborescence, Arbres et Domaine

Une forêt est un regroupement de plusieurs arborescences de domaines, autrement dit d'un ou plusieurs arbres. Ces arborescences de domaines sont indépendantes et distinctes bien qu'elles soient dans la même forêt. Bien que les arbres d'une forêt ne partagent pas d'espace de noms, une forêt aura un seul domaine racine appelé domaine racine de la forêt.
Le domaine racine de la forêt comporte deux groupes prédéfinis dans l'Active Directory :

- **Enterprise Admins** : Les membres de ce groupe disposent de droits administratifs étendus sur toute la forêt Active Directory.Ils exercent un contrôle absolu sur l'ensemble de la forêt.
- **Schema Admins** : Les membres de ce groupe ont la capacité de modifier le schéma d'Active Directory. Le schéma définit la structure des objets et des attributs dans Active Directory. C'est un composant important car toute modification du schéma affecte l'ensemble de la forêt.

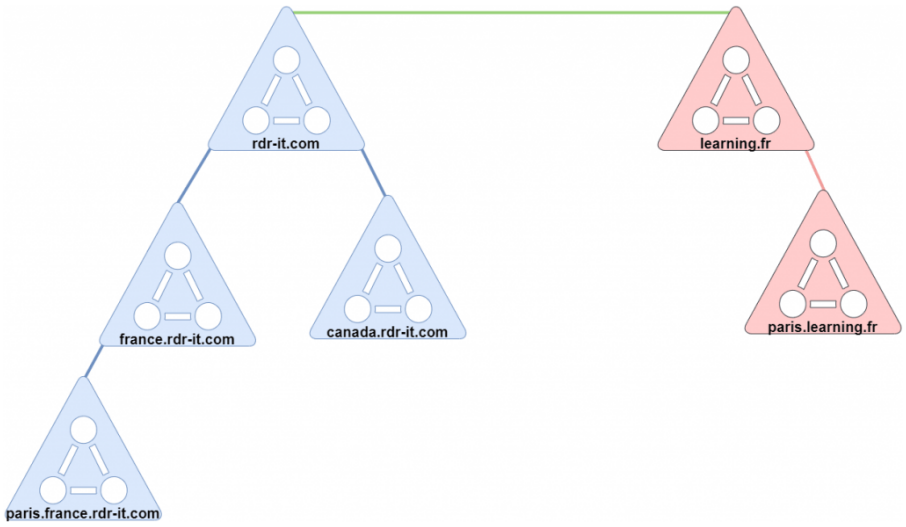



FIGURE 1.3 : Forêt Active Directory [7]

### 1.2.1 Arborescence et Arbres

Une arborescence est une structure hiérarchique de domaines au sein d'une forêt. Elle débute par un domaine racine et peut inclure plusieurs sous-domaines.
Un Arbre est une collection de domaines qui forment une arborescence. Chaque domaine dans un arbre est lié à son domaine parent par une relation de confiance bidirectionnelle et transitive, ce qui permet aux utilisateurs et aux ressources d'être accessibles à travers les différents domaines.

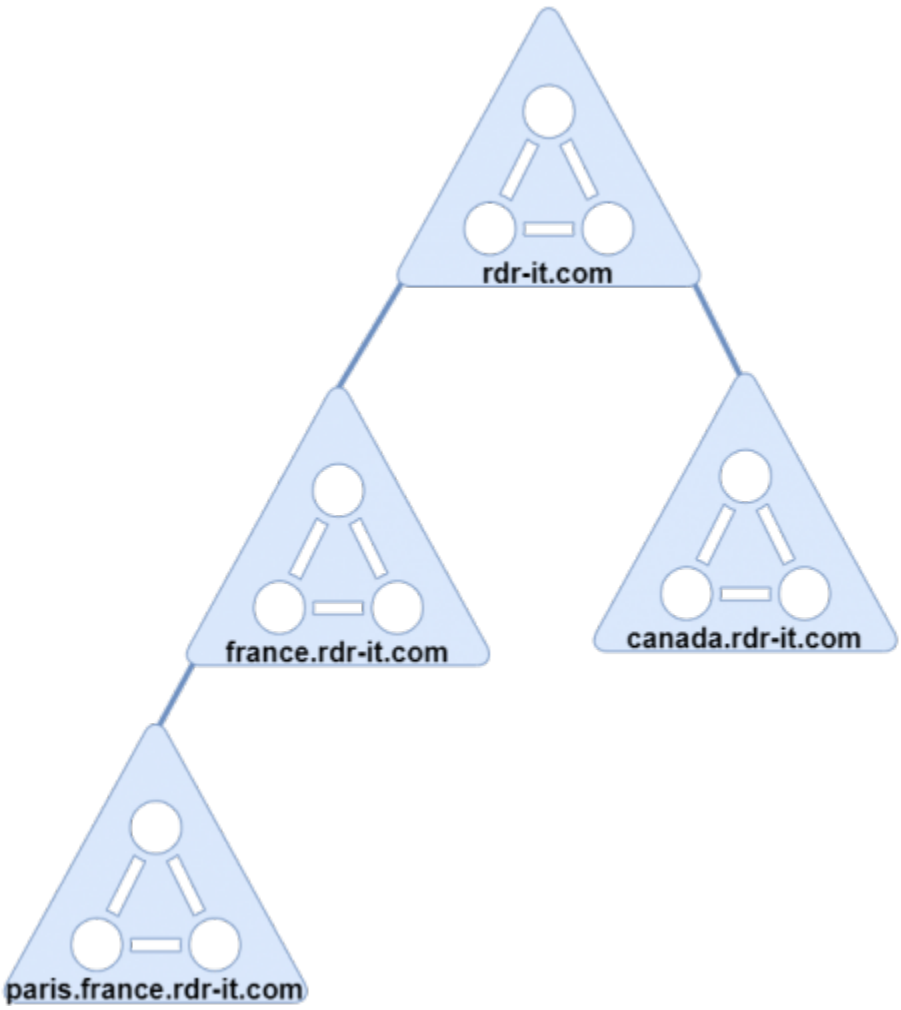



FIGURE 1.4 : Arbre Active Directory [8]

### 1.2.2 Domaine

Un domaine est une entité administrative d'Active Directory au sein de laquelle les fonctionnalités et caractéristiques sont partagées. Dans un domaine, on retrouve des utilisateurs et des ordinateurs ainsi que des stratégies pour en régir le fonctionnement.
Les domaines d'une forêt sont liés par des relations de confiance, permettant une authentification et une autorisation inter-domaines. Ces relations peuvent être configurées pour garantir une gestion et un accès sécurisés entre les domaines.

Toutefois, ces structures et composantes présentent des vulnérabilités, faisant de l'Active Directory une cible privilégiée pour les cyberattaques. Des failes, telles que l'utilisation de protocoles non sécurisés [9], augmentent considérablement les risques de compromission et d'exposition des données sensibles, compromettant ainsi la confidentialité, l'intégrité et la disponibilité des données.

## 1.3 Vulnérabilités de l'Active Directory

Comme vunérabilité au sein de l'Active Directory, on peut noter :

### 1.3.1 Authentication relays

Exploitant une faiblesse au niveau du protocole SMB, largement utilisé lors du partage de fichiers sur un réseau dans les environnement Windows, un attaquant peut intercepter et rediriger des requêtes d'authentification sans avoir besoin de compromettre directement les identifiants de l'utilisateur.

**Description de l'attaque**

L'**Authentication Relays** repose sur une stratégie de type Man-in-the-Middle. Lorsqu'un utilisateur tente de s'authentifier sur un service via SMB ou NTLM [10] un protocole de sécurité ancien mais encore largement utilisé, un attaquant positionné entre le client et le serveur intercepte les échanges d'authentification, notamment en capturant les hashes des identifiants. Une fois ces identifiants chiffrés interceptés, l'attaquant dispose de deux options :

- **Déchiffrement des Hashes** : L'attaquant tente de **craquer les hash** des mots de passe pour obtenir les informations en clair. Bien que cette approche peut prendre du temps selon la complexité des mots de passe, elle permet, une fois réussie, de se faire passer pour l'utilisateur légitime.
- **Relais d'authentification** : Plutôt que de déchiffrer les hashes, l'attaquant peut les **relayer** directement vers un autre service ou serveur, en exploitant le fait que ces identifiants sont valides. Cette approche offre à l'attaquant un accès immédiat, sans avoir besoin de connaître le mot de passe en clair.

Le succès de cette attaque repose sur une mauvaise configuration des services SMB, NTLM et autres protocoles d'authentification, permettant la réutilisation des tokens d'authentification sans vérification adéquate de l'origine des requêtes.

**Impacts potentiels**

- **Accès aux systèmes sensibles** : L'attaquant peut exploiter les identifiants d'utilisateurs légitimes pour accéder à des serveurs ou services protégés.
- **Élévation de privilège** : En relayant les informations d'un utilisateur avec des privilèges élevés (par exemple, un administrateur), l'attaquant peut compromettre l'ensemble du domaine Active Directory.
- **Mouvement latéral** : Une fois en possession des identifiants de connexion, l'attaquant peut tenter d'accéder à d'autres services ou ressources avec des privilèges similaires, poursuivant ainsi son exploitation du réseau.

**Mesures de mitigation**

- **Désactivation de NTLM** : Lorsque cela est possible, désactivez NTLM et adoptez des protocoles plus sécurisés, tels que Kerberos,
- **Signature SMB** : Activez la signature SMB pour garantir l'intégrité des requêtes et empêcher les modifications non autorisées des communications SMB.

### 1.3.2 LDAP

LDAP [11] est un protocole qui fonctionne comme un service de répertoire centralisé et efficace dans l'Active Directory, permettant l'accès et la gestion des informations dans un annuaire réseau. Vu son importance et utilisation dans l'AD, il constitue un risque du fait qu'il peut servir de moyen pour une énumération des objets ou comptes au sein du réseau. Ce qui est utile pour un attaquant qui peut récolter des informations sur le réseau une fois pénétré. Il effectuera donc une attaque dite du «LDAP Enumeration».

**Description de l'attaque**

L'énumération LDAP est une technique consistant à interroger un serveur LDAP pour récupérer des informations détaillées sur les objets d'un domaine Active Directory tels que les utilisateurs, les groupes, les ordinateurs et les politiques réseau. Cette attaque peut se résumer en trois différentes phases que sont : la **connexion au serveur LDAP** qui se fait après l'accès à un compte légitime du domaine ou même parfois directement via un serveur LDAP mal configuré, l'**envoi de requêtes LDAP** pour interroger le serveur et obtenir des informations sur les Objets présents dans l'Active Directory pouvant extraire des informations très détaillées en fonction du type de compte utilisé couplé aux requêtes envoyés et finalement l'**extraction et l'analyse des données** afin d'identifier des cibles potentielles comme des utilisateurs ayant des comptes avec des privilèges plus élevés, des systèmes critiques ou des configurations vulnérables. Plusieurs outils peuvent être utilisés mais le plus efficace reste le **ldapsearch**.

Le succès de cette attaque dépend principalement du type de compte utilisé ainsi que de la capacité de l'attaquant à identifier, récupérer et traiter les informations obtenues.

**Impacts potentiels**

- **Reconnaissance complète du réseau** : L'attaquant peut obtenir une vue d'ensemble du domaine Active Directory.
- **Escalade de privilèges** : Avec les informations collectées, l'attaquant peut identifier les chemins d'escalade de privilèges, comme des comptes ayant un accès aux systèmes critiques.

**Mesures de mitigation**

- **Utilisation d'une version sécurisée de LDAP (LDAPS)** : Utiliser LDAP sur SSL avec le port 636 pour chiffrer les communications.
- **Recherche anonyme** : Désactiver les recherches LDAP anonymes et exiger une authentification pour toutes les requêtes.

### 1.3.3 Pass-The-Hash

Pass-the-Hash est une technique d'attaque permettant à un attaquant d'**utiliser des hashes de mots de passe** pour s'authentifier sur un réseau sans avoir besoin du mot de passe en clair. Cette attaque exploite la manière dont les systèmes windows gèrent l'authentification via les protocoles **NTLM** et **Kerberos** [12], permettant ainsi d'authentifier les utilisateurs et services de manière sécurisée, sans transmettre les mots de passe en clair sur le réseau.

**Description de l'attaque**

L'attaque Pass-the-hash exploite le mécaninisme d'authentification de windows, qui permet aux utilisateurs de s'authentifier à l'aide du **hash de leur mot de passe** au lieu du mot de passe en clair. Lors de cette attaque, un attaquant accède initialement à une machine et extrait les hashes de mot de passe du système (via le fichier **sam** [13] ou le processus LSASS [14]). Plutôt que d'être cracker, ces hashes sont directement utilisés pour une authentification sur d'autres machines du réseau, facilitant ainsi un déplacement pouvant compromettre les ressources critiques ou les comptes à privilèges élevés.
Le succès de cette attaque repose sur plusieurs facteurs : le stockage des hashes de mots de passe sans vérification du mot de passe en clair et le recyclage fréquent des identifiants, notamment pour les comptes administrateurs locaux souvent réutilisés sur plusieurs systèmes. Cela permet à l'attaquant de se servir d'un même hash pour accéder à plusieurs machines.

**Impacts potentiels**

- **Accès à des comptes privilégiés** : L'attaquant peut obtenir les hashes des utilisateurs ayant des comptes privilégiés au sein du domaine.
- **Mouvement latéral rapide** : Avec les hashes valides, l'attaquant peut se déplacer rapidement d'une machine à une autre dans le réseau, augmentant son accès et son contrôle sur les ressources réseaux.

**Mesures de mitigation**

- **Isolation de comptes à hauts privilèges** : Limiter l'utilisation des comptes administratifs aux seules tâches nécessaires.
- **Limitation des points de connexions** : Limitation du nombre de points finaux sur lesquels les utilisateurs disposent de privilèges administratifs.

### 1.3.4 Kerberoasting

Le kerberoasting est une attaque spécifique aux environnements Active Directory ciblant le protocole Kerberos pour en extraire les identifiants de comptes et services, en particulier les mots de passe. Cette attaque tire parti du fait que les tickets kerberos peuvent être obtenus et ensuite attaqués hors ligne pour révéler les mots de passe en clair des comptes de service.

**Description de l'attaque**

Lorsque les utilisateurs ou services demandent à accéder à une ressource protégée, Kerberos génère un Ticket Granting Service [15] qui est chiffré avec le hash du mot de passe du compte de service correspondant. C'est donc cette particularité qu'exploite le kerberoasting. Se déroulant ainsi en quatre phases distinctes, l'attaque de kerberoasting se présente comme suit :

- **Collecte du TGS** : L'attaquant, disposant déjà d'un accès à l'environnement de Active Directory demande un ticket kerberos (TGS) pour accéder à un service spécifique, géré par un compte de service,

- **Extraction et stockage** : Une fois le TGS obtenu, l'attaquant l'extrait et le stocke hors ligne pour un traitement ultérieur,
- **Attaque hors ligne** : À ce stade, l'attaquant lance une attaque de type brute-force[16], dictionnaire (dictionary attack) [17], ou autre méthode similaire pour tenter de casser le hash du mot de passe du compte de service,
- **Accès et exploitation** : Après avoir déchiffré le mot de passe, l'attaquant peut accéder au service et poursuivre son infiltration.

Cette attaque est particulièrement efficace car elle permet à l'attaquant d'effectuer la majorité du travail, comme le cassage de mots de passe, hors ligne. Cela réduit considérablement les chances de détection par les mécanismes de sécurité en place.

#### Impacts potentiels

- **Escalade de privilèges** : Si l'attaquant obtient le mot de passe d'un compte de service à privilège élevé (ex : compte administrateur), il peut compromettre tout le domaine,
- **Accès non autorisé** : Une fois le mot de passe cassé, l'attaquant peut se connecter au service ou à d'autres de manière non autorisé.

#### Mesures de mitigation

- **Complexité des mots de passe pour les comptes de service** : Les mots de passe doivent être longs, complexes et régulièrement changés,
- **Utilisé des comptes gérer** : Les Managed Service Account et Group Managed Service Account [18] changent automatiquement les mots de passe, les rendant ainsi moins vulnérables aux attaques,
- **Limiter les droits de comptes de service** : Réduire au minimum les privilèges accordés aux comptes de service pour limiter l'impact d'une compromission.

## Conclusion

En conclusion de ce chapitre, il ressort que l'Active Directory, bien qu'étant un outil central et puissant pour la gestion des ressources réseau d'une entreprise, est également exposé à de nombreuses vulnérabilités en raison de son utilisation croissante. Il est donc impératif de déployer des mesures de protection adaptées afin de minimiser ces risques et d'assurer une sécurité optimale au sein de l'entreprise.

Chapitre 2

# Exploitations des failles et approches de solutions (Vulnérabilité du protocole SMB)

## Introduction

Une faille est une vulnérabilité dont l'exploitation pourrait engendrer des problèmes majeurs pour la sécurité d'un système. Dans ce chapitre, nous aborderons les vulnérabilités spécifiques au protocole SMB en réalisant divers tests au sein de l'Active Directory. À travers à une série de simulations, nous mettrons en évidences les risques et proposerons des solutions pour renforcer la sécurité et mieux protéger l'environnement AD contre ces menaces.

## 2.1 Importance du protocole SMB

Le protocole SMB (Server Messae Block) joue un rôle essentiel dans le fonctionnement de l'Active Directory en permettantt les communications nécessaires pour le partage de fichiers, d'imprimantes, et de services entre les ordinateurs sous Windows.
Au sein d'un domaine Active Directory, SMB facilite plusieurs opérations cruciales pour la gestion et l'accès aux ressources :

- Partage de fichiers et de ressources : SMB permet aux utilisateurs d'accéder aux dossiers et fichiers partagés sur les serveurs et autres ordinateurs du domaine,
- Authentification et sécurité : SMB Utilise les protocoles de sécurité NTLM ou Kerberos pour une authntification des connexions.

### 2.1.1 Risques liés à SMB dans l'Active Directory

Étant donné son rôle central au sein de l'Active Directory, le protocole SMB présente des risques potentiels pour la sécurité. Des vulnérabilités telles que celles exploitées par le ransomware WannaCry ou l'attaque par relai d'authentification.
Ces risques potentiels nuisent davantage au bon fonctionnement de l'Active Directory.

## 2.2 Exploitation

L'exploitation de cette vulnérabilité suivra le principe du Proof of Concept (POC), permettant de démontrer comment elle peut être exploitée.

### Matériels utilisés

- Un hyperviseur tel que VMWare Workstation Pro 17 pour la mise en place de l'environnement test ;
- Deux systèmes windows Server 2019 Datacenter évaluation, l'un pour le Contrôleur de Domaine et l'autre pour le Serveur de fichiers ;
- Un système Windows 10 pour le poste client ;
- Un système Kali Linux servant de machine attaquante.

### Méthodologie

Avant de commencer les différents tests, des mesures préliminaires ont été prises, telles que la mise en place de l'environnement de travail (VMWare) et l'installation des différentes machines, afin de se conformer au cadre défini. L'infrastructure de base pour la gestion des utilisateurs et des ordinateurs se présente comme suit :

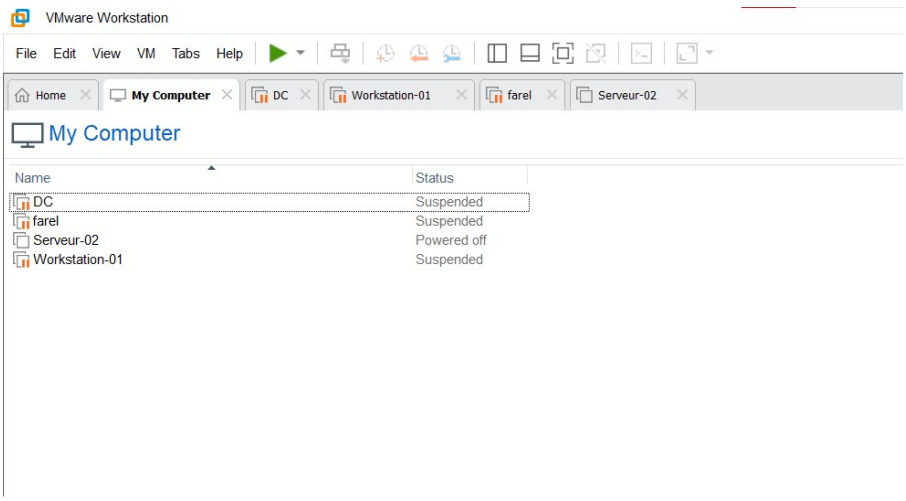



FIGURE 2.1 : Infrastructure globale

Comme illustrer dans la figure 2.1, cette petite infrastructure permettra de mieux comprendre le fonctionnement de l'Active Directory et facilitera l'exploitation de la vulnérabilité ciblée.
L'objectif est de tirée parti d'une des vulnérabilités associées au protocole SMB afin d'accéder à un fichier (flag.txt) situé sur le serveur de fichiers au sein du domaine, en utilisant un compte du domaine. Cela permet de démontrer les risques de sécurité liés à l'accès non autorisé.

Le contrôleur de domaine utilisé dans ce projet est une représentation simplifié et presque conforme à celui de la DGI afin de mieux représenter un environnement de production.

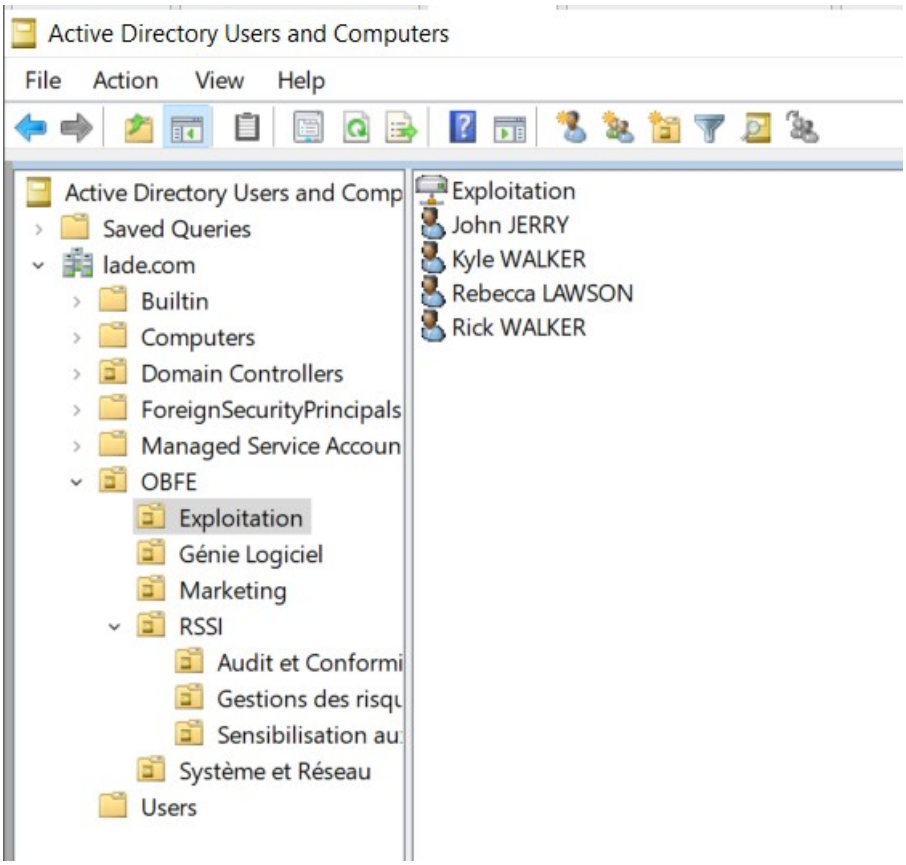



FIGURE 2.2 : Présentation globale du Contrôleur de Domaine

Comme illustrer dans cette figure, chaque utilisateur, groupe, compte, etc, est configuré au sein du Contrôleur de Domaine d'où son rôle de gestion centraliser des ressources.

Une fois tout en place, l'exploitation peut débuter. Cependant, avant de procéder, nous vérifions la présence du protocole SMB pour confirmer son exploitation. À cette fin, nous pouvons utiliser l'outil Nmap :

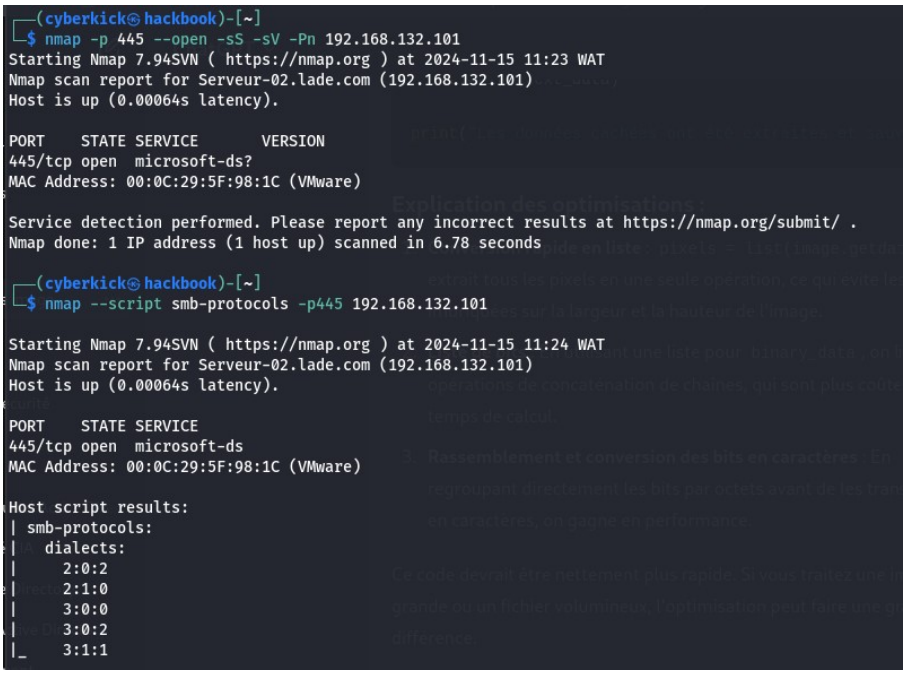



FIGURE 2.3 : Identification de présence

Dans cette figure, nous utilisons deux commandes Nmap pour confirmer la présence du protocole SMB sur le réseau et identifier sa version.

Ainsi fait nous commencons notre exploitation en interceptant les communications réseau impliquant le protocole SMB afin de récupérer les hashes de mot de passe, comme décrit dans l'attaque "Authentication Relays". Cela peut être réalisé en utilisant l'outil **Responder**, permettant d'intercepter les requêtes SMB non sécurisées sur le réseau, avec la commande : **sudo responder -I eth0**.
Cette commande configure Responder pour écouter sur l'interface réseau spécifiée (eth0) et capturer les requêtes SMB et NTLM associées, envoyées par les machines sur le réseau.

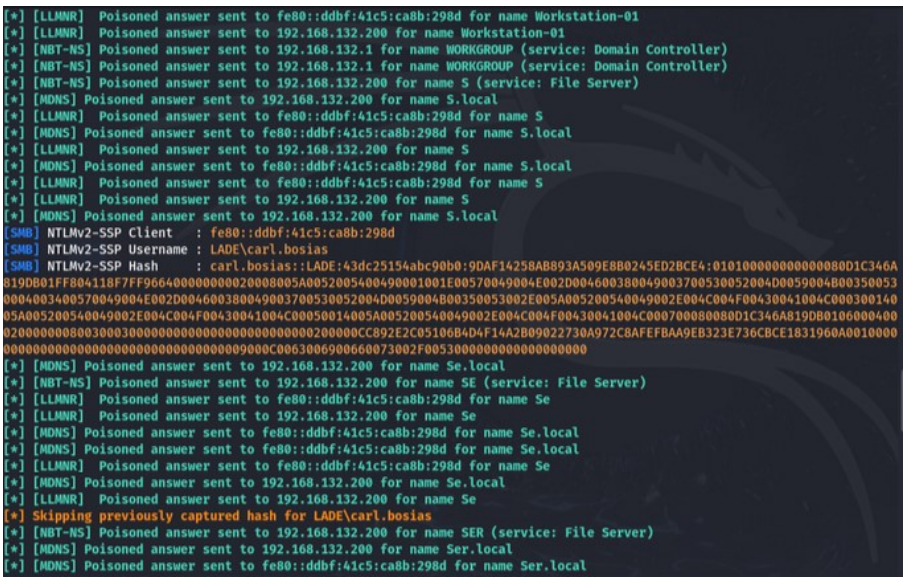



FIGURE 2.4 : Hash de l'utilisateur capturé

Une fois le hash récupéré, comme indiqué par la figure précedente nous allons maintenant le craquer afin de pouvoir récupérer le mot de passe de l'utilisateur.
La commande suivante nous aide dans ce but : **hashcat -m 5600 carl_hash pass.txt –force**.




FIGURE 2.5 : Mot de passe craqué de l'utilisateur

La figure 2.4 montre le mot de passe récupéré de l'utilisateur après l'opération de craquage, réalisée en utilisant pass.txt qui contient une liste de mots de passe générée à partir d'informations collectées au préalable. Ce fichier sert de base pour tester diverses combinaisons jusqu'à trouver le mot de passe correct.

Une fois le mot de passe obtenu on peut procéder à l'énumérattion des dossiers partagés sur le serveur de fichiers en exécutant la commande suivante : **crackmapexec smb 192.168.132.101 -u "carl.bosias" -p "c4rl_p4ss*." –shares**

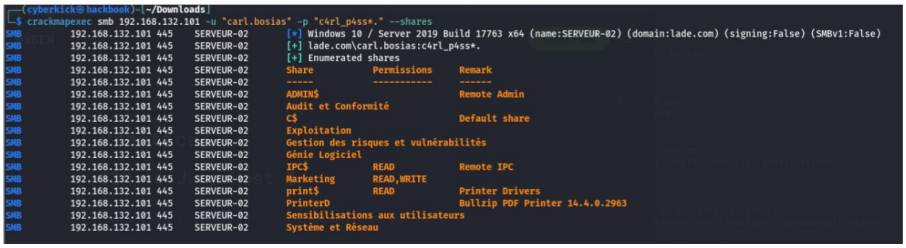



FIGURE 2.6 : Listing des dossiers partagés

Cette commande utilise l'outil **CrackMapExec** pour scanner le serveur SMB à l'adresse 192.168.132.101 avec les informations d'identifications de l'utilisateur "carl.bosias". L'option "–shares" permet d'afficher les ressources partagées accessibles avec les privilèges disponibles.
Dans cette figure on remarque ainsi les ressources auxquels l'utilisateur à accès, notamment le dossier **Gestion_AD**, qui contient le fichier flag.txt. Ce dossier représentant une ressource critique au sein du domine.

Il nous faut maintenant lire ce dossier afin de récupérer le fichier. Nous pouvons le faire grâce à l'outil **smbclient** : **smbclient -U lade.com\\carl.bosias \\\\192.168.132.101\\Gestion_AD**

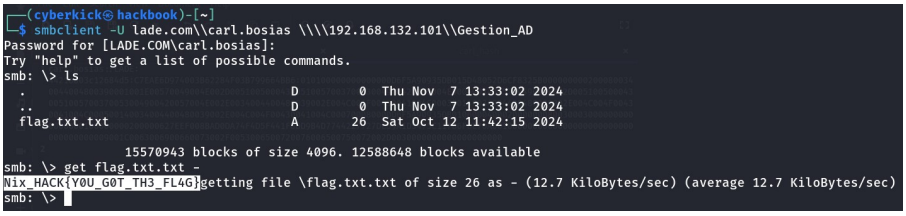



FIGURE 2.7 : Obtention du flag

La lecture du fichier flag.txt démontre ainsi l'accès non autorisé obtenu via l'exploitation, constituant une violation flaglante du principe de confifentialité l'un des piliers fondamentaux de sécurité informatique. Cette exploitation met en évidence les failles présentes et leur capacité à compromettre des données sensibles au sein de l'infrastructure Active Directory, soulignant l'importance de renforcer les mesures de sécurité pour protéger les ressources critiques.

## 2.3 Proposition de Solutions aux vulnérabilités

La sécurisation de l'Active Directory nécessite une approche globale, en protégeant chaque point, chaque niveau, et toutes les fonctionnalités qui assurent son fonctionnement.

### 2.3.1 Solutions spécifiques au protocole SMB

Pour limiter les attaques comme l'Authentication Relay, les mesures suivantes doivent être adoptées :

- Désactivation de SMB : Remplacer SMBv1 par SMBv2 ou SMBv3, plus sécurisés,
- Signature SMB : Activer la signature des communications pour protéger l'intégrité des données,
- Configuration NTLMv2 : Privilégier NTLMv2 pour renforcer les mécanismes d'authentification.
- Permissions strictes : Appliquer des permissions rigoureuses sur les ressources partagées,
- Restriction de l'accès au port 445 : Bloquer l'accès externe au port 445 et limiter son usage aux segments internes du réseau.

### 2.3.2 Contrôles d'accès et autorisations

Les contrôles d'accès visent à réguler et surveiller les accès pour minimiser les risques, en s'appuyant sur :

- Principe du moindre privilège : Attribuer uniquement les droits nécessaires aux utilisateurs, machines et applications, réduisant ainsi la surface d'attaque. Cela nécessite une bonne compréhension des rôles pour limiter les comptes avec privilèges élevés.
- Utilisation des groupes pour gérer les privilèges : Les droits sont attribués à des groupes de sécurité spécifiques, simplifiant l'administration en permettant une gestion centralisée et cohérente des autorisations.

### 2.3.3 Configurations de sécurité

Les configurations de sécurité regroupent des mesures techniques et organisationnelles pour protéger les systèmes et réduire les risques d'attaques, notamment :

- Durcissement des systèmes :
  - Fermant les ports réseau inutilisés,
  - Désactivant les services non essentiels,

  - Supprimant les comptes par défaut.

- Configuration des stratégies de groupe (GPO) : Utiliser des paramètres centralisés pour sécuriser les machines et les utilisateurs, avec des avantages tels que :
  - Gestion centralisée des politiques,
  - Cohérence des configurations,
  - Mise en œuvre rapide des modifications.

## Conclusion

Les vulnérabilités Active Directory proviennent principalement de fonctionnalités, et de composants intégrés, qui, en raison de mauvaises gestions, configurations ou utilisations deviennent des menaces susceptibles d'entraîner de graves conséquences pour le fonctionnement d'une entreprise. Il est donc essentiel d'adopter une utilisation correcte, surveillée, consciente et responsable de l'Active Directory afin de s'assurer un minimum de sécurité.

Chapitre 3

# Résultats des implémentations et recommandations

## Introduction

Dans ce chapitre, nous présenterons les résultats obtenus suite à la mise en œuvre des solutions visant à protéger notre environnement, puis nous formulerons quelques recommandations afin de maintenir une posture de sécurité robuste.

## 3.1 Résultats

En rapport avec les solutions proposées lors du chapitre précédent, une implémentation a été effectuée dans notre infrastructure afin de démontrer les résultats obtenus suite à leur application. Ces résultats mettent en évidence l'efficacité des mesures adoptées pour renforcer la sécurité de l'Active Directory, notamment en ce qui concerne les vulnérabilités liées au protocole SMB : Désactivation de SMBv1 et activation de SMBv2 ou v3, activation de la signature SMB, désactivation NTLM.

Ces configurations, ainsi que d'autres mesures, ont été appliquées via les politiques de groupe en suivant le chemin suivant : **Computer configuration > Policies > Windows settings > Security Settings > Local Policies > Security Options**.
Les figures suivantes illustreront les paramètres activés et leurs impacts sur la sécurité de l'infrastructure Active Directory.

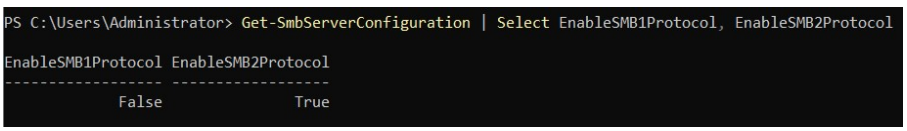



FIGURE 3.1 : Vérification de la présence du protocole SMB

Dans cette figure nous vérifions l'utilisation du protocole SMBv2 au sein du réseau. Cette utilisation nous assure une meilleure gestion des communications de partage de fichiers, et des authentifications au sein du réseau.

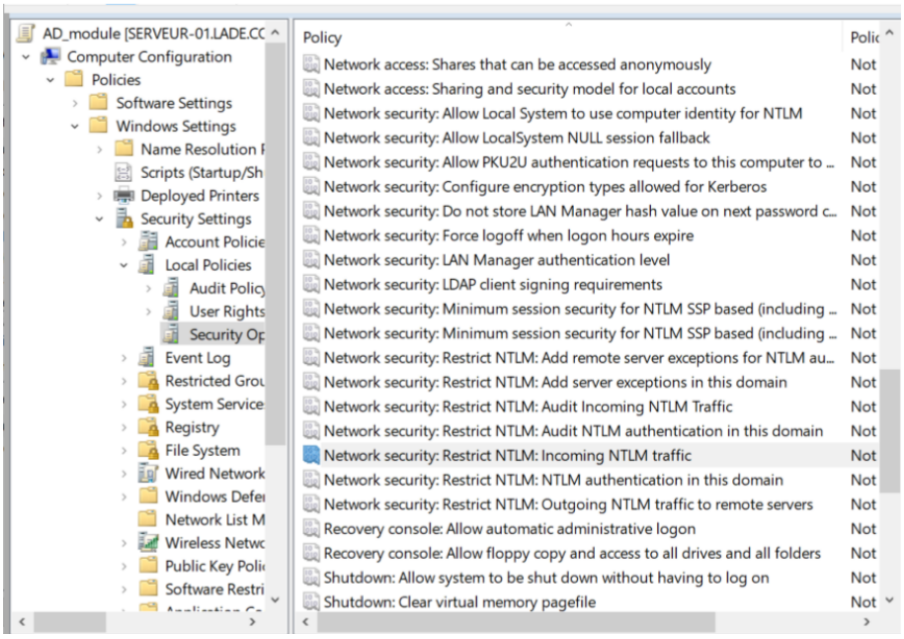



FIGURE 3.2 : Restriction de NTLM et signature SMB

A ce niveau nous effectuons les configurations nécéssaires au sein des politiques de sécurité pour mettre en place les mesures recommandées précédemment, et après avoir appliqué ces modifications, nous effectuons une nouvelle tentative d'attaque par "Authentication Relays".

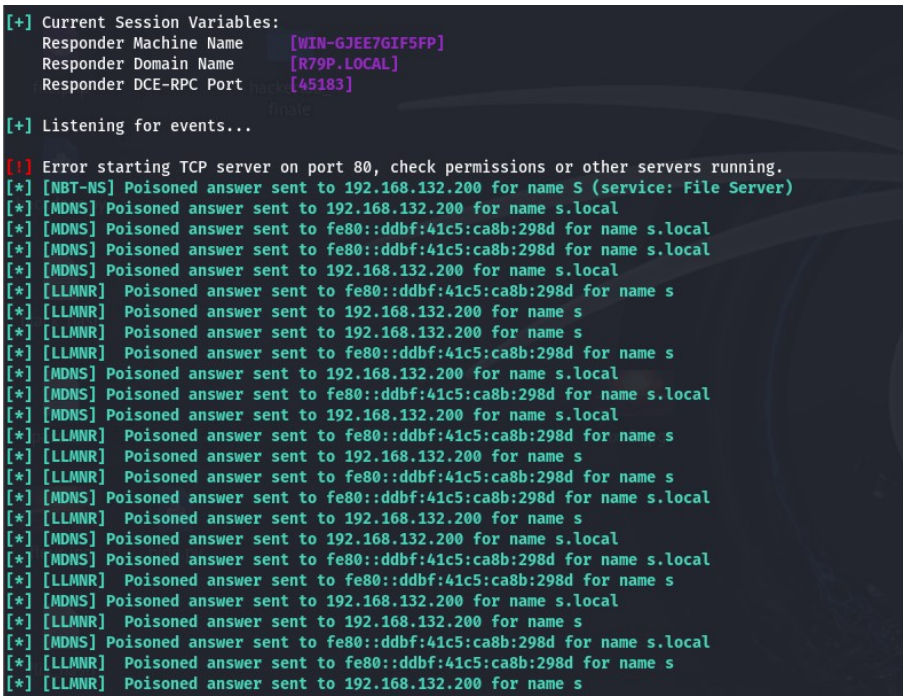



FIGURE 3.3 : Nouvelle tentative d'attaque

Les résultats montrent que, suite à l'application des solutions de sécurité, l'attaque n'est plus facilement exploitable. Cela prouve que les mesures mises en place ont efficacement renforcé la sécurité de l'infrastructure Active Directory, en protégeant mieux les communications réseau contre les attaques de type relais d'authentification.

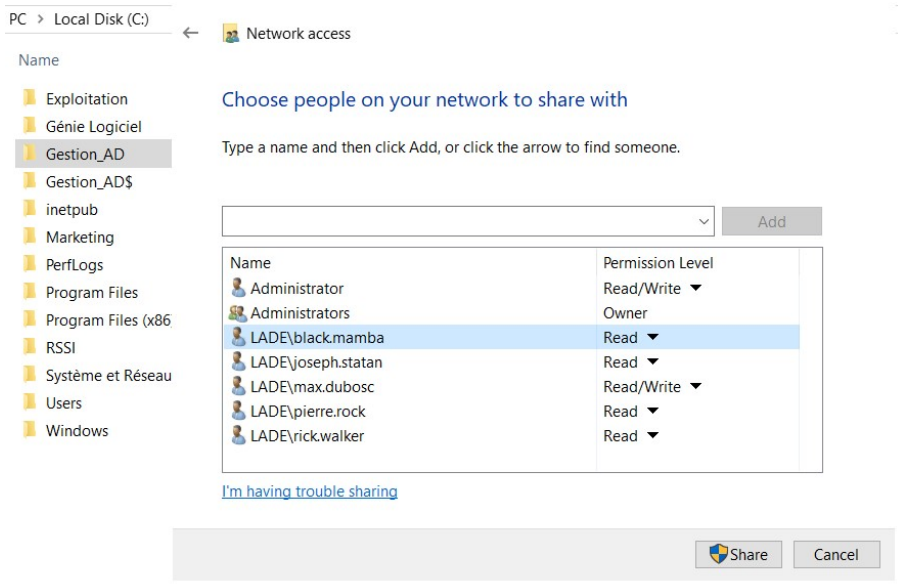



FIGURE 3.4 : Restrictions des accès

Cette figure ci nous montre les accès sur le fichier Gestion_AD qui est désormais restreint afin de se conformer aux nouvelles politiques de sécurité.

## 3.2 Recommandations

### 3.2.1 Formation des utilisateurs

Former les utilisateurs et les administrateurs sur les meilleures pratiques de sécurité, y compris l'utilisation de mots de passe forts, et la gestion des comptes à privilèges.

### 3.2.2 Recyclage des compétences

Pour s'assurer que les compétences restent à jour et les administrateurs conscients des nouvelles technologies ou menaces, il est essentiel de régulièrement programmés des ateliers. Ces sessions permettent aux administrateurs d'apprendre de nouvelles notions dans leur domaine, d'approfondir leurs connaissances, de consolider leurs compétences et de s'enrichir de nouvelles pratiques. Ainsi, ils seront mieux équipés pour exercer leurs fonctions et réagir efficacement face aux évolutions et aux menaces émergentes.

### 3.2.3 Mise à jour

Rien n'étant figé dans le temps, tout système, robuste tel qu'il soit peut devenir vulnérable après une période donnée. Il est donc conseillé de régulièrement mettre à jour les systèmes, les ressources et machines pour garantir leur pérennité face aux vulnérabilités émergentes. Il va sans dire que ces mises à jour doivent provenir de sources fiables pour éviter d'introduire de nouveaux risques.

### 3.2.4 Tests de sécurité

Afin de s'assurer de la résistance du réseau face aux vulnérabilités et failles de sécurité, il est préférable d'effectuer périodiquement des tests de sécurité. Ces tests permettent d'identifier les faiblesses

existantes, les nouvelles vulnérabilités apparues, ou celles qui persistent malgré les mesures de sécurité mises en place. Comme test de sécurité nous avons :

- **Test de pénétration (Pentest)** : Consistant à simuler des attaques pour identifier les vulnérabilités exploitables. Il évalue la robustesse des systèmes en reproduisant les techniques utilisées par des attaquants potentiels,
- **Audit de sécurité** : Visant à examiner les politiques, les configurations et les pratiques de sécurité pour vérifier leur conformité avec les normes de sécurité. Il identifie les écarts par rapport aux bonnes pratiques et aux exigences réglementaires,
- **Analyse de vulnérabilité** : Utilisant des outils automatisés pour scanner les systèmes et les réseaux à la recherche de vulnérabilités connues, il permet de rapidement détecter des failles potentielles et de recommander des actions correctives.

## 3.3 Contributions

Ce travail a permis de mettre en lumière plusieurs contributions significatives dans le domaine de la sécurisation de l'Active Directory :

- **Simulation technique et vailidation expérimentale** : Une infrastructure Active Directory simulée a été mise en place, intégrant un contrôleur de domaine, un serveur de fichiers et un poste client. Cette simulation a permis d'identifier les vulnérabilités du protocole SMB et de valider les contres-mesures proposées.
- **Analyse approfondie des vulnérabilités SMB** : L'exploitation des failles via des outils comme Responder et CrackMapExec a permis de démontrer le risque concret de compromission. Ces attaques ont été documentées étape par étape pour assurer leur reproductibilité à des fins pédagogiques.
- **Implémentation et test des solutions** : Les configurations suivantes ont été testées et validées dans l'environnement simulé :
  - Désactivation de SMBv1 et adoption de SMBv2/v3.
  - Signature SMB pour sécuriser les communications.
  - Restrictions au protocole NTLM.
    Les résultats obtenus montrent une amélioration notable de la sécurité en empêchant des attaques telles que Pass-the-Hash ou Authentication Relay.
- **Impact pratique des recommandations** : Les recommandations formulées (chapitre 3.2) offrent une base solide pour sécuriser les infrastructures réelles. Elles sont directement applicables dans un contexte professionnel, comme celui de la DGI où des environnements similaires existent.

## Conclusion

Ce chapitre nous a permis de présenter les résultats obtenus après la mise en place des différentes solutions au sein de notre Active Directory et ainsi de formuler des recommandations utiles pour le maintien et la pérennité d'une sécurité globale au sein des réseaux.

# Conclusion Générale

L'Active Directory est un composant clé pour la gestion des identités, des accès et des ressources, mais il est exposé à des vulnérabilités qui peuvent compromettre la sécurité du réseau. Ce travail a permis de contribuer à l'analyse approfondie des vulnérabilités liées au protocole SMB, notamment l'Authentication Relay, en simulant leur exploitation dans un environnement Active Directory complet. Grâce à ces simulations, des solutions concrètes ont été implémentées, telles que la désactivation de SMBv1, l'activation de SMBv2 et de la signature SMB, démontrant une amélioration significative de la sécurité.

En outre, ce projet propose une méthodologie reproductible pour identifier et corriger les failles, et offre des recommandations pratiques adaptées aux environnements réels, comme celui de la DGI, pour renforcer leur posture de sécurité. Enfin, l'intégration de l'intelligence artificielle est envisagée comme une solution prometteuse pour automatiser la gestion des comptes, détecter les anomalies et optimiser la sécurité globale des environnements Active Directory, ouvrant ainsi la voie à des systèmes plus résilients et adaptatifs.

# Webographie


[1] Présentation des services de domaine Active Directory https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview, Consulté le 10 Avril 2024.

[2] Active Directory https://fr.wikipedia.org/wiki/Active_Directory, Consulté le 19 Avril 2024.

[3] Régistre Windows https://www.avg.com/fr/signal/windows-registry, Consulté le 20 Avril 2024.

[4] HackTheBox, "Introduction to Active Directory." https://academy.hackthebox.com/module/details/74, Consulté le 20 Avril 2024

[5] Groupes Active Directory https://learn.rdr-it.io/Le%C3%A7on/groupes-active-directory/ Consulté le 22 Avril 2024.

[6] HackTheBox, "Introduction to Active Directory." https://academy.hackthebox.com/module/details/74

[7] RDR-IT -Cours, "Définition de domaine, arbre et forêt" https://learn.rdr-it.io/Leçon/definition-de-domaine-arbre-et-foret/

[8] RDR-IT -Cours, "Définition de domaine, arbre et forêt" https://learn.rdr-it.io/Leçon/definition-de-domaine-arbre-et-foret/

[9] Les 10 attaques les plus connues de l'Active Directory (AD) et comment se protéger https://www.linkedin.com/pulse/les-10-attaques-les-plus-courantes-de-lactive-directory-ad-minou-djeukui-alvse/ Consulté le 04 Mai 2024.

[10] NTLM https://www.crowdstrike.fr/cybersecurity-101/ntlm-windows-new-technology-lan-manager/ Consulté le 05 Mai 2024.

[11] Qu'est ce que le protocole LDAP ? https://www.ionos.fr/digitalguide/serveur/know-how/ldap/ Consulté le 07 Mai 2024.

[12] Explication de l'authentification Kerberos https://www.varonis.com/fr/blog/explication-de-lauthentification-kerberos Consulté le 07 Mai 2024.

[13] Security Account Manager https://fr.wikipedia.org/wiki/Security_Account_Manager Consulté le 10 Mai 2024.

[14] Local Security Authority System Service https://fr.wikipedia.org/wiki/Local_Security_Authority_Subsystem_Service Consulté le 10 Mai 2024.

[15] Kerberos Principe de Fonctionnement https://blog.devensys.com/2018/07/18/kerberos-principe-de-fonctionnement/comment-page-1/ Consulté le 11 Mai 2024.

[16] Attaques brute force : principes et bonnes pratique de sécurité https://www.vaadata.com/blog/fr/attaques-brute-force-principes-et-bonnes-pratiques-securite/ Consulté le 11 Mai 2024.

[17] Dictionary attack https://www.techtarget.com/searchsecurity/definition/dictionary-attack Consulté le 11 Mai 2024.

[18] Active Directory -gMSA https://www.it-connect.fr/active-directory-utilisation-des-gmsa-group-managed-service-accounts/ Consulté le 12 Mai 2024.

# Table des matières

**Liste des acronymes** 1

**Dédicace** ii

**Remerciements** iii

**Résumé** iv

. . . . . iv

**Abstract** v

. . . . . v

**List of Figures** vi

**Liste des acronymes** vii

**Introduction** 1

0.1 Objectifs . . . . . 1

0.1.1 Objectifs spécifiques . . . . . 1

0.2 Organisation du travail . . . . . 2

**1 Revue de littérature** 3

Introduction . . . . . 3

1.1 Objets . . . . . 4

1.1.1 Groupe . . . . . 4

1.1.1.1 Étendus des groupes . . . . . 4

1.1.1.2 Stratégie de Groupe (GPO) . . . . . 5

1.2 Forêts Arborescence, Arbres et Domaine . . . . . 5

1.2.1 Arborescence et Arbres . . . . . 6

1.2.2 Domaine . . . . . 7

1.3 Vulnérabilités de l'Active Directory . . . . . 7

1.3.1 Authentication relays . . . . . 8

1.3.2 LDAP . . . . . 9

1.3.3 Pass-The-Hash . . . . . 9

1.3.4 Kerberoasting . . . . . 10

Conclusion . . . . . 11

**2 Exploitations des failles et approches de solutions (Vulnérabilité du protocole SMB)** 12

Introduction . . . . . 12

2.1 Importance du protocole SMB . . . 12
2.1.1 Risques liés à SMB dans l'Active Directory . . . 12
2.2 Exploitation . . . 13
2.3 Proposition de Solutions aux vulnérabilités . . . 17
2.3.1 Solutions spécifiques au protocole SMB . . . 17
2.3.2 Contrôles d'accès et autorisations . . . 17
2.3.3 Configurations de sécurité . . . 17
Conclusion . . . 18

**3 Résultats des implémentations et recommandations 19**
Introduction . . . 19
3.1 Résultats . . . 19
3.2 Recommandations . . . 21
3.2.1 Formation des utilisateurs . . . 21
3.2.2 Recyclage des compétences . . . 21
3.2.3 Mise à jour . . . 21
3.2.4 Tests de sécurité . . . 21
3.3 Contributions . . . 22
Conclusion . . . 22

**Conclusion 24**

**Webographie 25**

**Table des matières 27**