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 :
Gbééré Achille **EYE**

Test de pénétration d'une infrastructure Active Directory: cas de l'entreprise LAG Solutions

Sous la supervision :
M. Laurel **LISHOU**

Membres du jury :

Dr Vinasétan Ratheil HOUNDJI	Enseignant-chercheur	IFRI	Président
Ing. Mawuénan Hervé AKAPKPO	Enseignant	IFRI	Examinateur
M. Laurel LISHOU	Enseignant	IFRI	Rapporteur

Année Académique : **2021-2022**

Sommaire

Dédicace ii

Remerciements iii

Résumé iv

Abstract v

Liste des figures vi

Liste des tableaux vii

Liste des acronymes viii

Glossaire 1

Introduction 2

1 Revue de littérature 4

2 Analyse, Choix, Justification 10

3 Test de pénétration, résultats et recommandations 14

Conclusion 26

Bibliographie 27

Webographie 28

Table des matières 30

Dédicace

À
Dieu et à toi *Olaoumi Mathias EYE* pour la bonne influence que tu as eue sur moi et qui m'a permis d'évoluer à ce niveau où je suis aujourd'hui, bien qu'il reste du chemin à faire encore.
À coup sûr, tu es un inspirant modèle d'excellence. À nos succès !

Remerciements

Nous remercions en premier lieu l'Éternel Dieu pour le souffle de vie et la grâce immense qu'Il ne cesse de nous accorder et à tous ceux qui ont contribué à ce travail.
Nous remercions notre maître de mémoire, M. Laurel LISHOU, pour avoir accepté nous accompagner dans ce travail. Merci pour votre soutien et encadrement.
Nous adressons nos remerciements au Prof Eugène C. EZIN pour son leadership, son sens d'écoute, et l'accompagnement qu'il ne cesse de faire preuve envers les étudiants de l'Institut dont il a la charge.
Nous remercions également toute l'administration de l'IFRI et tous les enseignants pour leurs efforts au quotidien pour nous fournir une formation de qualité.
Nous ne finirons pas sans adresser nos sincères remerciements à toutes les personnes qui ont contribué de près ou de loin à ce travail en particulier et à notre formation en général. Il s'agit notamment de :

- Toute la communauté des boursiers de la Mastercard Foundation à l'Université d'Abomey-Calavi avec qui nous avons passé de bons moments d'entraîde et de solidarité, avec un regard particulier à l'équipe de la Coordination de ce programme de bourses dont Prof Enoch G. ACHIGAN-DAKO à sa tête ;
- Toute la communauté des étudiants de l'IFRI et particulièrement nos camarades de la 6ème promotion ;
- Nos parents, amis et toutes les personnes dont les noms ne sont pas explicitement mentionnés mais qui nous ont soutenu d'une manière ou d'une autre, nous vous prions de recevoir nos sincères gratitudes également ;
- Sans nul doute, le président et les membres du jury qui ont accepté évaluer notre modeste travail et contribuer à son amélioration de par leurs suggestions et apports.

Résumé

Selon une estimation de Fortune 1000, près de 90% des entreprises corporates utilisent le service d'annuaire Windows Active Directory pour gérer l'authentification, l'accès et la gestion des ressources (ordinateurs, comptes utilisateurs, serveurs, stratégie de groupe, ...). Néanmoins, il n'est pas rare de constater au sein des entreprises qu'il existe des problèmes de mauvaise configuration, de mauvaise gestion, du manque de mise à jour dans les infrastructures Active Directory qui constituent pourtant le centre névralgique de tout le système d'informations. Cela rend ces infrastructures vulnérables et expose ces entreprises à des risques d'attaques dont les conséquences sont souvent lourdes. Dans un tel contexte, afin de contribuer à la sécurité des infrastructures Active Directory, nous avons mis en lumière à travers ce projet quelques vulnérabilités les plus récentes qui touchent les infrastructures Active Directory et nous avons déroulé une attaque en guise de preuve de concept en se servant du cas de l'entreprise LAG Solutions. L'objectif ultime poursuivi est d'attirer l'attention des administrateurs systèmes sur la nécessité d'appliquer les correctifs nécessaires sur leur parc informatique dès que ceux-ci sont publiés tout en respectant les procédures d'usage.

Mots clés : Active Directory, Windows Server, Administration des réseaux, Gestion d'identité et d'accès, Test de pénétration

Abstract

According to an estimate by Fortune 1000, almost 90% of corporate businesses use the Windows Active Directory service to manage authentication, access and resource management (computers, user accounts, servers, group policy, etc.). Nevertheless, it is not uncommon for companies to find problems of misconfiguration, mismanagement and lack of updating in Active Directory infrastructures, which are the nerve center of the entire information system. This makes these infrastructures vulnerable, and exposes companies to the risk of attacks, often with far-reaching consequences. Against this backdrop, and with a view to contributing to the security of Active Directory infrastructures, we have used this project to highlight some of the most recent vulnerabilities affecting Active Directory infrastructures, and have carried out a proof-of-concept attack using LAG Solutions as a case study. The ultimate aim is to draw the attention of system administrators to the need to apply the necessary patches to their IT assets as soon as they are released, while respecting standard procedures.

Key words: Active Directory, Windows Server, Network administration, Identity and Access Management, Penetration testing

Liste des figures

1.1 Hiérachisation des ressources avec Active Directory 5

3.1 Logo de l'outil Nmap 16
3.2 Logo de l'outil Bloodhound 17
3.3 Logo de l'outil CrackMapExec 18
3.4 Résultats de scan du réseau avec Nmap 19
3.5 Collecte des informations sur le contrôleur de domaine 20
3.6 NetBIOS name du contôleur de domaine 21
3.7 Exploitation de la vulnérabilité zerologon 22
3.8 Hashes des mots de passe des comptes 23
3.9 Connexion au compte administrateur du contrôleur de domaine via le shell 24

Liste des tableaux

1.1 Norme X500 [20] 8

Liste des acronymes

AAD :

Azure Active Directory

AD :

Active Directory

CVE :

Common Vulnerabilities and Exposures

DNS :

Domain Name System 6,

ISO/CEI :

International Organization for Standardization/Commission électrotechnique internationale

LDAP :

Lightweight Directory Access Protocol 6, 8, 11, 31,

MVS :

Multiple Virtual Storage (an IBM operating system) 7,

NAS :

Network Access Server

NIS :

Network Information Service 7,

NTLM :

Windows New Technology LAN Manager

PROFS :

IBM Professional Office System 7,

SMB :

Server Message Block 7,

UIT-T :

Secteur de standarisation des Télécommunications de l'Union Internationale des Télécommunications

Glossaire

attaque : selon le CNSS (Committee on National Security Systems), **une attaque** est tout type d'activité malveillante qui tente de collecter, de perturber, de refuser, de dégrader ou de détruire les ressources du système d'information ou l'information elle-même. 2, 8

Kerberos : est un protocole d'authentification. C'est l'un des protocoles d'authentification utilisés dans Active Directory 6

sAMAccountName : est un attribut unique sur tous les principaux de sécurité dans Active Directory et inclut les utilisateurs, les groupes et les ordinateurs. 9

Introduction Générale

L'administration des réseaux et systèmes informatiques n'est toujours pas une tâche aisée. Les administrateurs utilisent parfois des outils qui leur facilitent la vie dans leur rôle d'administrateur. Ainsi, Active Directory, qui est un service d'annuaire et qui permet de centraliser la gestion des objets d'un annuaire est un de ces outils que les administrateurs systèmes utilisent. A ce titre, Active Directory constitue un centre névralgique de l'infrastructure informatique et il devient donc impératif de s'assurer de la bonne configuration de celui-ci afin que l'organisation ne soit pas victime des attaques persistantes sachant que la plupart des entreprises ne font pas les mises à jour de sécurité, font une installation de leur contrôleur de domaine avec les options par défaut et l'application des stratégies de groupes pour appliquer des options de sécurité supplémentaires sur les objets qui sont administrés.
C'est dans ce cadre que nous nous proposons de mener notre travail de recherche de fin de formation sur le test de pénétration d'une infrastructure Active Directory afin de faire prendre conscience de l'exposition aux attaques aux administrateurs et à tous les autres acteurs impliqués dans la gestion et l'usage d'une telle infrastructure pour une meilleure sécurité de l'organisation.

1. Problématique

Dans beaucoup d'attaques informatiques surtout les attaques par rançongiciels que subissent les entreprises, Active Directory a été le point d'entrée des attaquants. L'attaque visant Colonial Pipeline aux Etats-Unis en mai 2021 en est un exemple parmi tant d'autres. Alors que ces attaques coûtent énormement aux entreprises victimes : la dégradation ou la perte de leur image de marque ou de leur réputation, les pertes financières, la perte de la confiance des clients, les sanctions par les autorités de régulation, la cessation des opérations, etc. Pourquoi Active Directory constitue le point d'entrée de certaines attaques ? Par quels moyens pourrait-on y rémedier ?

2. Contexte et justification

LAG Solutions est une société de droit béninois créée en 2020 et dont le but est d'être l'un des acteurs importants du secteur des intégrateurs de solutions de la place. LAG Solutions est spécialisée dans la fourniture des systèmes, du déploiement des réseaux, de la vente du matériel et du développement d'applications. Elle travaille en étroite collaboration avec plusieurs éditeurs de solutions de sécurité

et solutions diverses afin de proposer à ses clients une large gamme de produits et services. Elle est située à Sainte Rita au Carré 1527 Maison ADJOVI. Le capital de LAG Solutions est de 2 millions de F CFA.

L'entreprise LAG Solutions dispose d'un environnement d'homologation qui leur permet de faire des tests sur des applications nécessitant le protocole LDAP pour l'authentification des utilisateurs. C'est cet environnement comportant un clone des contrôleurs de domaine en production qui nous a permis de réaliser notre test. Notre travail a consisté à pentester un des contrôleurs de domaine pour relever les vulnérabilités qui s'y trouve afin de formuler des recommandations à l'administrateur système en vue de les corriger.

3. Objectifs

L'objectif général de ce projet est de contribuer à la sécurité de l'infrastructure Active Directory au sein de l'entreprise LAG Solutions. De manière spécifique, notre travail de recherche permettra :

- de relever les vulnérabilités que pourrait avoir une infrastructure Active Directory ;
- d'exploiter au moins une de ces vulnérabilités afin de démontrer l'exposition de l'entreprise face aux attaques ;
- de faire des recommandations afin de faire prendre conscience par rapport à l'exposition aux risques et à l'importance d'appliquer les mises à jour de sécurité ;
- de faire suivre les bonnes pratiques pour sécuriser les infrastructures Active Directory au sein de l'entreprise.

4. Organisation du mémoire

Ce document de mémoire est organisé en trois (03) chapitres dont le premier fait l'état de l'art des services d'annuaire notamment Active Directory avec les problèmes de sécurité qui se posent ; ensuite le deuxième chapitre fait l'analyse des différentes méthodes de déploiement de l'Active Directory puis le choix justifié du déploiement au sein de l'entreprise LAG Solutions ; enfin le troisième chapitre présente le test de pénétration, les résultats obtenus et formule des recommandations.

Chapitre 1

Revue de littérature

Introduction

Dès lors que le système informatique de votre entreprise ou organisation dispose de plusieurs ressources dont le nombre accroît, gérer ces ressources devient complexe et nécessite parfois l'utilisation des outils appropriés selon les besoins. Ainsi, il n'est pas rare de constater l'utilisation de Active Directory au sein des entreprises.
Dans ce chapitre, nous allons définir et clarifier Active Directory, son organisation et fonctionnement puis exposer quelques problèmes de sécurité liés à Active Directory tout en passant par l'historique des services d'annuaire jusqu'à Active Directory.

1.1 Généralités sur Active Directory

1.1.1 Définition : Active Directory

Active Directory est un service d'annuaire d'entreprise de Microsoft et est utilisé par prêt de 90% des entreprises [6]. Active Directory est une base de données qui contient des informations sur les objets d'un réseau et permet aux administrateurs de gérer les ressources de l'organisation. Autrement, on peut voir Active Directory comme un carnet d'adresses et un annuaire téléphonique, tout en gardant en tête la différence près qu'Active Directory dispose de beaucoup plus d'options dédiées aux administrateurs pour gérer, modifier, interroger et structurer les données utilisateur et objet stockés. Grâce à Active Directory, l'infrastructure informatique d'une organisation peut être subdivisée en « domaines » de manière à en obtenir une représentation claire.

1.1.2 Mission et fonction de Active Directory

Au sein d'une entreprise ou une organisation de 200 employés ou plus par exemple, ces derniers ont grandement besoin des différentes composantes de l'infrastructure informatique de l'entreprise : qu'il s'agisse des comptes utilisateurs, des scanners, des imprimantes, et du partage des autorisations sur les ordinateurs de différents groupes de travail. On s'en doute donc qu'une gestion, au cas par cas pour chaque poste de travail, des ressources informatiques serait fastidieuse et presqu'impossible. C'est alors là qu'Active Directory intervient et permet de représenter les différentes structures

de l'entreprise, sauvegarder les données utilisateur et objet, gérer et distrubier les autorisations de manière centralisée. L'administrateur système n'aura plus qu'à se concentrer sur l'administration de Active Directory et l'accès en écriture aux ressources informatiques.
Active Directory permet essentiellement d'accomplir les tâches suivantes : [12]

- l'organisation hiérarchique et la représentation des ressources informatiques internes, des utilisateurs et objets (matériel, logiciels, rôles d'utilisateur et composants/périphériques/services de réseau) ;
- la gestion et l'organisation de l'espace de stockage ;
- le partage et le verrouillage des droits d'accès et d'application (par exemple : sur les annuaires et les services) ;
- la sauvegarde et la protection du réseau de l'entreprise ;
- la sauvegarde des données utilisateur et objet, la gestion et la distribution des autorisations de manière centralisée.

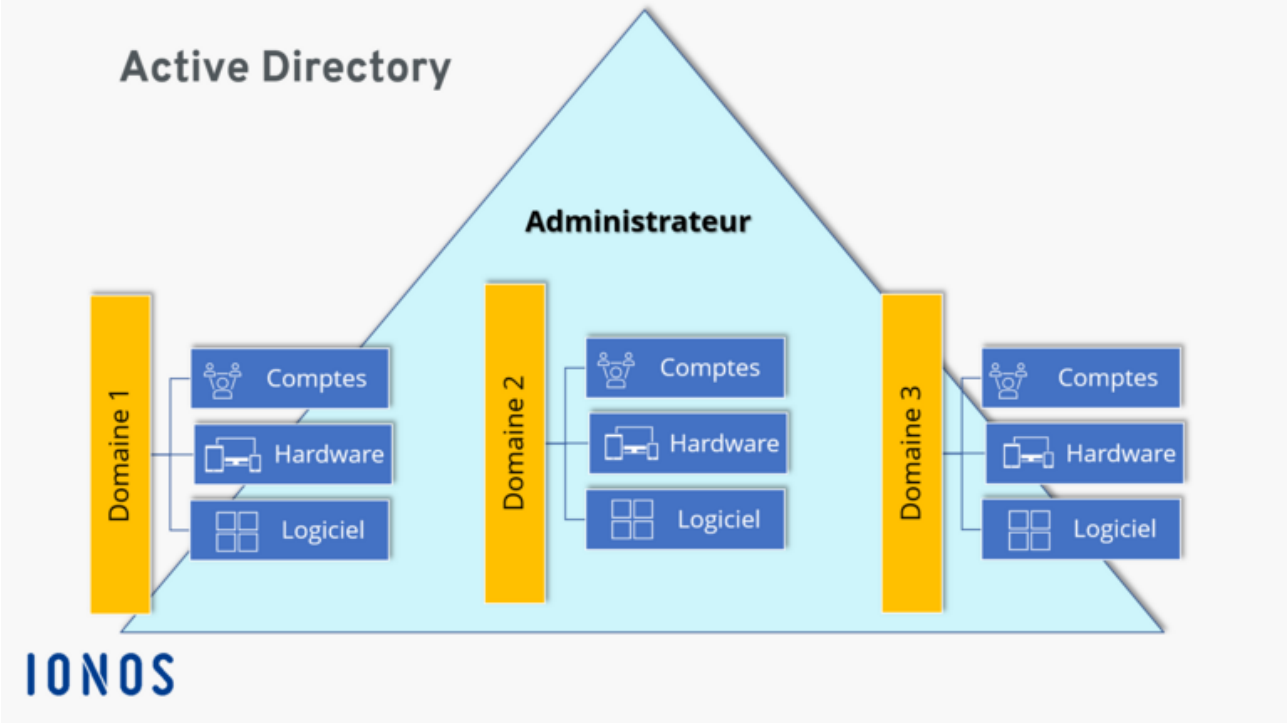


FIGURE 1.1 : Hiérachisation des ressources avec Active Directory

1.1.3 Structure de Active Directory

Active Directory est organisé d'une manière hiérachique et dispose de plusieurs composants pour son fonctionnement. Quatre composants centraux forment Active Directory à savoir : **schéma, configuration, domaine et base de données**.

1.1.3.1 Schéma

Le **schéma AD** est un composant qui sert de modèle aux classifications et types d'entrées AD requis et autorisés. Il s'agit notamment des objets, y compris les attributs, les classes et la syntaxe des attributs.

Le schéma utilise des définitions pour déterminer quels objets sont disponibles ou peuvent être mis à disposition dans le réseau.

1.1.3.2 Configuration

Pendant que le schéma définit les contenus possibles, la **configuration AD** représente la structure d'Active Directory et de tous les objets, rôles d'utilisateur et partages de contenus. Essentiellement, elle regroupe les domaines existants subdivisant les groupes de travail dans le réseau informatique. Les contenus et les informations spécifiques au domaine ne sont disponibles à leur tour que par le biais des **contrôleurs de domaine** internes du domaine concerné. Ces derniers contiennent un catalogue global contenant toutes les informations importantes et des informations partielles sur le schéma, la configuration et les autres domaines du même réseau. Le catalogue global peut être utilisé pour rechercher et consulter des informations partielles importantes sur tous les domaines.

1.1.3.3 Domaine

Les domaines représentent la base de la structure hiérarchique des objets, des groupes de travail et des utilisateurs gérés par les administrateurs. Un domaine contient toutes les informations sur les objets et les attributs qui concernent uniquement le domaine. Les informations spécifiques au domaine ne peuvent être consultées à partir d'autres domaines que si elles sont contenues dans le catalogue global. Toutes les autres informations sont disponibles uniquement sur le contrôleur de domaine interne. Un domaine sert donc d'élément structurant important, qui délimite les unités de gestion et de réseau sous la forme de divisions réelles, de groupes de travail et de services, et organise les autorisations de manière hiérarchique. Les noms de domaine sont attribués comme des serveurs DNS classiques.

1.1.3.4 Base de données

Comme un serveur Microsoft Exchange, la base de données d'Active Directory est basée sur le moteur Microsoft Jet. Elle est basée sur des objets et est structurée de manière hiérarchique. Les objets représentent les enregistrements respectifs et les stratégies de groupe pour les ressources informatiques. Leurs propriétés sont appelées attributs et leurs types sont définis en conséquence. Les objets sont divisés en catégories **"Comptes"** (par ex. : comptes de service et d'utilisateur pour les employés, les groupes ou les périphériques) et **"Ressources"** (par ex. : partage d'applications et de services).

1.1.4 Quatre composants techniques de Active Directory

Afin d'assurer une communication unifiée entre les ordinateurs, les applications, les services, les répertoires AD et les domaines, quatre standards fondammentaux entrent en jeu. Il s'agit de :

- **LDAP :** c'est le protocole utilisé pour les requêtes unifiées soumises aux répertoires Active Directory ;
- **Kerberos :** c'est le protocole utilisé pour l'authentification centralisée et unifiée et les droits d'accès des utilisateurs sur les serveurs AD ;
- **DNS :** c'est le système utilisé pour l'adressage uniformisé des noms d'ordinateurs et des domaines dans Active Directory ;

- **SMB :** ce protocole est utilisé pour les droits d'accès tels que les stratégies de groupe ou les scripts de connexion aux fichiers dans le réseau AD et les serveurs.

1.1.5 Autres terminologies dans Active Directory

1.1.5.1 Forêt Active Directory

Une forêt Active Directory est une base de données qui peut être partionnée en plusieurs domaines Active Directory.

1.1.5.2 Domaine Active Directory

Un domaine AD est une partition d'une forêt AD. Un domaine AD est encore appelé dommaine de sécurité car il est possible d'y stocker des mots de passe ou des certificats. Par ailleurs, un domaine contient des **unités organisationelles** encore appelées **conteneurs** qui peuvent par exemple représenter les différents services (comptabilité, marketing, logistique, etc.) d'une organisation.

1.1.5.3 Objet Active Directory

Les objets se retrouvent à l'intérieur des conteneurs et permettent de représenter les utilisateurs, les ordinateurs et toute autre ressource de l'organisation ou de l'entreprise.

1.1.5.4 Contrôleur de domaine

Le contrôleur de domaine est le serveur qui héberge les services Active Directory aussi appelés **Active Directory Domain Services (AD DS)**

1.1.5.5 Active Directory Domain Services

Il s'agit des services de Active Directory. AD DS permet de gérer le stockage des données d'un annuaire, de gérer l'authentification et de gérer aussi la réplication (dans le cas où il y a plusieurs contrôleurs de domaine)

1.2 Historique des services d'annuaire jusqu'à Active Directory

Il nous importe de rappeler ici l'historique des services d'annuaire. En effet, les annuaires ont fait leur apparition avec l'informatique en réseau à partir du moment où il était nécessaire d'identifier les utilisateurs pour leur donner accès ou non à des ressources spécifiques. Au rang des premiers annuaires, on peut citer la messagerie PROFS de IBM sous MVS et NIS sous UNIX

L'arrivée de la norme X500 en 1988 a donné une évolution aux services d'annuaire. En effet, la norme X500 a pour objectif de normaliser les annuaires électroniques quel que soit leur domaine d'application. Une nouvelle version de cette norme a été mise au point en 1993.

L'objectif étant de mettre à disposition des acteurs des télécommunications un standard indépendant de tout constructeur pouvant alors faire communiquer et cohabiter de manière globale les annuaires et ainsi constituer un annuaire de type Pages Blanches ou Pages Jaunes unique.

TABLE 1.1 : Norme X500 [20]

Numéro UIT-T	Numéro ISO/CEI	Titre du standard
X.500	ISO/CEI 9594-1	Vue d'ensemble des concepts, modèles et services
X.501	ISO/CEI 9594-2	Modèles
X.509	ISO/CEI 9594-8	Framework d'authentification
X.512	ISO/CEI 9594-3	Définition de service
X.518	ISO/CEI 9594-4	Procédures pour les opérations distribuées
X.519	ISO/CEI 9594-5	Spécifications de protocoles
X.520	ISO/CEI 9594-6	Types d'attributs sélectionnés
X.521	ISO/CEI 9594-7	Classes d'objets selectionnés
X.525	ISO/CEI 9594-9	Replication d'annuaire
X.530	ISO/CEI 9594-10	Administration d'annuaire

Grâce à cette norme, les annuaires doivent pouvoir s'interconnecter, peuvent être extensible, réplicable sur plusieurs serveurs.

La norme X500 a montré ses defaillances et cela a conduit à la création de LDAP. Ainsi, plusieurs constructeurs se sont servis de ces différentes normes (X500, LDAP) pour mettre en place des annuaires propriétaires. C'est ainsi que dans les années 90 **Active Directory vit le jour sous le nom de « NT Directory Services » puis celui-ci a évolué dans le temps pour être ce qu'il est à nos jours.**

1.3 Problèmes de sécurité liés à Active Directory

Pour commencer par parler des problèmes de sécurité liés à Active Directory, rappelons d'abord que selon le rapport Global Threat Report de CrowdStrike publié en 2022, 80% des cyberattaques actuelles s'appuient sur l'identité. Et cela sera confirmé davantage avec un autre rapport, celui du groupe Gartner qui précise que les attaquants les plus sophistiqués s'attaquent désormais aux infrastructures de gestion des identités et des accès. [23]

Active Directory étant aussi une infrastructure de gestion d'identité et d'accès ne fait pas exception aux rapports ci-dessus et fait donc objet des attaques. En Mai 2021, Colonial Pipeline, un système oléoduc américain, a subi une attaque de type ransomware. Cette attaque avait entraîné l'arrêt des opérations de cette entreprise et une déclaration d'un état d'urgence par le gouvernement [7]. Le service d'authentification de base, Active Directory, aurait été le point d'entrée pour les attaquants pour perpétrer cette attaque contre Colonial Pipeline. [8]

Voici donc quelques raisons qui rendent Active Directory vulnérable et une cible pour les attaquants :

- **les erreurs de configuration et de gestion**
  Les erreurs de configuration ou de gestion restent la plus grande raison de vulnérabilité de Active Directory. S'agissant de ces erreurs, nous pouvons entre autres citer : utilisation des comptes avec des privilèges d'administrateurs pour un usage quotidien, ajout d'utilisateurs au groupe d'administrateurs au lieu de déléguer l'accès, un plan de sauvegarde et de récupération insuffisant, gestion de Active Directory depuis les contrôleurs de domaine, manque de résiliation des comptes périmés, mauvaise politique de gestion des mots de passe, manque d'audit regulier de Active Directory, manque d'application des correctifs (ou mises à jour de sécurité), ... [9]

- **les vulnérabilités**
  Active Directory fait objet de plusieurs vulnérabilités et attaques. En effet, dans la même semaine que la vulnérabilité log4j a été connue du public, il y avait une autre vulnérabilité qui touchait Active Directory mais qui était peu connue. Il s'agit de la vulnérabilité sAMAccountName qui est une vulnérabilité de contournement de sécurité qui permet à des attaquants potentiels de se faire passer pour un contrôleur de domaine en utilisant l'usurpation d'identité du compte d'ordinateur sAMAccountName. Fort heureusement que Microsoft a proposé un correctif, le CVE-2021-42278. En plus, le 10 mai 2022, une autre vulnérabilité a été découverte et permet l'élevation de privilèges dans Active Directory : CVE-2022-26923 [11]. Aussi, faut-il ajouter que d'autres vulnérabilités affectent Active Directory vu que ce denier utilise des protocoles qui sont parfois vulnérables comme : Kerberos, NTLM, LanManager.

Conclusion

Les services d'annuaire existaient il y a longtempts et ceux-ci ont évolué au fil du temps. Ce premier chapitre nous a permis de faire l'état de l'art des services d'annuaire avec un accent particulier sur le service d'annuaire d'entreprise de Microsoft, Active Directory. Nous avons exploré les notions de ce service d'annuaire et abordé les questions de sécurité qui touchent ce service.

Chapitre 2

Analyse, Choix, Justification

Introduction

Active Directory est un outil bien connu des administrateurs réseaux et systèmes. Active Directory se déploie de plusieurs manières et a même des alternatives pour répondre aux besoins de l'environnement informatique d'une entreprise. Dans ce chapitre, nous allons faire une analyse par une étude comparative des différentes méthodes de déploiement de Active Directory et mettre en lumière ses alternatives pour ensuite présenter l'architecture de l'entreprise LAG Solutions et les raisons qui expliquent ce choix du déploiement de Active Directory.

2.1 Différentes méthodes de déploiement de Active Directory

De nos jours, avec l'évolution constante des technologies dans le domaine informatique, les entreprises disposent de plusieurs possibilités de déploiement de leur solution Active Directory selon leurs besoins, choix et budgets.

2.1.1 Active Directory en Local

Microsoft Active Directory (le plus souvent appelé contrôleur de domaine) est le système d'annuaire de facto utilisé aujourd'hui dans la plupart des organisations. Active Directory est excellent pour gérer les fonctions d'authentification et d'autorisation des utilisateurs et des ordinateurs au sein d'une organisation. Active Directory uniquement sur site ou en local, ce qui signifie que toute l'infrastructure d'authentification fonctionne sur du matériel interne.
L'insuffisance de ce premier mode de déploiement de Active Directory est le fait qu'il dépende d'ordinateurs membres reliés en permanence à un domaine et de protocoles tels que LDAP pour l'interrogation de l'annuaire et Kerberos pour l'authentification à l'annuaire ; ce qui n'est plus adapté à l'environnement de travail moderne, centré sur Internet et mobile, qui devient la norme aujourd'hui.

2.1.2 Azure Active Directory

Azure Active Directory (AAD) est une version des services d'annuaire "dans le nuage" hébergée sur Microsoft Azure. AAD a des capacités et des fonctionnalités assez différentes de celles de Win-

dows Server Active Directory (AD). Sa fonction principale est actuellement de gérer les utilisateurs et la myriade d'appareils (ordinateurs Windows, Apple et Linux, tablettes et smartphones, etc.) que les utilisateurs emploient dans leur vie professionnelle et sociale, en particulier pour les utilisateurs distants. L'AAD estompe la distinction entre les utilisateurs "sur site" et "distants". L'AAD est le mécanisme d'authentification et d'autorisation non seulement pour Azure, Office 365 et Intune, mais aussi pour de nombreux autres systèmes d'authentification tiers.
Néanmoins, Azure Active Directory est un service en ligne (ou "en nuage") uniquement et ne supporte pas l'intégration de certaines applications ou logiciels notamment ceux anciens.

2.1.3 Hybrid Active Directory

Hybrid Azure AD est utilisé lorsque vous avez votre Active Directory local (contrôleur de domaine) sur site et que vous souhaitez synchroniser vos données avec Azure Active Directory. Au lieu d'avoir deux jeux d'informations d'identification à deux endroits différents, vous pouvez les ajouter dans le contrôleur de domaine "sur site", et ils seront répliqués vers Azure AD à l'aide d'un logiciel complémentaire de Microsoft appelé Azure AD Connect.

2.2 Alternatives de Active Directory

Microsoft Active Directory n'étant disponible que sur Windows, nous avons recherché quelques alternatives de Active Directory disponibles pour d'autres plateformes telles que Linux et Mac. En effet, nous avons trouvé trois alternatives de Microsoft Active Directory sous Linux et Mac :

2.2.1 Lightweight Directory Access Protocol (LDAP)

Celui-ci est un protocole qui permet aux applications d'intégrer des données d'annuaire à partir d'une base de donées centralisée. LDAP se compose essentiellement d'un répertoire qui est comme une base de données, mais qui contient des informations basées sur des attributs. Chaque entrée du répertoire possède un ensemble d'attributs. Chaque attribut a un nom et des valeurs. Ces attributs sont définis dans un schéma. Chaque entrée de la directive est reconnue par l'utilisation d'un identifiant unique connu sous le nom de **Distinguished Name (DN)**. Chaque entrée possède également son **Nom Distingué Relatif (RDN)**. Le DN peut être considéré comme un chemin d'accès complet au fichier, tandis que le RDN est le nom de fichier relatif dans le dossier parent. Par exemple : DN=/ifri/licence/newfile.txt, RDN=newfile.txt.
Il faut noter qu'un DN peut changer au cours de la durée de vie de l'entrée si les entrées sont déplacées dans l'arbre.

Mécanisme d'authentification avec LDAP : Pour authentifier un utilisateur avec un LDAP, il est important d'obtenir le DN de l'utilisateur ainsi que son mot de passe. Dans un formulaire de connexion, les utilisateurs saisissent généralement leur nom d'utilisateur ou leur adresse électronique. Un client LDAP envoie une requête au serveur LDAP et utilise la résolution de DN pour prendre le nom ou l'adresse électronique de l'utilisateur, effectuer une recherche dans les entrées utilisateur et trouver le DN correspondant. Si le nom d'utilisateur correspond au DN, le serveur LDAP authentifie l'utilisateur et lui donne accès au système. Si le nom d'utilisateur ne correspond pas, l'authentification échoue.

2.2.2 Radius

Radius est un protocole utilisé pour authentifier les utilisateurs sur un réseau local. Grâce à l'utilisation du serveur Radius, les utilisateurs peuvent se connecter à un réseau en utilisant un nom d'utilisateur et un mot de passe individuels. RADIUS peut également séparer le trafic des utilisateurs ou segmenter les utilisateurs vers un sous-réseau particulier.
Radius permet aux organisations de conserver les profils des utilisateurs dans une base de données centrale (serveur Radius) que les serveurs distants peuvent partager.
Radius utilise deux paquets pour gérer l'authentification, l'autorisation et l'accounting (ou l'audit). Il s'agit de **access-request** pour l'autentification et l'autorisation, puis **accounting-request** pour l'accounting

Mécanisme de fonctionnement de Radius : Pour s'authentifier auprès d'une ressource du réseau, un utilisateur ou une machine utilisateur envoie une demande au serveur d'accès au réseau (NAS) en utilisant des informations d'accès. Le NAS envoie un message de demande d'accès à l'aide d'un protocole Radius, à un serveur RADIUS. La demande comprend généralement des informations d'accès sous la forme d'un nom d'utilisateur ou d'un mot de passe. Le serveur Radius valide le message à l'aide de schémas d'authentification. Après vérification, le serveur Radius renvoie la réponse au NAS. La réponse peut être :

- **Access-Reject :** L'utilisateur se voit refuser inconditionnellement l'accès à toutes les ressources demandées ;
- **Access-Challenge :** L'utilisateur doit fournir des informations supplémentaires telles qu'un mot de passe secondaire, un jeton, une carte ou un code PIN ;
- **Access-Accept :** L'accès est accordé à l'utilisateur.

2.2.3 FreeIPA

FreeIPA est une solution intégrée de gestion des informations de sécurité combinant Linux (Fedora), 389 Directory Server, MIT Kerberos, NTP, DNS, Dogtag (système de certificats). Il se compose d'une interface web et d'outils d'administration en ligne de commande. C'est également une solution intégrée d'identité et d'authentification pour les environnements en réseau Linux/UNIX. Un serveur FreeIPA fournit des informations centralisées sur l'authentification, l'autorisation et les comptes en stockant des données sur les utilisateurs, les groupes, les hôtes et d'autres objets nécessaires pour gérer les aspects de sécurité d'un réseau d'ordinateurs.
FreeIPA est construit sur la base de composants Open Source bien connus et de protocoles standard, avec un accent particulier sur la facilité de gestion et l'automatisation des tâches d'installation et de configuration.
Plusieurs serveurs FreeIPA peuvent facilement être configurés dans un domaine FreeIPA afin d'assurer la redondance et l'évolutivité. Le serveur d'annuaire 389 est le magasin de données principal et fournit une infrastructure d'annuaire LDAPv3 multi-maître complète. L'authentification par signature unique est assurée par le KDC Kerberos du MIT. Les capacités d'authentification sont renforcées par une autorité de certification intégrée basée sur le projet Dogtag. En option, les noms de domaine peuvent être gérés à l'aide du serveur ISC Bind intégré.
Les aspects de sécurité liés au contrôle d'accès, à la délégation des tâches d'administration et à

d'autres tâches d'administration du réseau peuvent être entièrement centralisés et gérés via l'interface Web ou l'outil de ligne de commande ipa. [18]

2.3 Architecture du système d'information de l'entreprise LAG Solutions

Le système d'information de LAG Solutions est composée d'une armoire informatique dans laquelle nous retrouvons :

- 1 commutateur Ubiquiti ;
- 2 points d'accès Ubiquiti et un controleur Ubiquiti Unifi ;
- Un serveur qui joue le role d'hyperviseur avec Hyper V sous Windows serveur 2016 ;
- 2 controleurs de domaine sous Windows Serveur 2016 (Des machines virtuelles) ;
- 1 serveur virtuel de fichier ;
- 1 serveur virtuel d'application et sa base de données ;
- 1 serveur virtuel Wsus (pour la gestion des mises à jour) ;
- 1 serveur virtuel de téléphone sous Astérsik ;
- et un firewall Pfsense qui assure la sécurité de la connexion internet de la structure ;
- Une dizaine de PC fixes et portables partageant cette connexion internet

Ce choix d'architecture on premise (en local) de l'entreprise LAG Solutions s'explique par différentes raisons comme :
- la stratégie budgétaire ;
- la politique de sécurité de l'entreprise incluant les plans de continuité d'activité et de reprise d'activité.

Conclusion

Active Directory qui est un service d'annuaire d'entreprises de Microsoft peut se deployer de différentes manières et prendre en compte les besoins et les contraintes des entreprises. Il existe également d'autres alternatives et des concurrents pour rendre possible ce service sur d'autres plateformes.

Chapitre 3

Test de pénétration, résultats et recommandations

Introduction

Dans ce dernier chapitre, nous allons dans un premier temps relever quelques vulnérabilités relatives à Active Directory, ensuite nous allons faire le test de pénétration de l'infrastructure Active Directory de l'entreprise LAG Solutions, présenter les résultats découlant de ce test puis formuler des recommandations à l'endroit de l'administrateur système afin d'assurer la sécurité de leur infrastructure Active Directory de l'entreprise LAG Solutions.

3.1 Vulnérabilités relatives à Active Directory

Plusieurs vulnérabilités sont connues et publiées sur le site CVE MITRE affectant Active Directory. A la date de la rédaction de ce document, nous avons 235 CVE publiées sur le site en rapport avec Active Directory.

Dans cette liste de 235 vulnérabilités publiées, nous avons relevé quelques-unes les plus récentes : [21]

- **CVE-2023-35351** : une vulnérabilité permettant l'exécution de code à distance en se basant sur le service de certificat de Active Directory. Le mode opératoire consiste pour un attaquant disposant des droits d'accès en lecture à l'autorité de certification (CA) à envoyer une requête spécialement conçue à un serveur de certificats vulnérable. Les systèmes affectés sont Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022. [22]
- **CVE-2023-33254** : une vulnérabilité qui se traduit par l'exposition aux informations d'identification LDAP bind par les appliances KACE Systems Deployment et Remote Site 9.0.146. Les informations d'identification capturées peuvent fournir un niveau de privilège plus élevé sur le

domaine Active Directory. Pour exploiter cette vulnérabilité, un attaquant authentifié modifie les paramètres d'authentification de l'utilisateur pour spécifier un serveur LDAP contrôlé par l'attaquant, clique sur le bouton **Tester les paramètres** et capture les informations d'identification en texte clair.

- **CVE-2023-23749** : une vulnérabilité qui consiste en une injection LDAP et qui affecte l'extension 'LDAP Integration with Active Directory and OpenLDAP - NTLM & Kerberos Login' grâce au paramètre POST 'username' qui n'est pas correctement analysé. Un attaquant peut donc manipuler ce paramètre pour extraire un contenu arbitraire de la base de données LDAP.

3.2 Test de pénétration

3.2.1 Test de pénétration et ses différentes phases

Avant de présenter les outils que nous avons utilisés dans le cadre de ce test de pénétration de l'infrastructure Active Directory, il nous paraît important de rappeler d'abord quelques notions sur un test de pénétration notamment ses différentes phases.

En effet, un **test de pénétration**, ou un **test d'intrusion** ou encore **test de sécurité** est un test qui simule des attaques sur un système d'information en se mettant sous la peau d'un attaquant. L'objectif de ce type de test est de mesurer (ou évaluer) le niveau de sécurité du système d'information et de prendre des mesures nécessaires afin de ne laisser aucune chance à un potentiel attaquant.

Le test de pénétration se déroule sur plusieurs phases notamment : [15]

- **La planification et la reconnaissance :** Au niveau de cette étape, la portée et les objectifs du test et les méthodes de test à utiliser sont clairement définis. Ensuite il faut effectuer une collecte d'informations pour mieux connaître la cible, son fonctionnement et ses vulnérabilités potentielles.
- **Le scanning :** Au cours de cette étape, une interprétation des données collectées à l'étape précédente est faite. C'est à ce niveau que l'on analyse les services, les ports, les domaines, etc. de la cible. On peut aussi acquérir des informations à l'aide des outils d'analyse actifs.
- **L'aquisition d'accès :** A cette étape, des attaques applicatives, systèmes, réseau, etc. peuvent être utilisées afin d'exploiter les vulnérabilités relevées au niveau de la cible.
- **Le maintien d'accès :** Ici, on voit si la vulnérabilité peut être utilisée pour obtenir une présence persistante, c'est-à-dire maintenir l'accès, dans le sytème exploité.
- **Le rapport :** Les résultats du test de pénétration sont compilés et présentés en un rapport qui contient des détails sur les vulnérabilités exploitées, les données sensibles accédées, etc.

Il faut mentionner qu'il existe plusieurs types de test de pénétration à savoir : **le test d'intrusion de la boîte ouverte, le test d'intrusion de la boîte fermée, le test d'intrusion secret, le test d'intrusion externe et le test d'intrusion interne** en fonction de ce que l'on connait de la cible. [16]
Dans le cadre de notre travail, il s'agit d'un test de pénétration interne.

3.2.2 Outils utilisés

Alors, s'agissant des outils dont nous avons fait usage dans le cadre de ce travail, il y a entre autres :

3.2.2.1 Impacket

Impacket est un outil qui a été créé à l'origine par SecureAuth, et est maintenant maintenu par Fortra's Core Security.

Impacket est une collection de classes Python pour travailler avec des protocoles de réseau. Il se concentre sur la fourniture d'un accès programmatique de bas niveau aux paquets et, pour certains protocoles (par exemple SMB1-3 et MSRPC), à l'implémentation du protocole lui-même. Les paquets peuvent être construits à partir de zéro, ainsi qu'analysés à partir de données brutes, et l'API orientée objet permet de travailler facilement avec des hiérarchies profondes de protocoles. La bibliothèque fournit un ensemble d'outils comme exemples de ce qui peut être fait dans le contexte de cette bibliothèque.

3.2.2.2 Nmap

Nmap pour Network Mapper est un outil de découverte de réseaux qui permet de collecter des informations sur ces derniers, sur les ports ouverts, les services qui utilisent ces ports et bien d'autres informations qui peuvent être utiles lors de la phase de collecte d'information d'un test de pénétration.



FIGURE 3.1 : Logo de l'outil Nmap

3.2.2.3 BloodHound

BloodHound est une application web Javascript d'une seule page, construite sur Linkurious, compilée avec Electron, avec une base de données Neo4j alimentée par un collecteur de données C#. BloodHound utilise la théorie des graphes pour révéler les relations cachées et souvent involontaires au sein d'un Active Directory ou d'un environnement Azure. Les attaquants peuvent utiliser BloodHound pour identifier facilement des chemins d'attaque très complexes qui seraient autrement impossibles à identifier rapidement. Les défenseurs peuvent utiliser BloodHound pour identifier et éliminer ces mêmes chemins d'attaque. Les équipes bleues et rouges peuvent utiliser BloodHound pour mieux comprendre les relations de privilèges dans un environnement Active Directory ou Azure. BloodHound est maintenu par l'équipe BloodHound Enterprise. [17]



FIGURE 3.2 : Logo de l'outil Bloodhound

3.2.2.4 CrackMapExec (CME)

CrackMapExec (CME) est un outil de post-exploitation qui permet d'automatiser l'évaluation de la sécurité des grands réseaux Active Directory. Construit dans un esprit de discrétion, CME suit le concept de "Living off the Land" : abuser des fonctionnalités/protocoles intégrés d'Active Directory pour atteindre sa fonctionnalité et lui permettre d'échapper à la plupart des solutions de protection des points d'extrémité IDS/IPS.
CME fait un usage intensif de la bibliothèque Impacket (développée par @asolino) et de la boîte à outils PowerSploit (développée par @mattifestation) pour travailler avec les protocoles réseau et réaliser une variété de techniques de post-exploitation.
Bien que conçu pour être utilisé principalement à des fins offensives (par exemple par les équipes rouges), CME peut également être utilisé par les équipes bleues pour évaluer les privilèges des comptes, trouver d'éventuelles erreurs de configuration et simuler des scénarios d'attaque. [19]



FIGURE 3.3 : Logo de l'outil CrackMapExec

3.2.3 Déroulement et résultats du test de pénétration

Pour commencer, nous avons lancé un scan avec l'outil NMAP sur le réseau **192.168.1.0/24** où se trouve probablement notre contrôleur de domaine, le serveur AD suivant la commande ci-après :

```
1  # nmap -sC -sV -p- 192.168.1.0/24
```

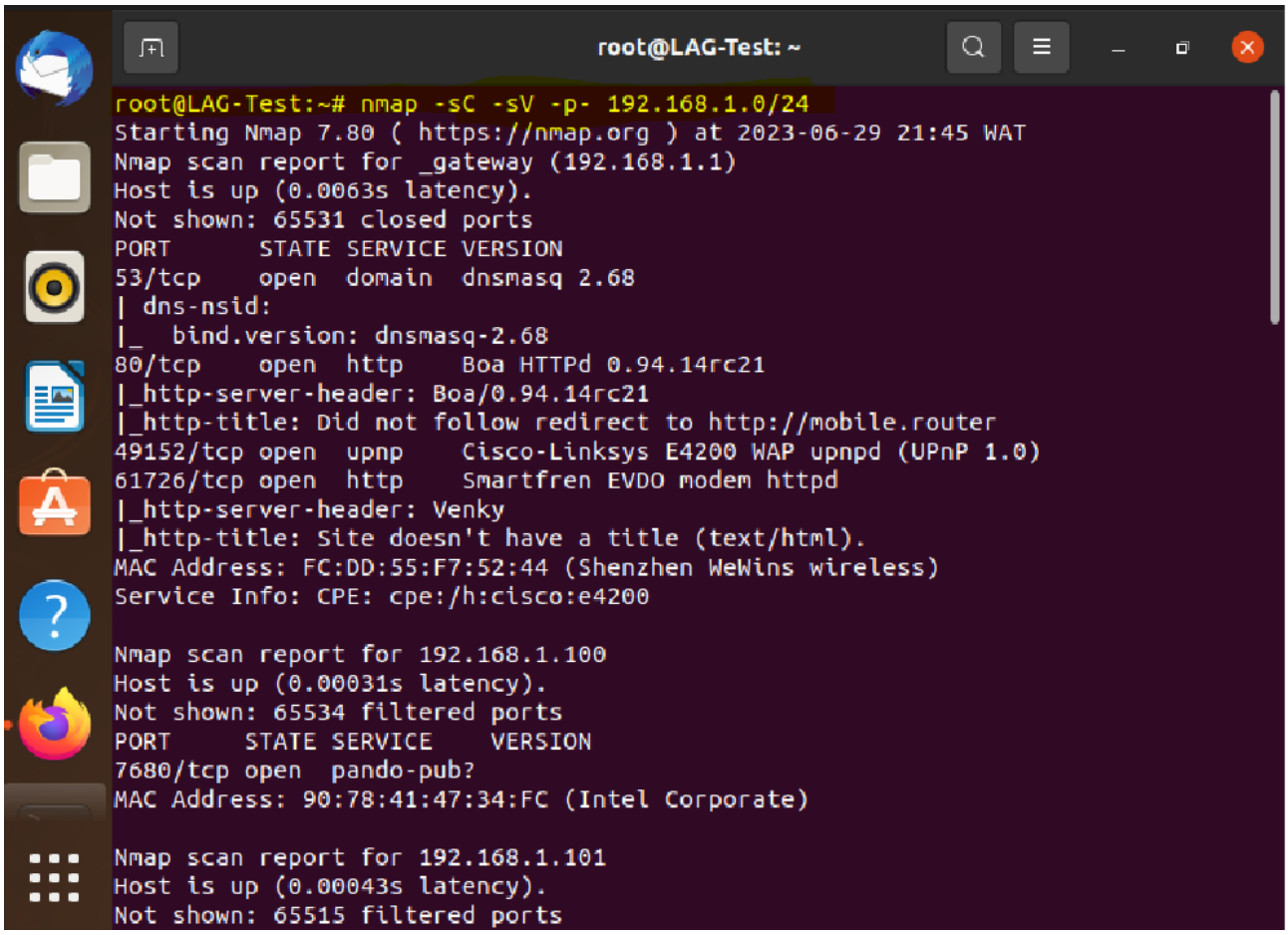


FIGURE 3.4 : Résultats de scan du réseau avec Nmap

Les résultats de ce scan du réseau nous ont permis de connaître l'adresse IP **(192.168.1.101)** et le nom du domaine de l'entreprise LAG Solutions **(lagsolutions.local)** et d'avoir les détails suivants sur les services tournant sur le controleur de domaine :

- le port 53 pour le DNS est ouvert ;
- le port 88 pour le Kerberos est ouvert ;
- les ports 389 et 3268 pour LDAP sont ouverts ;

La figure ci-après montre la capture d'écran des résultats obtenus sur ces détails :

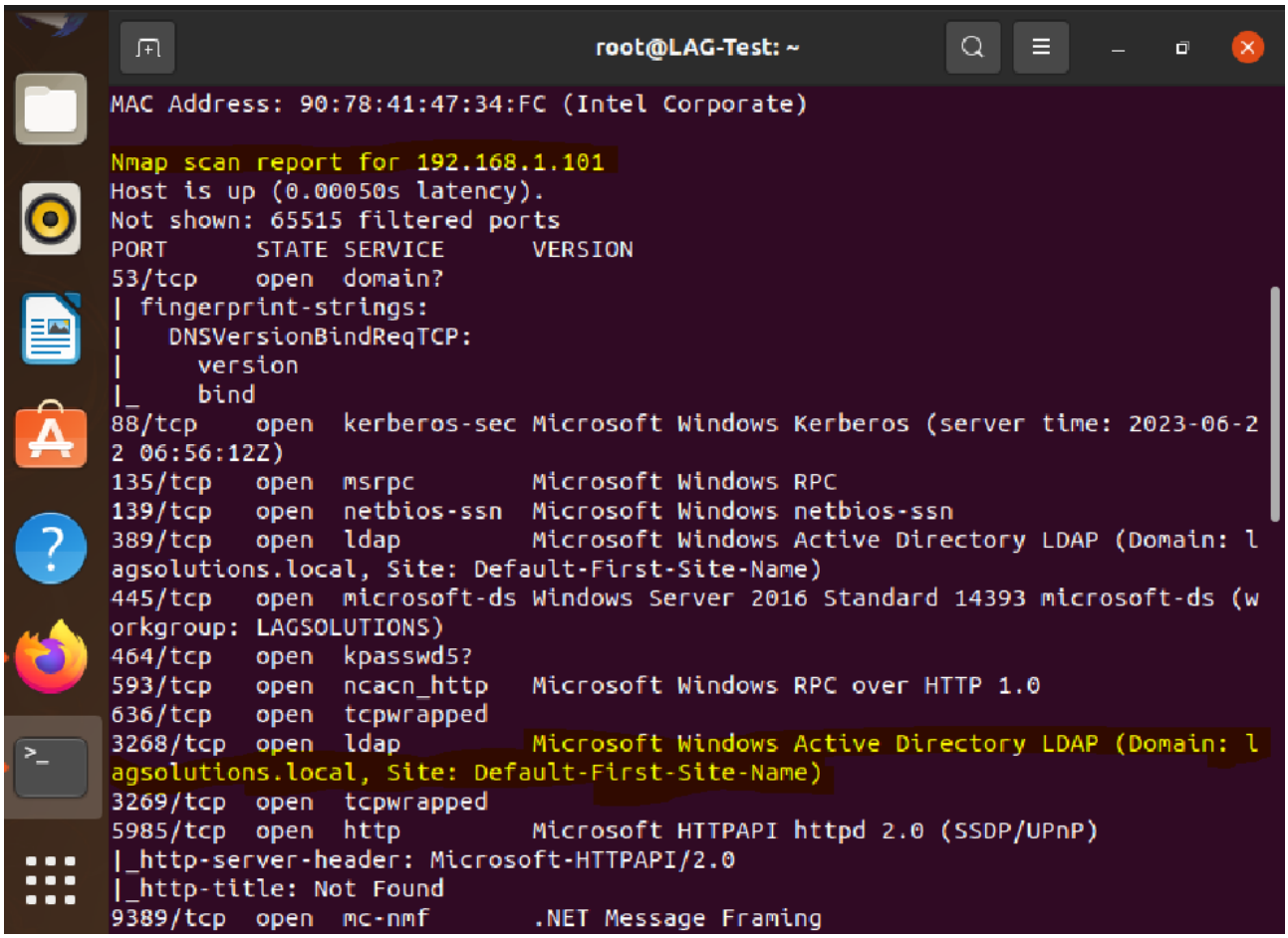


FIGURE 3.5 : Collecte des informations sur le contrôleur de domaine

Nous constatons que le système d'exploitation du contrôleur de domaine est **Windows Server 2016**. Nous avons donc fait de recherche sur les vulnérabilités qui affectent Windows Server 2016 et nous avons une liste de quelques vulnérabilités qui se présente comme suit :

- **CVE-2020-1472** : une vulnérabilité de type élévation de privilèges qui se traduit par l'établissement par un attaquant d'une connexion de canal sécurisé Netlogon vulnérable avec un contrôleur de domaine, en utilisant le protocole à distance Netlogon (MS-NRPC). Pour exploiter la vulnérabilité, un attaquant non authentifié devrait utiliser MS-NRPC pour se connecter à un contrôleur de domaine afin d'obtenir l'accès à l'administrateur de domaine.
- **CVE-2023-35310** : une vulnérabilité qui affecte Windows Server 2016 notamment le service DNS et qui a comme impact l'exécution de code à distance.
- **CVE-2023-32044** : une vulnérabilité de déni de service de Microsoft Message Queuing (MSMQ).

Nous nous sommes intéressés à la vulnérabilité CVE-2020-1472 qui a beaucoup plus rapport avec un contrôleur de domaine. Il faut noter que cette vulnérabilité n'affecte pas que Windows Server 2016 mais aussi d'autres Windows Server dont Windows Server 2019 qui est plus récent comparativement à Windows Server 2016.

Pour dérouler l'attaque avec la CVE-2020-1472, il nous faut connaître le NetBIOS name du contrôleur de domaine. Pour ce faire, connaissant déjà l'adresse IP du contôleur de domaine à travers les résultats du précédent scan du réseau, nous avons utilisé l'outil **ntbscan** pour lancer la commande ci-après :

```
# ntbscan 192.168.1.101
```

La figure ci-dessous montre le résultat de cette commande :

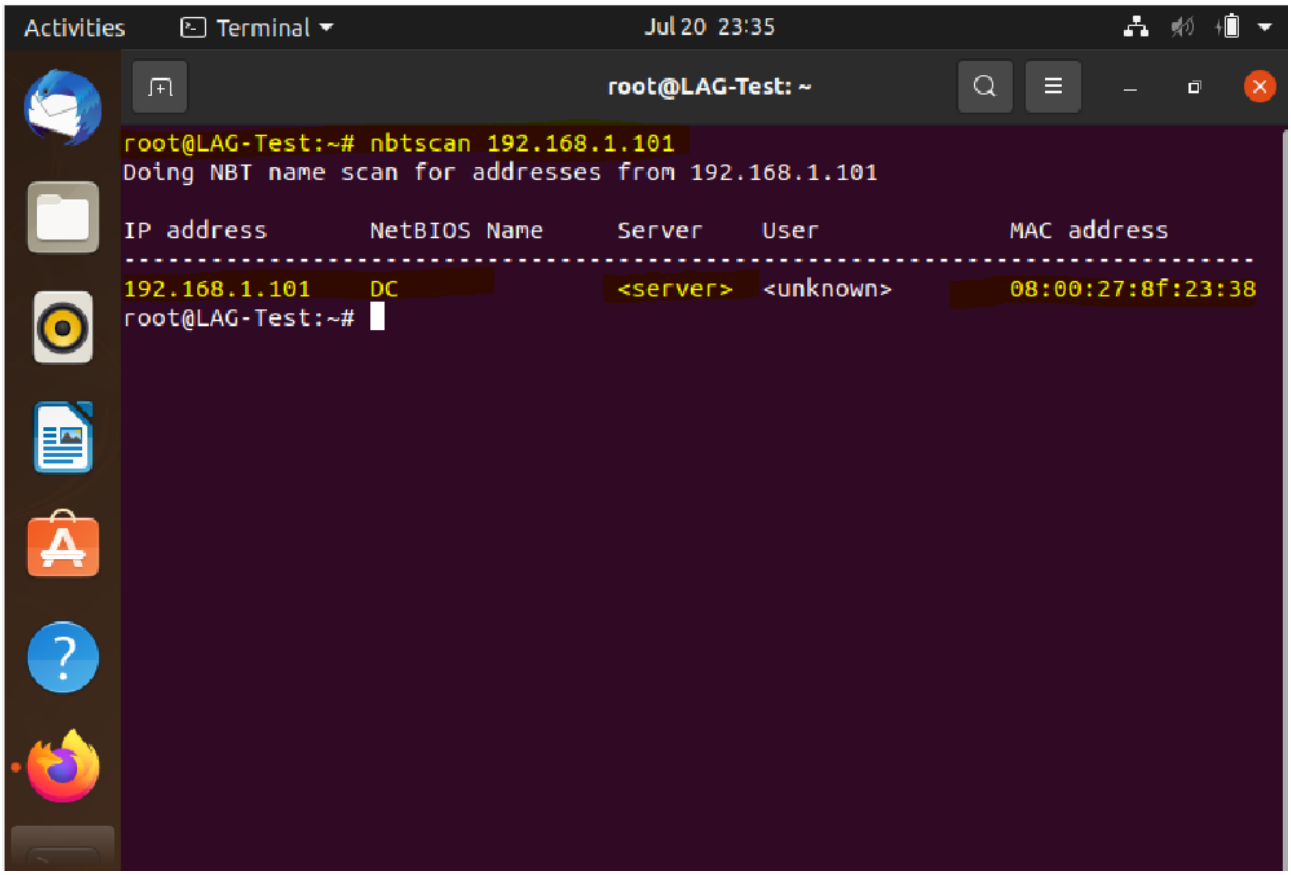


FIGURE 3.6 : NetBIOS name du contôleur de domaine

Nous retenons donc que le NetBIOS name est : **DC**

Ensuite, connaissant maintenant le NetBIOS name du contrôleur de domaine, nous avons lancé le script de l'exploit de la CVE-2020-1472 en utilisant la commande ci-après :

```
# python3 cve-2020-1472-exploit.py -n DC -t 192.168.1.101
```

Le résultat de cette commande est présenté à travers la capture d'écran ci-dessous :

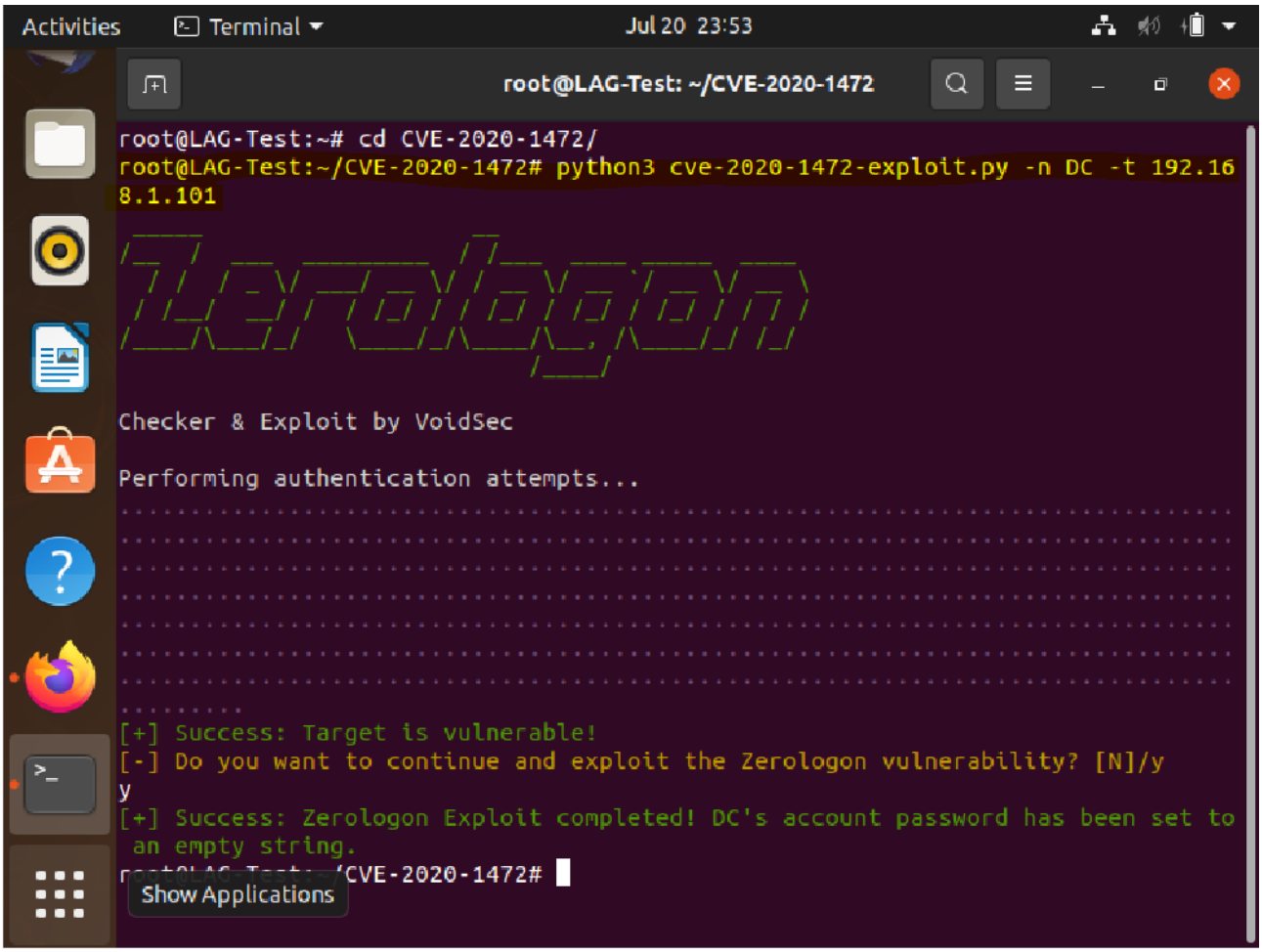


FIGURE 3.7 : Exploitation de la vulnérabilité zerologon

Avec cette vulnérabilité, nous sommes arrivé à définir le mot de passe du contrôleur de domaine à une chaine de carractère vide, ce qui nous permettra de faire le dump des mots de passe de tous les comptes sur le domaine.

Pour faire le dump des mots de passe de tous les comptes sur le contrôleur de domaine et récuperer les hashes de ces mots de passe, nous avons utilisé le module **secretsdump.py** de l'outil **Impacket** avec la commande suivante :

```
# python3 secretsdump.py -no-pass -just-dc LAGSOLUTIONS/DC\$@192.168.1.101
```

Le résultat de cette commande se présente comme suit :

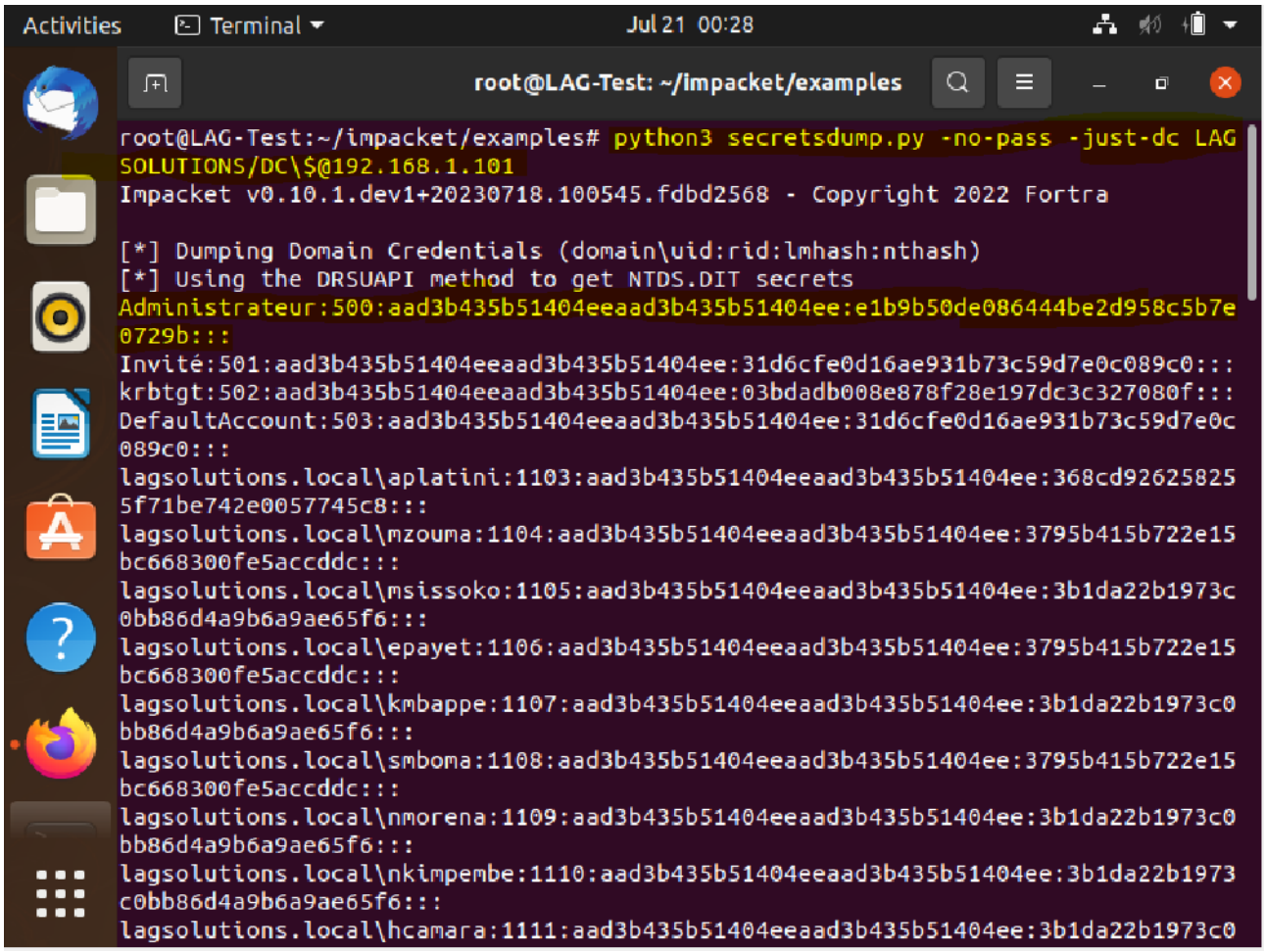


FIGURE 3.8 : Hashes des mots de passe des comptes

Parmi les hashes recupérés, nous avons celui du mot de passe du compte administrateur du contrôleur de domaine qui est : **aad3b435b51404eeaad3b435b51404ee :e1b9b50de086444be2d958c5b7e0729b**.

Nous avons utilisé ce hash pour nous connecter et prendre le contrôle du domaine à travers le shell. Pour ce faire, nous avons utilisé le module **wmiexec.py** de l'outil **Impacket** pour lancer la commande suivante :

```
#python3 wmiexec.py -hashes <hash_admin> lagsolutions.local/Administrateur@192.168.1.101
```

Il faut noter que <hash_admin> est remplacé par le hash du mot de passe du compte administrateur précédemment recupéré : **aad3b435b51404eeaad3b435b51404ee :e1b9b50de086444be2d958c5b7e0729b**

Le résultat de cette commande est présenté à travers la capture d'écran suivante :

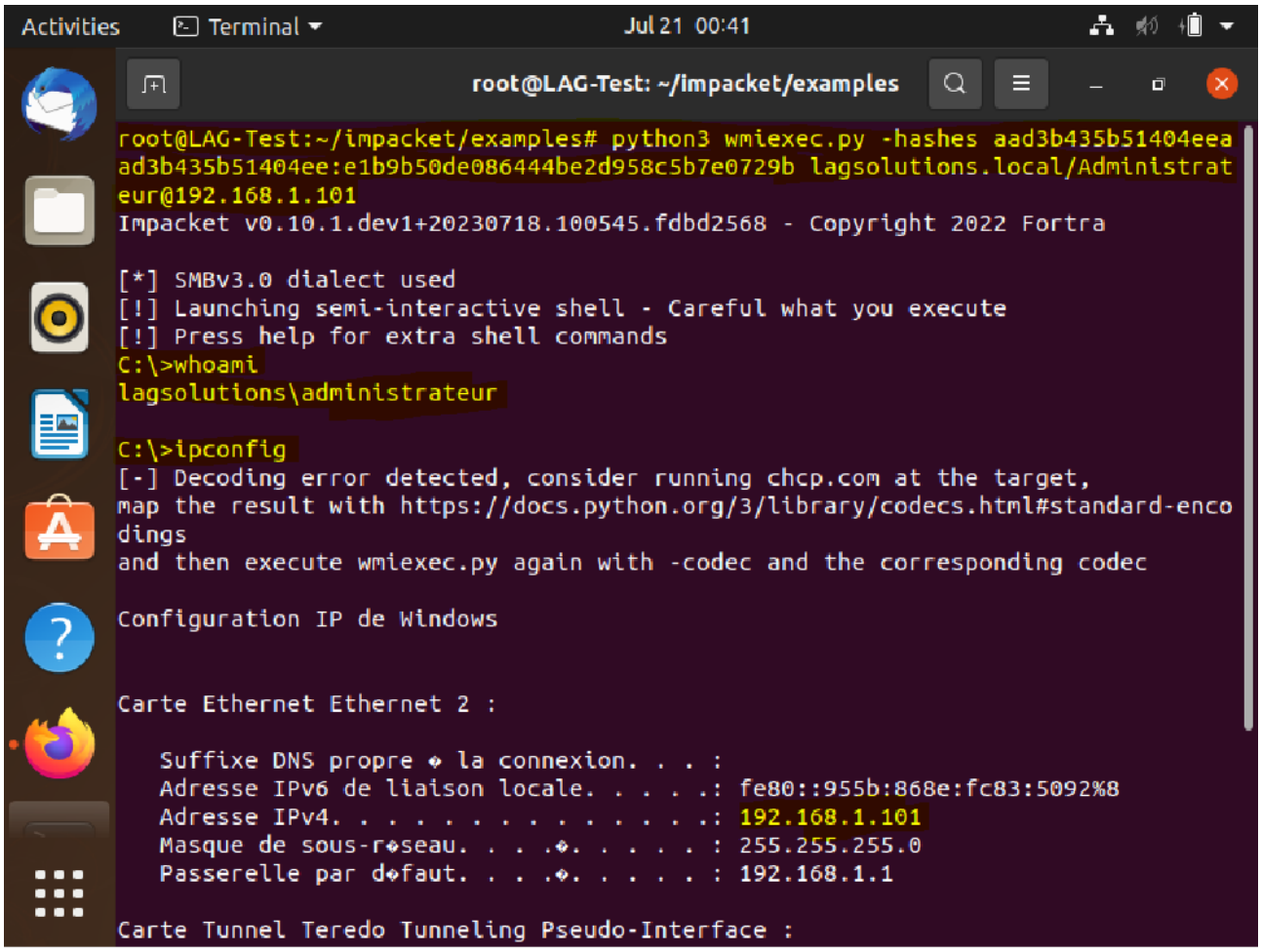


FIGURE 3.9 : Connexion au compte administrateur du contrôleur de domaine via le shell

3.3 Recommandations

Les résultats du test de pénétration effectué nous permettent de conclure que l'infrastructure Active Directory de LAG Solutions notamment le contrôleur de domaine (Windows Server 2016) est vulnérable à la CVE-2020-1472, ce qui permet d'exploiter cette vulnérabilité afin de prendre contrôle du compte administrateur du domaine. Dans une attaque réelle, l'attaquant pourrait se servir de ce compte administrateur pour installer des malwares, ou pour crypter les données importantes au niveau du contrôleur de domaine et ainsi réclamer une rançon.

Pour rémédier à une telle exposition et à ce risque, il est recommandé à l'administrateur système d'appliquer la mise à jour de sécurité de Microsoft qui corrige cette vulnérabilité. Les détails sur cette mise à jour de sécurité sont disponibles à travers ce lien : https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

En addition, puisque le contrôleur de domaine de l'entreprise est homologué et utilisé pour les tests des applications, nous recommandons ce qui suit à l'administrateur système de LAG Solutions pour la bonne gestion des comptes sur le contrôleur de domaine :

- Désactiver les comptes créés pour les tests d'applications après la finalistion de chaque projet

de tests d'applications ;

- Restreindre les privilèges des comptes et n'attribuer que ceux requis pour l'accomplissement des tâches de l'utilisateur ;
- Créer un groupe spécifique avec des privilèges restreints pour les comptes utilisés pour les tests d'applications ;

Par ailleurs, de manière globale et au vu des diverses raisons dont nous avons évoquées dans le chapitre 1 de ce document et qui rendent Active Directory vulnérable aux attaques, nous faisons également les recommandations supplémentaires qui se présentent comme suit :

- Faire regulièrement le test de pénétration de l'infrastructure Active Directory pour découvrir les failles et les corriger en appliquant efficacement les mises à jour de sécurité nécessaires ;
- Faire de la veille technologique pour être au courant des nouvelles attaques relatives aux environnements Active Directory et vérifier si son infrastructure n'est pas vulnérable à ces attaques ;
- Suivre les bonnes pratiques recommandées par Microsoft en matière de configuration et de gestion des infrastructures Active Directory notamment les politiques de groupes, les politiques de mot de passe, les droits d'accès, etc. ;
- Avoir un plan bien défini de sauvegarde de son infrastructure Active Directory ;
- Former les employés et les collaborateurs à la culture de l'hygiène numérique car l'humain est considéré comme le maillon le plus faible des systèmes d'information.

3.4 Conclusion

Comme annoncé au niveau de l'introduction de ce chapitre, il a été question du test de pénétration de l'architecture AD tout en relevant quelques vulnérabilités affectant les environnements Active Directory. Nous avons essentiellement exploité la vulnérabilité CVE-2020-1472 sur l'infrastructure Active Directory, ce qui nous a permis d'avoir acccès au compte administrateur du contrôleur de domaine. Cette vulnérabilité affecte les systèmes comme Windows Server 2012, Windows Server 2016, et même Windows Server 2019. Il urge donc à tout administrateur système utilisant ces systèmes affectés comme contrôleur de domaine d'appliquer au plus vite la mise à jour de sécurité disponible à cet effet afin d'éviter toute exposition à une attaque découlant de l'exploitation de cette vulnérabilité.

Conclusion Générale

Tout au long de ce document de mémoire, nous avons travaillé sur Active Directory en commençant au niveau de notre révue de littérature par les généralités de Active Directory, ses différentes méthodes de déploiement, les alternatives à Active Directory. Nous avons également mis en lumière quelques vulnérabilités rencontrées dans les environnements Active Directory. Nous avons traité un cas de problème de sécurité notamment l'élévation de privilège en exploitant la vulnérabilité CVE-2020-1472 sur l'environnement Active Directory qui nous a été mis à disposition par l'entreprise LAG Solutions dans le cadre de ce mémoire. A travers ce test, nous sommes parvenus à formuler des recommandations à l'entreprise en particulier et aux administrateurs systèmes en général quant à l'importance de mettre à jour les environnements Active Directory afin de corriger les failles de sécurités de leurs systèmes d'informations pour limiter leurs expositions aux attaques. Par ailleurs, en termes de perspectives, nous pensons qu'il serait intéressant d'explorer d'autres attaques dont une infrastructure Active Directory fait l'objet et même étendre le test sur d'autres environnements AD pour prendre en compte les autres méthodes de déploiement de AD : à savoir AD en ligne (le cas de Azure Active Directory) et AD en mode hybride.

Bibliographie

[1] L. B. Paterson. Mémoire de licence : Mise en place d'un système de prévention et de détection d'intrusion basé sur ossec : Cas de bénin digital. Université d'Abomey-Calavi, Institut de Formation et de Recherche en Informatique (IFRI), 2021-2022.

[2] B. M. Posey. Active directory security risk assessment and attack path management [quest ebook].

[3] P. Security. The complete active directory security handbook [picus security]. 2023.

[4] R. M. SODJI. Mémoire de licence : Evaluation de la vulnérabilité des serveurs de messagerie du .bj à l'usurpation de mail. Université d'Abomey-Calavi, Institut de Formation et de Recherche en Informatique (IFRI), 2019-2020.

[5] B. Svidergol. What is active directory ? [netwrix ebook].

Webographie

[6] https://kidan.co/fr/blog/quest-ce-quactive-directory-et-pourquoi-est-il-necessaire/. Consulté le 3 Janvier 2023.

[7] https://fr.wikipedia.org/wiki/Cyberattaque_de_Colonial_Pipeline. Consulté le 11 Janvier 2023.

[8] https://www.journaldunet.com/solutions/dsi/1511731-proteger-ses-infrastructures-critiques-contre-les-cyberattaques/. Consulté le 11 Janvier 2023.

[9] https://blog.netwrix.fr/2018/02/08/gestion-dactive-directory-top-7-des-erreurs-courantes/. Consulté le 11 Janvier 2023.

[10] https://www.semperis.com/blog/ad-vulnerability-cve-2022-26923/. Consulté le 12 Janvier 2023.

[11] https://www.semperis.com/blog/ad-vulnerability-cve-2022-26923/. Consulté le 12 Janvier 2023.

[12] https://www.ionos.fr/digitalguide/serveur/know-how/active-directory-cest-quoi/. Consulté le 18 Janvier 2023.

[13] https://activedirectorypro.com/create-active-directory-test-environment/#lesson-3. Consulté le 27 Février 2023.

[14] https://openclassrooms.com/fr/courses/7723396-assurez-la-securite-de-votre-active-directory-et-de-vos-domaines-windows. Consulté le 28 Février 2023.

[15] https://www.devensys.com/cybersecurite/pentest-test-intrusion. Consulté le 03 Mars 2023.

[16] https://www.cloudflare.com/fr-fr/learning/security/glossary/what-is-penetration-testing/. Consulté le 24 Avril 2023.

[17] https://github.com/BloodHoundAD/BloodHound. Consulté le 28 Mai 2023.

[18] https://freeipa.org/About.html. Consulté le 27 Juin 2023.

[19] https://ptestmethod.readthedocs.io/en/latest/cme.html. Consulté le 28 Juin 2023.

[20] https://fr.wikipedia.org/wiki/X.500#Liste_des_normes_X.500. Consulté le 11 Janvier 2023.

[21] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Active+Directory. Consulté le 18 Juillet 2023.

[22] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35351. Consulté le 19 Juillet 2023.

[23] https://www.crowdstrike.com/resources/reports/gartner-top-trends-in-cybersecurity-2022-identity-threat-detection-response/. Consulté le 19 Juillet 2023.

Table des matières

Dédicace ii

Remerciements iii

Résumé iv

. iv

Abstract v

. v

Liste des figures vi

Liste des tableaux vii

Liste des acronymes viii

Glossaire 1

Introduction 2

1 Revue de littérature 4

Introduction 4

1.1 Généralités sur Active Directory 4

1.1.1 Définition : Active Directory 4

1.1.2 Mission et fonction de Active Directory 4

1.1.3 Structure de Active Directory 5

1.1.3.1 Schéma 5

1.1.3.2 Configuration 6

1.1.3.3 Domaine 6

1.1.3.4 Base de données 6

1.1.4 Quatre composants techniques de Active Directory 6

1.1.5 Autres terminologies dans Active Directory 7

1.1.5.1 Forêt Active Directory 7

1.1.5.2 Domaine Active Directory 7

1.1.5.3 Objet Active Directory 7

1.1.5.4 Contrôleur de domaine 7

1.1.5.5 Active Directory Domain Services 7

1.2 Historique des services d'annuaire jusqu'à Active Directory 7

1.3 Problèmes de sécurité liés à Active Directory 8

Conclusion . . . 9

2 Analyse, Choix, Justification **10**
Introduction . . . 10
2.1 Différentes méthodes de déploiement de Active Directory . . . 10
2.1.1 Active Directory en Local . . . 10
2.1.2 Azure Active Directory . . . 10
2.1.3 Hybrid Active Directory . . . 11
2.2 Alternatives de Active Directory . . . 11
2.2.1 Lightweight Directory Access Protocol (LDAP) . . . 11
2.2.2 Radius . . . 12
2.2.3 FreeIPA . . . 12
2.3 Architecture du système d'information de l'entreprise LAG Solutions . . . 13
Conclusion . . . 13

3 Test de pénétration, résultats et recommandations **14**
Introduction . . . 14
3.1 Vulnérabilités relatives à Active Directory . . . 14
3.2 Test de pénétration . . . 15
3.2.1 Test de pénétration et ses différentes phases . . . 15
3.2.2 Outils utilisés . . . 16
3.2.2.1 Impacket . . . 16
3.2.2.2 Nmap . . . 16
3.2.2.3 BloodHound . . . 16
3.2.2.4 CrackMapExec (CME) . . . 17
3.2.3 Déroulement et résultats du test de pénétration . . . 18
3.3 Recommandations . . . 24
3.4 Conclusion . . . 25

Conclusion **26**

Bibliographie **27**

Webographie **28**

Table des matières **30**