

# Rapport de compromission



**Entreprise :** Death Star's

**Consultant :** Cédric BLONDEL

**Date :** 19 décembre 2024

# **Sommaire**

- 1. Introduction**
- 2. Contexte et objectif**
- 3. Description de la vulnérabilité**
- 4. Exploitation de la vulnérabilité**
- 5. Score CVSS et impact de la vulnérabilité**
- 6. Recommandations**
- 7. Conclusion**
- 8. Annexes**

# 1. Introduction

Dans le cadre d'un audit de sécurité mené sur l'infrastructure de Death Star's, une vulnérabilité critique a été identifiée sur la machine 10.0.1.200.

Cette machine héberge un service Samba mal configuré, permettant à un attaquant de se connecter en tant qu'invité et d'accéder à des fichiers partagés sans aucune authentification.

Cette faille représente un risque majeur : elle permet l'accès non autorisé à des données sensibles et pourrait, dans un scénario réel, être exploitée pour exfiltrer des informations, modifier des fichiers critiques ou encore obtenir une persistance sur le système.

L'objectif de ce rapport est de :

- Présenter les conditions ayant permis la compromission,
- Décrire le processus d'exploitation,
- Évaluer l'impact de cette vulnérabilité,
- Fournir des recommandations concrètes pour y remédier.

# 2. Contexte et objectif

L'hôte analysé repose sur un environnement Docker basé sur Alpine Linux. Les services exposés incluent :

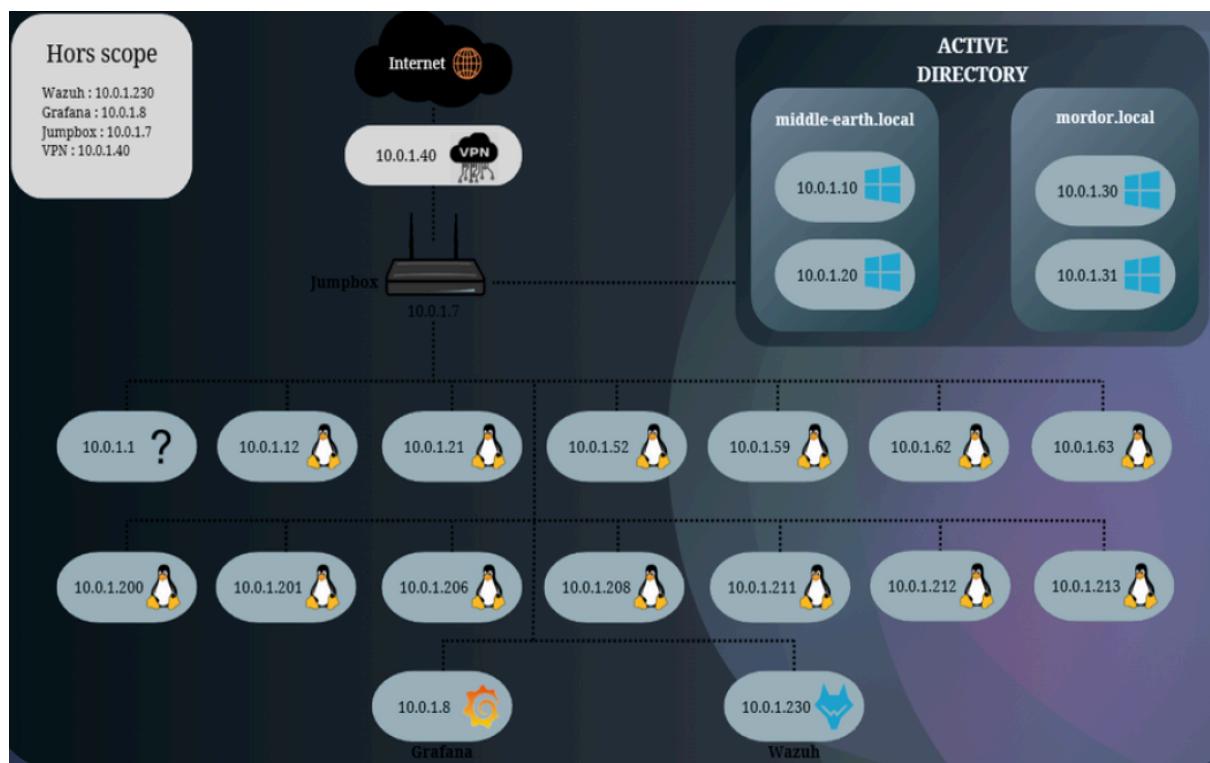
- SSH (ports 22 et 22022) exécuté en tant que root,
- Samba (smbd 4.14.5 et nmbd 4.14.5) également exécuté en tant que root.

Les ports identifiés comme ouverts sont :

- 22/tcp (SSH),
- 22022/tcp (SSH alternatif),
- 139/tcp (NetBIOS-SSN),
- 445/tcp (Microsoft-DS, SMB).

L'analyse des capabilities du conteneur a révélé la présence de privilèges élevés (*cap\_sys\_chroot, cap\_net\_raw, etc.*), ce qui pourrait permettre à un attaquant expérimenté d'effectuer un breakout de conteneur si la faille était combinée avec une autre vulnérabilité.

Ce contexte montre que la machine analysée constitue une surface d'attaque particulièrement sensible au sein du SI.



*L'image ci-dessus illustre la place de la machine 10.0.1.200 dans l'infrastructure globale, mettant en évidence son exposition réseau et son rôle critique.*

### 3. Description de la vulnérabilité

Une vulnérabilité critique a été identifiée dans la configuration du service **Samba** de la machine **10.0.1.200**.

Cette faille permet à un attaquant présent sur le réseau local de se connecter au serveur en utilisant le protocole SMB avec un compte invité et d'accéder sans autorisation aux fichiers partagés.

L'origine de cette vulnérabilité réside dans une combinaison de paramètres incorrectement configurés :

- l'activation des connexions invitées via l'option `guest ok = yes` dans le fichier de configuration `smb.conf`,
- et des permissions excessivement permissives appliquées aux répertoires partagés.

**La vulnérabilité est très facile à exploiter** : un attaquant peut se connecter au serveur via SMB sans fournir d'identifiants, ce qui représente un risque important de fuite de données sensibles et d'élévation de privilèges dans le système d'information.

### 4. Exploitation de la vulnérabilité

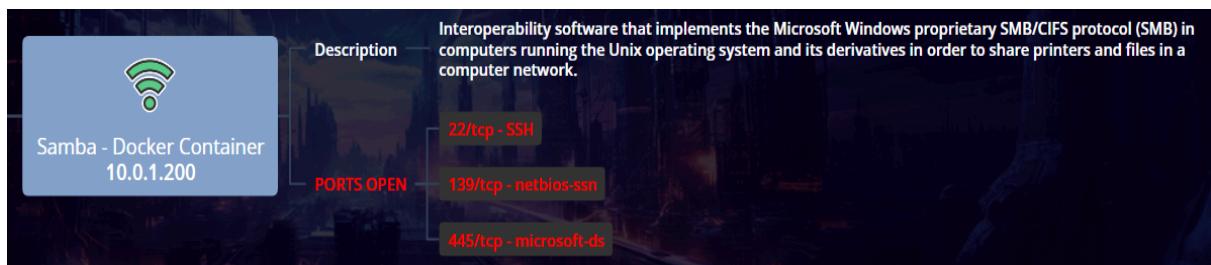
L'exploitation de cette vulnérabilité a été réalisée en plusieurs étapes, permettant de démontrer concrètement les failles liées à la configuration de Samba sur la machine 10.0.1.200.

## 4.1 Phase de reconnaissance

Un scan réseau a révélé que la machine 10.0.1.200 exposait plusieurs ports, dont 22/tcp (SSH), 139/tcp (NetBIOS-SSN) et 445/tcp (Microsoft-DS).

Ces services étant associés aux connexions distantes et au partage de fichiers via SMB/CIFS, ils représentaient une surface d'attaque évidente.

L'analyse des bannières a confirmé que les ports 139 et 445 étaient associés à une instance de Samba 4.6.2 vulnérable.



## 4.2 Connexion en tant qu'invité

Une première tentative avec la commande suivante a permis de lister les partages disponibles sur le serveur Samba : **smbclient -L //10.0.1.200**

Le service a accepté la requête sans demander d'authentification, révélant la présence de plusieurs partages, dont **share**.

Une connexion directe à ce répertoire a ensuite permis de lister son contenu et d'identifier un fichier sensible, **secrets.txt**, confirmant la compromission de données confidentielles.

```
apognu@ares ~ [1]> smbclient -L //10.0.1.200
Password for [WORKGROUP\apognu]:
      Sharename      Type      Comment
      -----
      homes          Disk      Home Directories
      share          Disk      Public File Sharing
      IPC$           IPC       IPC Service (SMB Share)
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 10.0.1.200 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available
apognu@ares ~> smbclient //10.0.1.200/share
Password for [WORKGROUP\apognu]:
Try "help" to get a list of possible commands.
smb: \> ls
.
D      0   Wed Nov 27 01:01:24 2024
..
D      0   Wed Nov 27 01:01:34 2024
secrets.txt      N      27   Tue Nov 26 20:52:30 2024
7941576 blocks of size 1024. 4737028 blocks available
smb: \>
```

## 4.3 Risques supplémentaires

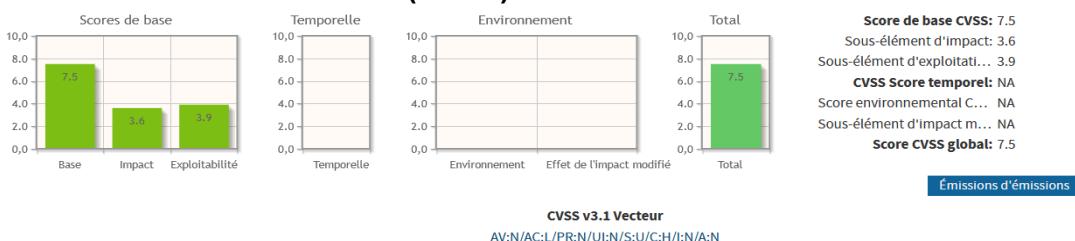
Au-delà de la simple lecture, cette vulnérabilité pourrait être exploitée pour :

- déposer des fichiers malveillants,
- exécuter du code arbitraire,
- ou préparer une élévation de privilèges, compromettant potentiellement tout le système d'information.

## 5. Score CVSS et impact de la vulnérabilité

L'évaluation de la vulnérabilité identifiée dans le service Samba de la machine 10.0.1.200 a été réalisée selon le standard CVSS v3.1.

**Le score obtenu est de 7.5 (Élevé).**



**Score de la base Métrologie**

Exploitabilité métriques				Champ d'application (S)			Impact métrique		
Attaque Vecteur (AV)				Inchangé (S:U)	Changement (S:C)	Confidentialité Impact (C)			
Réseau (AV:N)    Adjacent Réseau (AV:A)    Local (AV:L)    Physique (AV:P)				Néant (C:N)	Faible (C:L)	Élevé (C:H)	Intégrité Impact (I)		
Attaque Complexité (AC)				Faible (AC:L)	Élevé (AC:H)	Néant (I:N)	Faible (I:L)	Élevé (I:H)	
Priviléges Requis (PR)				Néant (PR:N)	Faible (PR:L)	Élevé (PR:H)	Disponibilité Impact (A)		
Utilisateur Interaction (UI)				Néant (UI:N)	Requis (UI:R)	Néant (A:N)	Faible (A:L)	Élevé (A:H)	

*Ce score reflète une faille sérieuse qui compromet principalement la confidentialité des données, sans impact direct sur l'intégrité ni la disponibilité.*

## Justification :

La configuration du fichier smb.conf autorise explicitement les connexions invitées

```
[global]
netbios name = SMB Share
workgroup = WORKGROUP
server string = SMB Share
server role = standalone
map to guest = bad user
usershare allow guests = yes

[homes]
comment = Home Directories
browseable = no
writable = yes

[share]
comment = Public File Sharing
path = /share
browseable = yes
read only = yes
guest ok = yes
```

Cela permet à un attaquant d'accéder en lecture seule aux répertoires partagés et de télécharger des fichiers sensibles (exemple : secret.txt).

En revanche, l'absence de droits d'écriture ou d'exécution explique que l'intégrité et la disponibilité ne soient pas impactées, ce qui justifie la note finale de **7.5**.

## 6. Recommandations

Afin de sécuriser le service Samba exposé sur la machine 10.0.1.200, plusieurs mesures correctives doivent être mises en œuvre.

Il est tout d'abord nécessaire de désactiver l'accès invité dans la configuration smb.conf, afin d'empêcher toute connexion non authentifiée. L'accès aux partages devra être exclusivement réservé aux utilisateurs légitimes, protégés par des identifiants et des mots de passe robustes, conformes aux recommandations de l'ANSSI.

Il est également recommandé de renforcer la protection contre les attaques par force brute, notamment à l'aide d'un mécanisme tel que Fail2ban, permettant de bloquer automatiquement les tentatives répétées de connexion non autorisée.

Enfin, une supervision renforcée doit être mise en place, incluant des agents de détection d'intrusion (IDS) et la centralisation des journaux d'accès Samba, afin d'assurer une traçabilité complète et de détecter rapidement toute tentative d'exploitation.

### Validation de la remédiation

Après mise en œuvre des mesures correctives, une nouvelle tentative de connexion au service Samba (10.0.1.200) a été effectuée.

Le résultat montre que l'accès invité a bien été désactivé :

```
apognu@ares ~ [1]> smbclient -L //10.0.1.200
Password for [WORKGROUP\apognu]:
      Sharename      Type      Comment
      -----
      IPC$          IPC       IPC Service (SMB Share)
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
Protocol negotiation to server 10.0.1.200 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available
apognu@ares ~> smbclient //10.0.1.200/share
Password for [WORKGROUP\apognu]:
tree connect failed: NT_STATUS_ACCESS_DENIED
apognu@ares ~ [1]>
```

L'erreur *NT\_STATUS\_ACCESS\_DENIED* confirme que les partages ne sont plus accessibles sans authentification, attestant de la correction effective de la vulnérabilité.

## 7. Conclusion

L'audit réalisé sur la machine 10.0.1.200 a permis d'identifier une mauvaise configuration critique du service Samba, ouvrant la voie à un accès non authentifié aux fichiers partagés. Cette vulnérabilité, facilement exploitable, démontrait un risque élevé pour la confidentialité et l'intégrité des données de l'organisation.

La mise en œuvre des mesures correctives, incluant la désactivation de l'accès invité, le durcissement des politiques de mots de passe, le déploiement de mécanismes de défense tels que Fail2ban et l'intégration de la supervision via des outils de détection, a permis de corriger efficacement cette faille.

Ces actions renforcent significativement la posture de sécurité de l'infrastructure et réduisent la probabilité de futurs incidents similaires. Toutefois, il est recommandé de maintenir une vigilance continue par le biais d'audits réguliers, de tests de sécurité et de formations des utilisateurs.

