RAPPORT D'AUDIT DE SÉCURITÉ (Pentest)

Cible : Infrastructure Docker (Samba & WebApp)
Date : 22 Novembre 2025
Auditeur : Zoubir Rayan
Entreprise : Zoubir Organisation

Autorisation :

- **Approbation :** Validée par M. Ludovic Laborde.
- **Objectif technique :** Compromission de systèmes et élévation de privilèges.
- **Infrastructure cible :** Conteneurs Docker vulnérables.
- **Scope Réseau :** Sous-réseaux 172.18.0.0/16 et 172.19.0.0/16.

CONFIDENTIALITÉ & DISCLAIMER

> **Attention :** Ce rapport contient des détails critiques sur l'architecture du système. Il est classé "Usage Interne".

Les opérations offensives décrites ici ont été réalisées exclusivement sur les machines désignées, dans un but éducatif et éthique, sans impact sur les systèmes de production réels.

CONTACT Ludovic Laborde – Professeur de Pentesting *Email :* ludovic@connect3s.fr

1. Résumé Exécutif (Executive Summary)

Durant cet audit, nous avons évalué la sécurité d'une infrastructure composée de deux serveurs segmentés. L'objectif était d'identifier les vulnérabilités permettant de compromettre les systèmes.

Résultats clés :

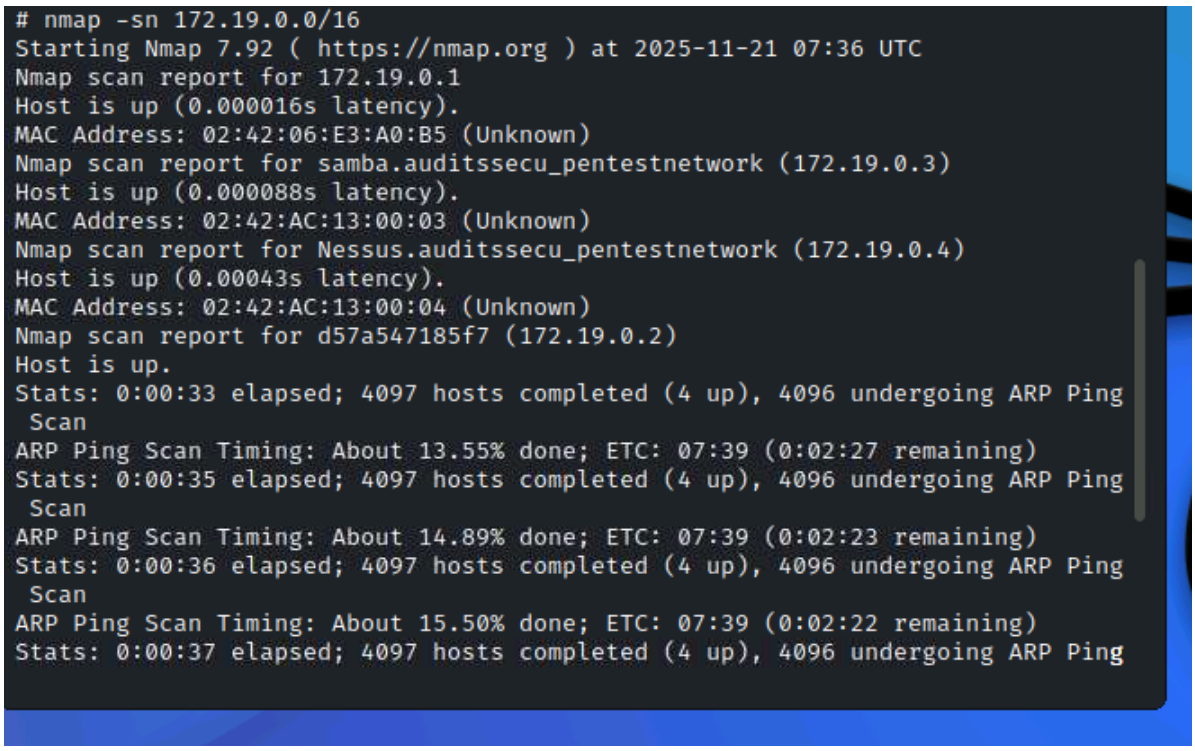
- **Niveau de risque global : CRITIQUE.**
- Nous avons réussi à prendre le contrôle total (Root) des deux serveurs.
- Le réseau interne, censé être protégé, est accessible depuis l'extérieur via un "Pivot".
- Des correctifs urgents sont nécessaires sur le service Samba et la configuration des droits administrateurs (sudo).

2. Méthodologie Technique (Selon PTES)

Phase 1 : Collecte d'informations (Intelligence Gathering)

Objectif : Identifier les machines actives sur le réseau accessible.

- **Outil utilisé :** Nmap
- **Action :** Scan du réseau 172.19.0.0/16 (Ping Sweep).
- **Résultat :** Découverte de la machine cible Samba (IP : 172.19.0.X).
- **Scan de service :** Le scan de ports a révélé les ports 139 et 445 ouverts (Service Samba version 4.6.3).



```
# nmap -sn 172.19.0.0/16
Starting Nmap 7.92 ( https://nmap.org ) at 2025-11-21 07:36 UTC
Nmap scan report for 172.19.0.1
Host is up (0.000016s latency).
MAC Address: 02:42:06:E3:A0:B5 (Unknown)
Nmap scan report for samba.auditssecu_pentestnetwork (172.19.0.3)
Host is up (0.000088s latency).
MAC Address: 02:42:AC:13:00:03 (Unknown)
Nmap scan report for Nessus.auditssecu_pentestnetwork (172.19.0.4)
Host is up (0.00043s latency).
MAC Address: 02:42:AC:13:00:04 (Unknown)
Nmap scan report for d57a547185f7 (172.19.0.2)
Host is up.
Stats: 0:00:33 elapsed; 4097 hosts completed (4 up), 4096 undergoing ARP Ping
 Scan
ARP Ping Scan Timing: About 13.55% done; ETC: 07:39 (0:02:27 remaining)
Stats: 0:00:35 elapsed; 4097 hosts completed (4 up), 4096 undergoing ARP Ping
 Scan
ARP Ping Scan Timing: About 14.89% done; ETC: 07:39 (0:02:23 remaining)
Stats: 0:00:36 elapsed; 4097 hosts completed (4 up), 4096 undergoing ARP Ping
 Scan
ARP Ping Scan Timing: About 15.50% done; ETC: 07:39 (0:02:22 remaining)
Stats: 0:00:37 elapsed; 4097 hosts completed (4 up), 4096 undergoing ARP Ping
```

```
Nmap scan report for samba.auditssecu_pentestnetwork (172.19.0.3)
Host is up (0.00038s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 02:42:AC:13:00:03 (Unknown)

Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\172.19.0.3\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Samba Server Version 4.6.3)
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|   \\172.19.0.3\myshare:
|     Type: STYPE_DISKTREE
|     Comment: smb share test
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\share
|_    Anonymous access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 5.87 seconds
Segmentation fault (core dumped)
```

Phase 2 : Modélisation de la menace & Analyse de vulnérabilité

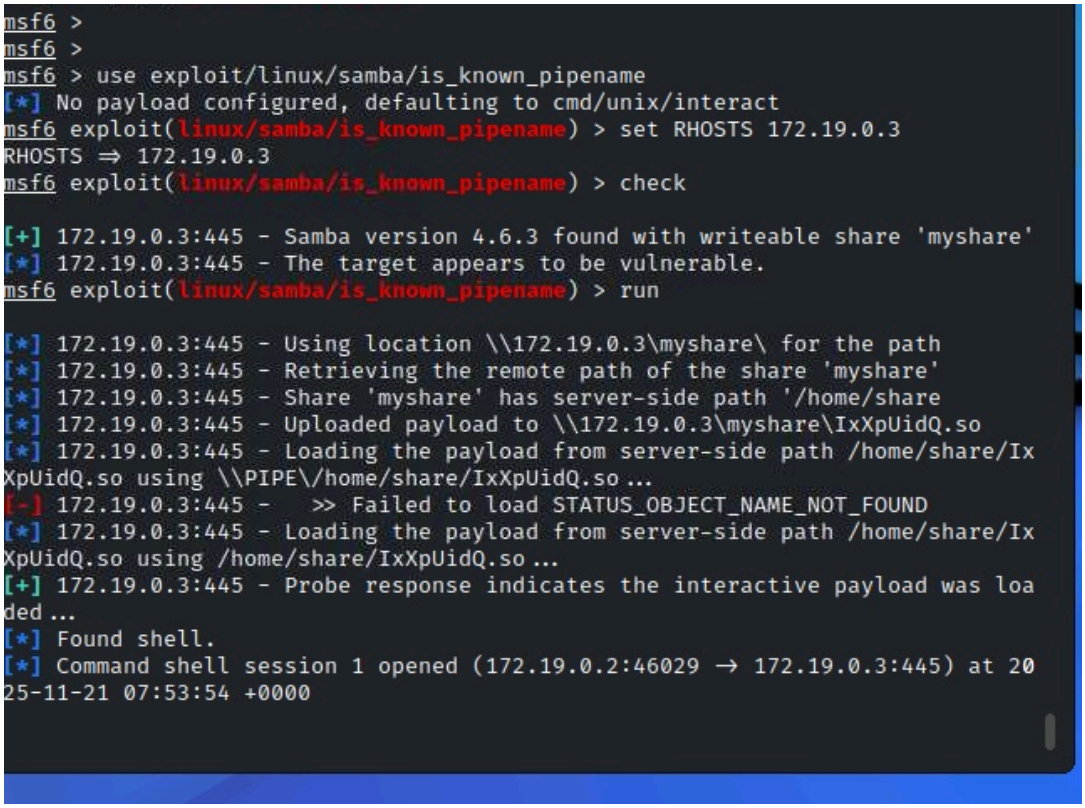
Objectif : Trouver une faille exploitable sur le service découvert.

- **Vulnérabilité identifiée :** CVE-2017-7494 (surnommée "SambaCry").
- **Description :** Cette version de Samba permet le chargement de bibliothèques partagées malveillantes via un partage inscriptible.
- **Sévérité :** Critique (Exécution de code à distance).

Phase 3 : Exploitation (Machine 1 - Samba)

Objectif : Obtenir un accès initial au système.

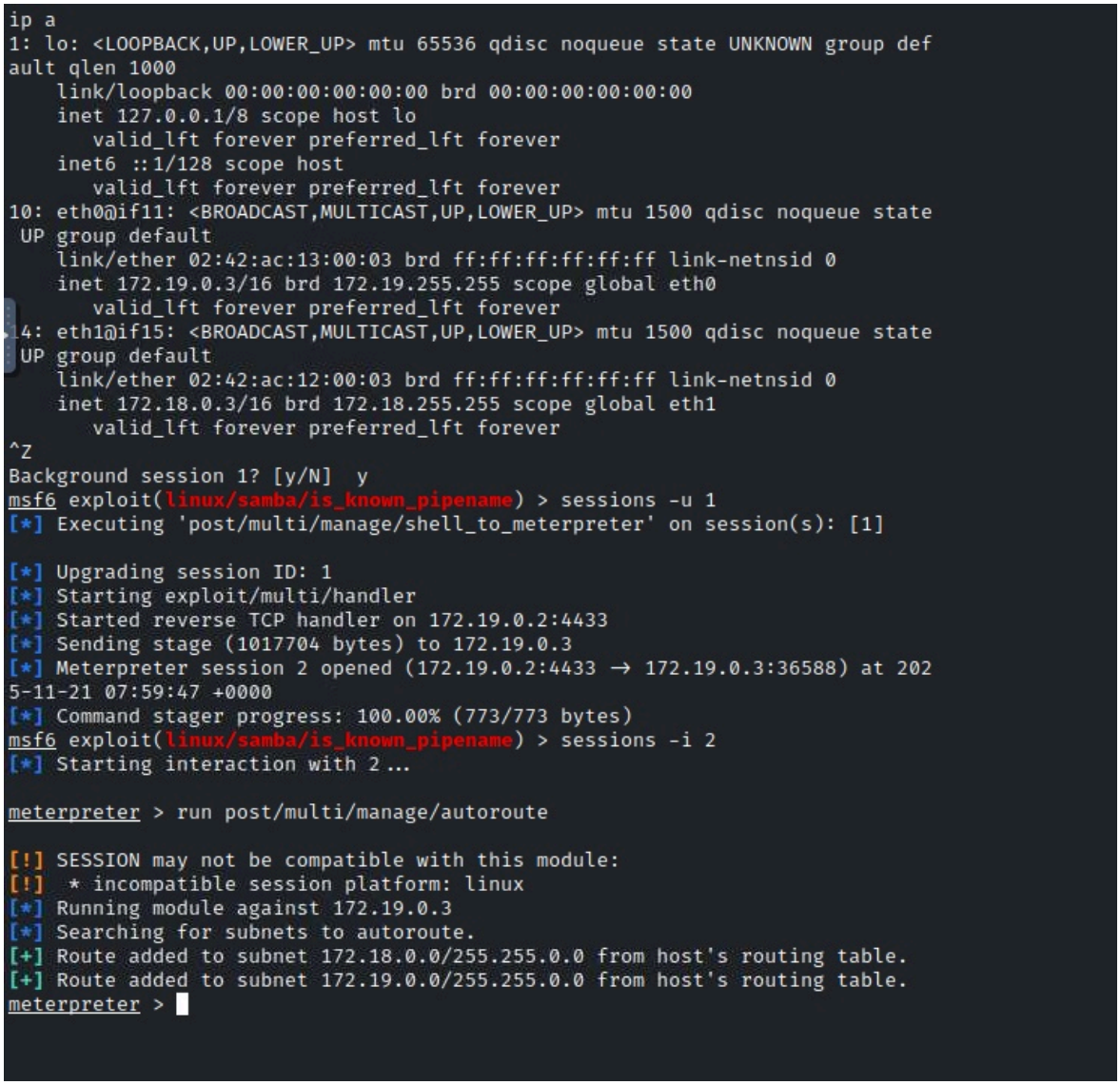
- **Outil :** Metasploit Framework (exploit/linux/samba/is_known_pipename).
- **Action :** Exécution de l'exploit contre la cible.
- **Résultat :** Ouverture d'une session "Command Shell" avec les privilèges **Root**.
- **Preuve :** La commande id renvoie uid=0(root).



Phase 4 : Post-Exploitation & Pivot (Discovery & Pivoting)

Objectif : Explorer le réseau interne depuis la machine compromise.

- **Découverte :** La commande ip a sur la machine Samba a révélé une seconde interface réseau (eth1) connectée à un sous-réseau caché (172.18.0.0/24).
- **Action (Pivoting) :** Utilisation du module autoroute de Metasploit pour router le trafic à travers la machine Samba.
- **Scan interne :** Découverte d'une seconde machine (WebApp) à l'adresse 172.18.0.2 portant un service Web (Port 80).
- **Tunneling :** Mise en place de portfwd pour accéder au site web interne depuis la machine attaquante.



Phase 5 : Exploitation (Machine 2 - WebApp)

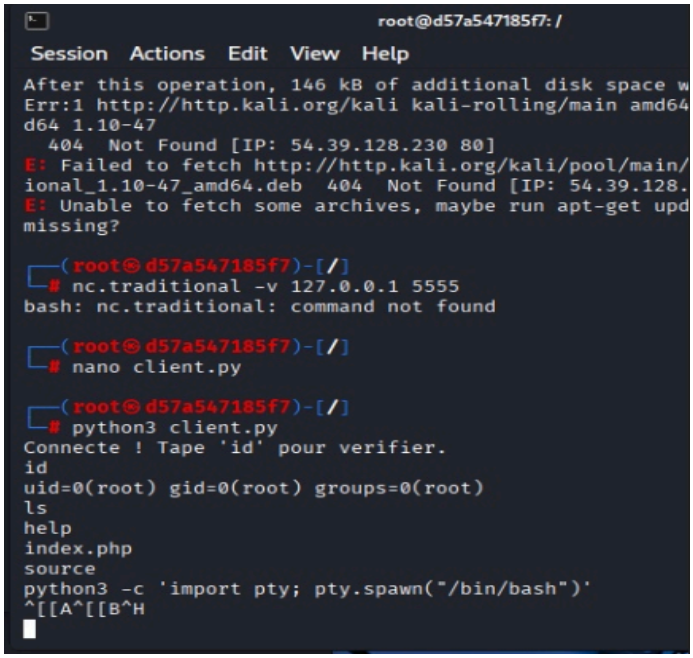
Objectif : Compromettre le serveur Web interne.

- **Cible :** DVWA (Damn Vulnerable Web Application).
- **Vulnérabilité :** Command Injection (Injection de commande).
- **Vecteur :** Le formulaire "Ping" ne filtre pas correctement les entrées utilisateur, permettant d'enchaîner des commandes Linux (ex: 127.0.0.1; cat /etc/passwd).
- **Automatisation :** Création d'un script Python pour exploiter la faille malgré l'instabilité du tunnel réseau.

Phase 6 : Escalade de Privilèges (Privilege Escalation)

Objectif : Obtenir les droits administrateur (Root) sur la WebApp.

- **Analyse :** La commande sudo -l a révélé une mauvaise configuration : l'utilisateur www-data pouvait lancer /bin/nc (Netcat) en tant que Root sans mot de passe.
- **Exploitation :**
  1. Utilisation du script Python pour lancer un Netcat en écoute (sudo nc -l -p 5555 -e /bin/sh).
  2. Connexion à ce port depuis la machine attaquante.
- **Résultat Final :** Obtention d'un shell **Root** sur la deuxième machine.



3. Recommandations (Remédiation)

Pour sécuriser cette infrastructure, il est impératif d'appliquer les correctifs suivants :

1. **Mettre à jour Samba :** Passer à une version ultérieure à 4.6.4 pour corriger la faille SambaCry.
2. **Cloisonner le réseau :** Mettre en place des règles de pare-feu (iptables) pour empêcher la machine Samba de communiquer librement avec la WebApp sur tous les ports.
3. **Sanitiser les entrées Web :** Modifier le code PHP de l'application pour filtrer les caractères spéciaux (;, &, |) afin d'empêcher l'injection de commandes.
4. **Durcir la configuration Sudo :** Retirer le droit NOPASSWD pour l'utilitaire nc (Netcat) dans le fichier /etc/sudoers, car c'est un binaire trop dangereux pour être laissé en accès libre.

Conclusion

L'audit a démontré qu'une seule vulnérabilité sur un service exposé (Samba) a permis, par rebond (Pivot), de compromettre l'intégralité du réseau interne jusqu'au niveau administrateur.