🎓 Rapport d’Investigation Forensic - Cas 3

Système Linux compromis – Simulation pédagogique et réaliste

Auteur : Lets'hack

Établissement : La Plateforme – Marseille

Date de début d’analyse : 15 septembre 2025

Date de fin d’analyse : 23 septembre 2025

Encadrant : Mr Joffrey Weertz – Module Forensic

Sommaire

Cas 3 – Système Linux compromis (Ubuntu 22.04)

1. Introduction

Ce rapport présente les résultats d'une investigation numérique menée dans le cadre d'un exercice pédagogique proposé par l'école La Plateforme à Marseille. L'objectif était de simuler une attaque réelle sur un serveur Linux hébergeant un site e-commerce vulnérable, afin de mettre en pratique les compétences en forensic et détection d'activités malveillantes.

2. Cadre du scénario

Le cas étudié repose sur une simulation réaliste d'un serveur Ubuntu 22.04 compromis, hébergeant l'application DVWA (Damn Vulnerable Web Application). Ce serveur, situé au Royaume-Uni, a été victime d'une série d'attaques ayant conduit à sa défiguration, à l'installation de webshells, et à des tentatives d'exfiltration de données. L'image forensique fournie contient les artefacts nécessaires à une analyse approfondie.

3. Présentation du cas

- **Date de compromission :** 6 juin 2024
- **Système ciblé :** Ubuntu 22.04.3
- **Nom d'hôte (Le patient Zéro):** shop
- **IP locale :** 10.24.44.5
- **Domaine :** shop.example.org
- **Serveur DNS :** 10.24.44.1
- **Application vulnérable :** DVWA (Damn Vulnerable Web Application)
- **Image forensique :** Case.E01 – Format EnCase – Taille ≈ 5 GB
- **Source :** CFReDS (NIST)
- **Auteur** : Benjamin Donnachie

4. Mise sous séquestre et vérification

Type d'image	Format	Outil utilisé	Date d'acquisition	Hash initial (MD5 / SHA256)	Hash final (MD5 / SHA256)
Image disque	E01	FTK Imager	14/09/2025	25cc6b6eb35a09acd0ab57368393521f	25cc6b6eb35a09acd0ab57368393521f

Intégrité confirmée : les empreintes sont identiques.

5. Méthodologie

- Analyse de l'image disque avec FTK Imager
- Vérification des logs (syslog, auth.log, apt.log)
- Inspection des fichiers web (/var/www/html)
- Analyse des tâches cron et scripts de démarrage
- Détection de persistance et de techniques d'évasion
- Corrélation des événements et reconstruction du vecteur d'attaque

6. Résultats de l'analyse

6.1 Attaques identifiées

Type d'attaque	Description
Phishing	Lien malveillant vers **https://bit.ly/byobu-tips** redirigeant vers un script frauduleux **(/user/bin/byobu-shell**)
Webshell	**shell.php** : variante de p0wny shell permettant exécution de commandes à distance **(/ var/www/html/hackable**)
Command Injection	Via **low.php** dans DVWA : injection directe dans une commande système **(/var/www/html/dvwa/vulnerabilities/exec/**)
Upload malveillant	**Uploader.php** : permet l'envoi de fichiers malveillants sur le serveur **(/var/www/html/dvwa/vulnerabilities/exec**/)
Persistance	Tâche cron suspecte exécutant **/usr/lib/php/sessionclean** hors contexte système

6.2 Malware et artefacts

Fichier	Type	Fonction
shell.php	Webshell	Contrôle à distance via navigateur
Mysql web shell.php	Webshell	Interface SQL malveillante
byobu-shell	Script	Téléchargement via lien frauduleux
low.php	Injection	Exécution de commandes système
Uploader.php	Upload	Téléversement de fichiers malveillants

7. Frise chronologique

Date	Événement
28/05/2024	Déploiement de DVWA vulnérable
01/06/2024	Accès initial via injection de commande
03/06/2024	Téléversement de shell.php
06/06/2024	Défiguration du site web
07/06/2024	Exfiltration de données via sessions réseau
15/09/2025	Début de l'analyse forensic
23/09/2025	Fin de l'analyse et rédaction du rapport

8. Recommandations

Actions immédiates

- Isolement du serveur shop
- Révocation des accès root et audit des utilisateurs
- Suppression des fichiers malveillants et tâches cron suspectes

Court terme

- Réinstallation propre du serveur avec durcissement
- Mise en place d'un WAF (Web Application Firewall)
- Surveillance réseau renforcée (IDS/IPS)

Long terme

- Formation des développeurs sur la sécurité applicative
- Tests réguliers de vulnérabilité (Pentest)
- Implémentation de journaux centralisés et corrélation automatique

9. Conclusion

Le serveur **shop.example.org** a été compromis via une série d'attaques ciblant des vulnérabilités connues dans **DVWA**. L'attaquant a utilisé une webshell avancée pour maintenir un accès persistant et exfiltrer des données. L'analyse a permis d'identifier les vecteurs d'attaque, les artefacts malveillants et les techniques d'évasion. Des mesures correctives et préventives sont proposées pour renforcer la sécurité du système.

10. Annexes

Logs système analysés

Les journaux suivants ont été extraits et examinés pour identifier les traces d'activités suspectes, les connexions non autorisées et les tentatives de persistance :

- `/var/log/syslog` : journal principal du système
- `/var/log/auth.log` : journal d'authentification (connexions SSH, sudo, etc.)
- `/var/log/apt/history.log` : historique des installations et mises à jour de paquets
- `/var/log/cron.log` : exécution des tâches planifiées
- `/var/log/apache2/access.log` et `error.log` : accès au serveur web et erreurs HTTP

Liste des fichiers malveillants identifiés

Fichier	Chemin	Type	Fonction
shell.php	/var/www/html/hackable/	Webshell	Exécution de commandes à distance via HTTP
Mysql web shell.php	/var/www/html/hackable/	Webshell SQL	Interface malveillante pour requêtes SQL
byobu-shell	/usr/bin/byobu-shell	Script	Téléchargé via lien frauduleux (bit.ly/byobu-tips)
low.php	/var/www/html/dvwa/vulnerabilities/exec/	Injection	Permet l'exécution de commandes système
Uploader.php	/var/www/html/dvwa/vulnerabilities/exec/	Upload	Téléversement de fichiers malveillants