

# Rapport d'évaluation et de remédiation de l'infrastructure

## Introduction:

Ce rapport expose l'évaluation approfondie et les mesures correctives mises en œuvre au cours du projet final de l'équipe Blue Cyber. L'objectif principal est de présenter nos actions entreprises chez Jedha, en mettant en lumière les démarches entreprises pour évaluer et renforcer l'infrastructure existante. Notre approche repose sur l'application des meilleures pratiques en matière d'administration et de sécurité des infrastructures, avec une focalisation particulière sur la disponibilité, l'intégrité et la confidentialité des données.

Dans le cadre de cet audit, l'accès a été facilité par la fourniture de noms d'utilisateur et de mots de passe par le client.

L'ensemble des machines identifiées présentait une ouverture sur le Port 22022. Par le biais de la Jumpbox, nous avons réussi à effectuer des opérations de pivoting sur toutes ces machines.

November 28, 2023

To:  
Blue Team Stormtroopers  
Death Star Defense Headquarters

Dear Blue Team Stormtroopers,

It is imperative that we maintain the utmost security of the Death Star against the constant threat of rebel hackers. Your dedication to this mission is of paramount importance to the Galactic Empire.

As we continue to strengthen our defenses, I would like to provide you with a list of vulnerable machines on the Death Star that require your immediate attention. These machines may be targeted by rebel hackers seeking to exploit weaknesses in our system. You are authorized to access and secure these machines using the provided credentials.

• **List of Vulnerable Machines:**

- 10.0.1.53
- 10.0.1.59
- 10.0.1.62
- 10.0.1.200
- 10.0.1.202
- 10.0.1.206
- 10.0.1.208
- 10.0.1.211
- 10.0.1.213

Please make it a priority to assess and fortify these vulnerable systems to prevent any unauthorized access or compromise. The security of the Death Star relies on your vigilance and expertise.

You may connect to any of these machines using the following credentials on port 22022:

Username: root  
Password: BigB0ngTh30ry

Remember, failure is not an option. The fate of the Galactic Empire rests on your shoulders.

Sincerely,

Darth Vader  
*Dark Lord of the Sith*  
*Supreme Commander of the Death Star*

## Synthèse:

Au cours de notre analyse approfondie de l'infrastructure, plusieurs lacunes significatives en matière de sécurité ont été mises en lumière, nécessitant une attention immédiate. En résumé, les points critiques identifiés comprennent l'absence de certaines mesures de sécurité fondamentales :

1. **Absence de Firewall** : L'infrastructure ne dispose pas d'une barrière de protection efficace, exposant ainsi le réseau à des menaces externes non autorisées.
2. **Absence de WAF (Web Application Firewall)** : La protection des applications web est insuffisante, laissant ainsi des vulnérabilités potentielles dans les applications exposées.
3. **Absence d'EDR/IPS (Endpoint Detection and Response / Intrusion Prevention System)** : La couche de défense au niveau des points d'extrémité est inexistante, augmentant le risque d'attaques ciblées et de compromission des systèmes.
4. **Politique de Mot de Passe Faible** : Les pratiques de gestion des mots de passe présentent des faiblesses, créant des vulnérabilités potentielles face à des attaques par force brute.
5. **Mauvaise Configuration du SIEM (Security Information and Event Management)** : Le système de gestion des informations de sécurité et d'événements est mal configuré, compromettant son efficacité dans la détection précoce des incidents de sécurité.
6. **Absence de Mise à Jour** : Les systèmes ne sont pas régulièrement mis à jour, exposant l'infrastructure à des failles de sécurité connues.
7. **Mauvaise Centralisation des Logs** : La centralisation des journaux d'événements est défaillante, entravant la capacité à détecter et à répondre efficacement aux incidents de sécurité.

Ces constats soulignent la nécessité urgente d'implémenter des mesures correctives et de renforcer la posture globale de sécurité de l'infrastructure.

## Evaluation et remédiations de l'infrastructure

### 1. Sensibilisation et Formation en Sécurité :

---

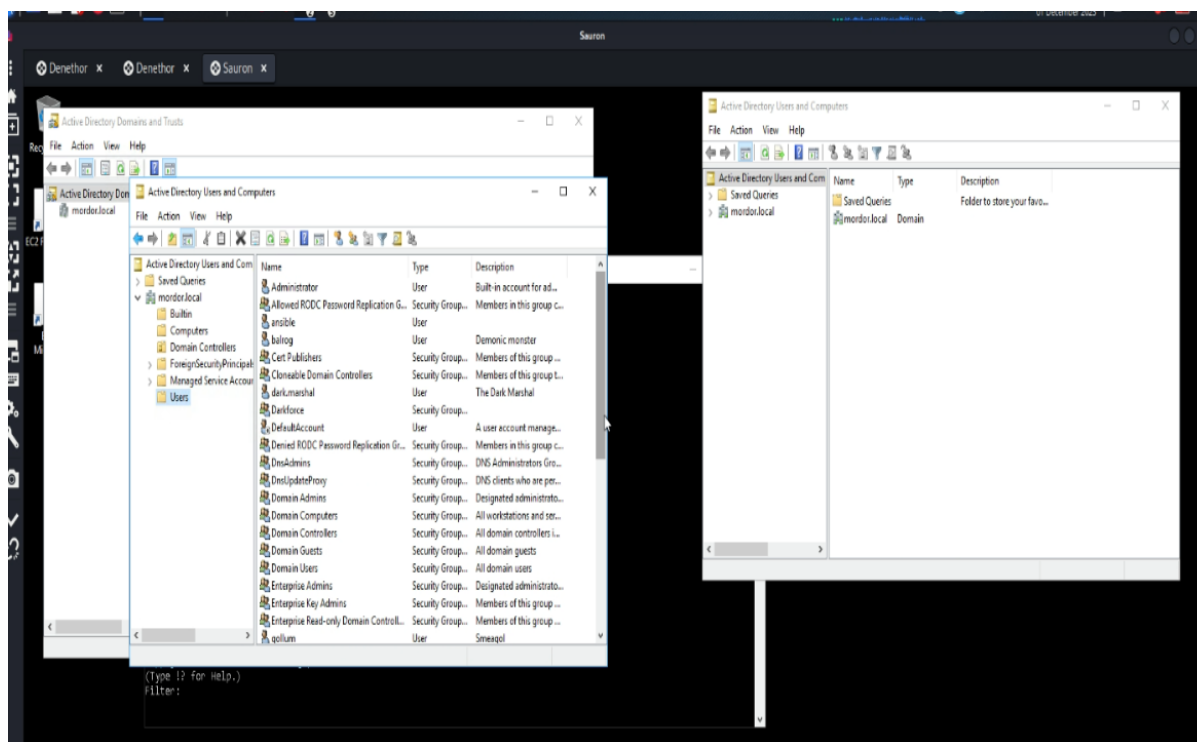
**Évaluation** : Les politiques de sécurité ont fait l'objet d'une révision, mais une communication et une formation efficaces auprès du personnel restent à améliorer.

**Remédiation :** Nous prévoyons de lancer une campagne de sensibilisation visant à informer le personnel des mises à jour des politiques de sécurité. Des sessions de formation régulières seront organisées pour assurer une compréhension approfondie des directives de sécurité.

## 2. Audit et Gestion des Accès :

**Évaluation :** Les contrôles d'accès actuels ne respectent pas les principes du moindre privilège.

**Remédiation :** Nous initierons un audit approfondi des droits d'accès, préconisant la mise en place d'une politique du moindre privilège sur l'Active Directory. Des revues régulières seront instaurées pour maintenir cette approche de manière constante.



## 3. Pare-feu et Filtrage :

**Évaluation :** La configuration du pare-feu a fait l'objet d'une révision, mais il est impératif d'accroître la fréquence d'analyse des journaux.

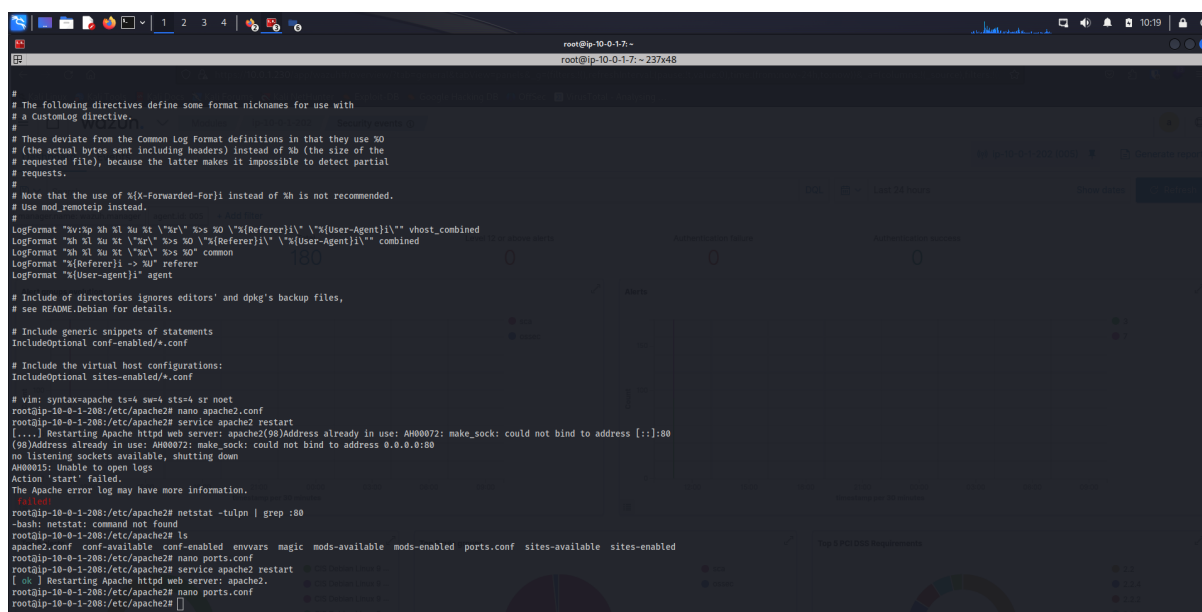
**Remédiation :** Nous prévoyons d'établir un processus de surveillance continue des journaux du pare-feu. Des analyses fréquentes seront réalisées afin de détecter

promptement toute activité suspecte, renforçant ainsi notre capacité à réagir rapidement aux éventuelles menaces.

#### 4. Mise à Jour et Patch Management :

**Évaluation :** Bien que la gestion des correctifs soit en place, l'application des correctifs de sécurité pourrait être accélérée.

**Remédiation :** Nous entreprendrons une révision approfondie du processus de gestion des correctifs, mettant un accent particulier sur la mise en œuvre rapide des correctifs de sécurité critiques. L'objectif est d'optimiser la réactivité face aux vulnérabilités et de renforcer la résilience de l'infrastructure.



```
root@ip-10-0-1-7: ~
root@ip-10-0-1-7: ~ 237x48

# The following directives define some format nicknames for use with
# a CustomLog directive.
#
# These deviate from the Common Log Format definitions in that they use %O
# (the actual bytes sent including headers) instead of %b (the size of the
# requested file), because the latter makes it impossible to detect partial
# requests.
#
# Note that the use of %[X-Forwarded-For] instead of %h is not recommended.
# Use mod_remoteip instead.
#
LogFormat "%v:%p %h %l %u %t \"%r\" %s %O \"%[Referer]i\" \"%[User-Agent]i\"" vhost_combined
LogFormat "%h %l %u %t \"%r\" %s %O \"%[Referer]i\" \"%[User-Agent]i\"" combined
LogFormat "%h %l %u %t \"%r\" %s %O" common
LogFormat "%[Referer]i -> %U" referer
LogFormat "%[User-Agent]i" agent

# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.

# Include generic snippets of statements
IncludeOptional conf-enabled/*.conf

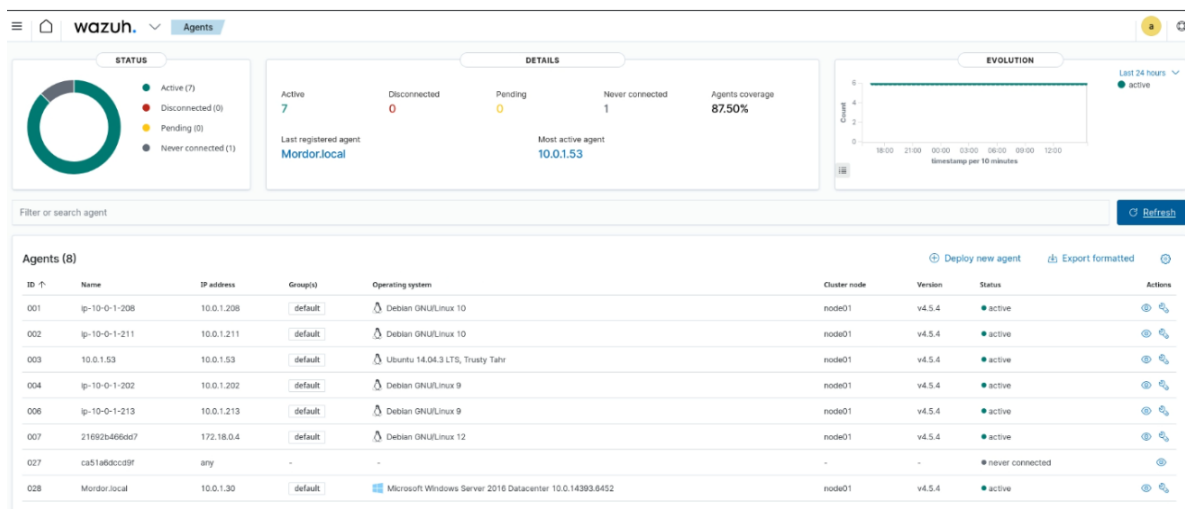
# Include the virtual host configurations:
IncludeOptional sites-enabled/*.conf

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
root@ip-10-0-1-208:/etc/apache2# nano apache2.conf
root@ip-10-0-1-208:/etc/apache2# service apache2 restart
[....] Restarting Apache httpd web server: apache2(90)Address already in use: AH00072: make_sock: could not bind to address [::]:80
(90)Address already in use: AH00072: make_sock: could not bind to address 0.0.0.0:80
no listening sockets available, shutting down
AH00015: Unable to open logs
Action 'start' failed.
The Apache error log may have more information.
root@ip-10-0-1-208:/etc/apache2# netstat -tulpn | grep :80
--bash: netstat: command not found
root@ip-10-0-1-208:/etc/apache2# ls
apache2.conf  conf-available  conf-enabled  envvars  magic  mods-available  mods-enabled  ports.conf  sites-available  sites-enabled
root@ip-10-0-1-208:/etc/apache2# nano ports.conf
root@ip-10-0-1-208:/etc/apache2# service apache2 restart
[ ok ] Restarting Apache httpd web server: apache2.
root@ip-10-0-1-208:/etc/apache2# nano ports.conf
root@ip-10-0-1-208:/etc/apache2#
```

#### 5. Sécurité des Terminaux :

**Évaluation :** Aucune solution dédiée à la sécurité des terminaux n'était en place. La conformité des terminaux nécessitait une surveillance plus efficace.

**Remédiation :** Pour remédier à cette lacune, notre équipe a implémenté la solution Wazuh, intégrant des agents sur l'ensemble des terminaux. Ce dispositif permet la mise en place d'un processus de surveillance continue assurant la conformité des terminaux. Des rapports réguliers sur l'état de la sécurité des terminaux seront générés, fournissant une visibilité accrue et permettant une réactivité proactive aux éventuelles menaces.



## 6. Surveillance du Réseau :

**Évaluation :** Aucune solution active de surveillance du réseau n'a été identifiée, mettant en évidence un besoin pressant d'améliorer nos capacités de détection et de réponse aux incidents.

**Remédiation :** Nous envisageons des investissements ciblés visant à renforcer nos capacités de détection et de réponse aux incidents. Une initiative clé sera la mise en place d'exercices réguliers de simulation d'incidents, permettant d'évaluer et d'améliorer l'efficacité de notre processus de réponse aux événements de sécurité.



## 7. Cryptographie :

**Évaluation :** Actuellement, la cryptographie est implémentée via la connexion SSH, cependant, l'utilisation de protocoles plus robustes est recommandée.

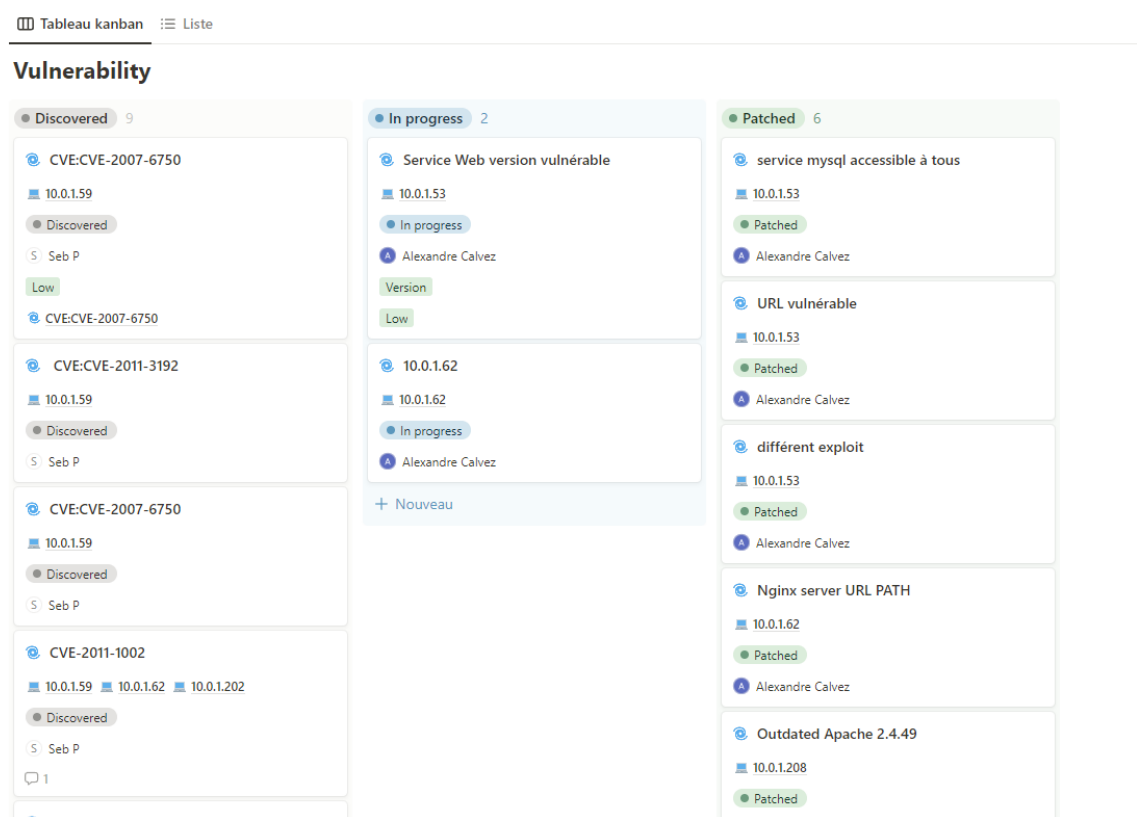
**Remédiation :** Nous proposons la mise en place de protocoles de cryptographie plus solides. Une révision complète des algorithmes de chiffrement sera effectuée, conformément aux meilleures pratiques, pour renforcer la sécurité des communications.

## 8. Gestion des Vulnérabilités :

**Évaluation :** Bien que le processus de gestion des vulnérabilités soit en place, une amélioration de la réactivité aux vulnérabilités critiques est nécessaire.

**Remédiation :** Nous envisageons l'automatisation de la détection des vulnérabilités critiques et l'établissement de procédures claires pour une priorisation et un déploiement rapides des correctifs.

# Vulnerability management



## **9. Gestion des Incidents :**

**Évaluation :** Aucun plan de gestion des incidents n'est actuellement en place (PRA ou PCA).

**Remédiation :** Nous planifierons des exercices de simulation d'incidents réguliers pour tester la capacité de réponse, en mettant à jour le plan de gestion des incidents en conséquence.

## **10. Contrôle d'Identité :**

**Évaluation :** Aucune solution d'authentification à double facteur n'est en place.

**Remédiation :** Nous instituerons des revues trimestrielles des droits d'accès et utiliserons des outils d'analyse pour détecter et corriger les anomalies d'accès.

## **11. Sauvegarde et Récupération :**

**Évaluation :** Actuellement, aucune politique de sauvegarde n'est en place, et il n'y a pas de serveur de sauvegarde.

**Remédiation :** Nous planifierons des tests mensuels de restauration à partir des sauvegardes et réviserons régulièrement la politique de sauvegarde pour garantir une protection complète des données critiques.

## **12. Sécurité Applicative :**

**Évaluation :** L'intégration de la sécurité dans le développement est en cours, mais des tests de sécurité réguliers sont nécessaires.

**Remédiation :** Nous intégrerons la sécurité dès les phases initiales du développement et mettrons en place des évaluations régulières de la sécurité des applications, ainsi qu'une revue de code.

## **13. Audit et Conformité :**

**Évaluation :** Aucun audit de sécurité n'a été effectué.

**Remédiation :** Nous mettrons en œuvre une solution automatisée pour le suivi continu de la conformité et planifierons des audits réguliers pour garantir la



conformité aux normes et aux réglementations.

#### **14. Analyse des Menaces :**

**Évaluation :** La veille sur les menaces émergentes doit être renforcée.

**Remédiation :** Nous mettrons en place un service de veille sur les menaces pour assurer une détection précoce des menaces émergentes et ajusterons les défenses en conséquence.

#### **15. Documentation et Rapports :**

**Évaluation :** Aucun document ou rapport de sécurité n'a pu être récupéré.

**Remédiation :** Nous instaurerons un calendrier régulier de génération de rapports sur l'état de la cybersécurité et mettrons à jour la documentation des configurations de manière régulière.

### **Conclusion:**

La mise en œuvre rigoureuse de ces remédiations contribuera significativement à renforcer la maturité en cybersécurité de notre infrastructure. Il est vivement recommandé de suivre ces recommandations de manière systématique et de procéder à des évaluations périodiques pour garantir la résilience face aux menaces émergentes.