Rapport d'Investigation Numérique

Compromission du serveur srv01.local

Auteur : [Nom de l'analyste]
Date : [Date du rapport]
Version : 1.0

---

1. Résumé Exécutif

Le 04/02/2025, une intrusion a été détectée sur le serveur Linux **srv01.local**. L'analyse des logs a révélé qu'un attaquant a utilisé une attaque par force brute pour obtenir un accès SSH avec l'utilisateur user. Une escalade de privilège à root a ensuite été effectuée. Enfin, une exfiltration de données a été identifiée via une requête HTTP POST vers une IP externe.

Ce rapport présente les éléments de preuve collectés et les recommandations pour prévenir de futures intrusions.

---

2. Informations Générales

- **Date de l'investigation** : 04/02/2025
- **Organisation concernée** : [Nom de l'entreprise]
- **Investigateur(s)** : [Nom]
- **Matériel analysé** :
    - **Système** : Linux srv01.local
    - **IP** : 192.168.1.10
    - **Image mémoire** : memory.raw
    - **Logs** : auth.log
    - **Capture réseau** : network.pcap

---

3. Collecte des Preuves

Les éléments suivants ont été collectés et analysés :

- **Logs d'authentification** (/var/log/auth.log)
- **Dump mémoire** (image RAM memory.raw)
- **Fichier PCAP** (network.pcap)
- **Empreintes cryptographiques des fichiers analysés** :
- sha256sum memory.raw auth.log network.pcap

---

4. Analyse et Découvertes

4.1 Analyse des Logs (auth.log)

Connexion SSH suspecte

grep "sshd" auth.log

Résultat :

Feb 4 10:32:01 srv01 sshd[1234]: Failed password for invalid user admin from 192.168.1.100 port 4545 ssh2

Feb 4 10:32:02 srv01 sshd[1234]: Accepted password for user from 192.168.1.100 port 4545 ssh2

Feb 4 10:33:00 srv01 sudo: user : TTY=pts/1 ; PWD=/home/user ; USER=root ; COMMAND=/bin/bash

IP de l'attaquant : 192.168.1.100
Escalade de privilège : sudo -i exécuté par user

4.2 Analyse Mémoire (RAM)

Identification des processus actifs

volatility -f memory.raw --profile=LinuxUbuntu pslist

Processus suspect détecté :

PID   PPID Name   Command Line

4567 1   malware   /tmp/malware

Fichier suspect en exécution : /tmp/malware

4.3 Analyse Réseau (PCAP)

Requête suspecte vers une IP externe

tshark -r network.pcap -Y "http.request.method == POST"

Résultat :

192.168.1.10 -> 203.0.113.50 POST /upload.php

Exfiltration de données vers 203.0.113.50

---

5. Conclusions et Recommandations

5.1 Synthèse des événements

- **L'attaquant (192.168.1.100) a réussi à se connecter en SSH** avec l'utilisateur user.
- **Il a escaladé ses privilèges en root**.
- **Un programme malveillant (éventuel malware) a été identifié en mémoire**.
- **Une exfiltration de données via HTTP POST vers une IP externe a été détectée**.

5.2 Recommandations

Désactiver l'accès SSH par mot de passe et utiliser des clés SSH.
Vérifier et renforcer les permissions sudo.
Mettre en quarantaine la machine compromise.
Scanner le système pour détecter d'autres présences malveillantes.

---

6. Annexes

Commandes utilisées

sha256sum memory.raw

volatility -f memory.raw --profile=LinuxUbuntu pslist

volatility -f memory.raw --profile=LinuxUbuntu filescan

wireshark network.pcap

Pièces Jointes

- **Fichiers logs analysés**
- **Hash des fichiers pour vérification**
- **Captures d'écran des preuves**

Fin du rapport.