

Lab 01 - Cybersecurity 3

Analyse Forensique d'un poste Windows compromis

Rapport d'Analyse Forensique

Référence : RF-2026-047 Auteur : Gauvain BOICHÉ Date du rapport : 3 août 2026 Objet : Analyse forensique suite à suspicion d'intrusion sur un poste utilisateur

0. Mise en place (partie hors-rapport, explication de l'élève au correcteur)

Afin de reproduire l'environnement d'analyse attendu, et en raison de l'indisponibilité de l'image Docker Sleuthkit originellement prévue, un environnement containerisé sur mesure a été déployé.

Préparation du répertoire de travail et copie de l'image disque brute :

```
mkdir -p ./cyberlab/data
cp .\L01-ntfs1-gen2.E01 .\cyberlab\data\
cd .\cyberlab\
```

Création d'un `Dockerfile` basé sur Ubuntu 22.04 intégrant les outils forensiques nécessaires (Sleuth Kit, outils EWF et Autopsy) :

```
FROM ubuntu:22.04

ENV DEBIAN_FRONTEND=noninteractive

RUN apt-get update && apt-get install -y \
    sleuthkit \
    ewf-tools \
    autopsy \
    kpartx \
    python3 \
    && rm -rf /var/lib/apt/lists/*

WORKDIR /data

CMD ["bash"]
```

Configuration du fichier de déploiement `docker-compose.yml` avec l'attribution des privilèges permettant le montage de systèmes de fichiers virtuels FUSE (partie générée à l'aide de l'IA Gemini 3.6 Raisonnement) :

```
version: "3.8"

services:
  forensic-lab:
    build: .
    container_name: forensic_lab
    volumes:
      - ./data:/data
    devices:
      - "/dev/fuse:/dev/fuse"
    cap_add:
      - SYS_ADMIN
    security_opt:
      - apparmor:unconfined
    stdin_open: true
    tty: true
```

Lancement du conteneur et connexion au terminal de l'environnement d'analyse :

```
docker compose up -d --build
docker exec -it forensic_lab bash
```

Création du point de montage et chargement de l'image disque cible (.E01) via l'utilitaire ewfmount :

```
mkdir -p /mnt/ewf
ewfmount /data/L01-ntfs1-gen2.E01 /mnt/ewf
```

1. Contexte de l’investigation

Le 2 août 2026 à 9h45, le SOC (Security Operation Center) a détecté une activité anormale sur le poste utilisateur WIN-DEV-07, appartenant à un développeur de l'équipe R&D. L'alerte provenait de l'EDR SentinelOne, signalant l'exécution d'un binaire suspect non reconnu par l'utilisateur légitime. Les présentes investigations visent à éclaircir la nature de cette compromission.

2. Objectifs de l’analyse

- Confirmer ou infirmer la compromission effective du poste de travail.
- Identifier avec certitude les vecteurs d’attaque et le point d’entrée initial.
- Déterminer l’étendue et le périmètre exact de l’intrusion sur le système de fichiers.
- Relever la présence d’éventuels artefacts de persistance, de tentatives d'escalade de privilèges ou d'indicateurs de mouvements latéraux.
- Formuler des mesures correctives et des préconisations de durcissement.

3. Méthodologie

Afin de mener à bien ces investigations, une chaîne de traitement logicielle spécialisée a été mobilisée. Les outils suivants ont été principalement utilisés :

Outil	Utilisation principale
Sleuth Kit (CLI)	Extraction d'artefacts, génération de timelines (MACB) et exploration du système de fichiers brut.
Autopsy	Analyse graphique du disque (.E01) et corrélation visuelle des preuves.
EWF-Tools	Montage et interaction native avec les formats d'image forensique EnCase (.E01).

(Note : Volatility, FTK Imager et Wireshark, bien que pertinents dans une analyse globale, n'ont pas été sollicités dans ce rapport centré exclusivement sur l'analyse statique d'un système de fichiers).

4. Sources analysées

4.1. Structure du volume disque

La première phase de l'investigation a consisté à interroger les métadonnées globales du système de fichiers afin d'en comprendre l'architecture et les spécificités via la commande `fsstat`. Le volume analysé est de type NTFS (Windows XP).

```
fsstat /mnt/ewf/ewf1
FILE SYSTEM INFORMATION
-----
File System Type: NTFS
Volume Serial Number: DA5048E85048CCC7
OEM Name: NTFS
Volume Name: NTFS1
Version: Windows XP

METADATA INFORMATION
-----
First Cluster of MFT: 336298
First Cluster of MFT Mirror: 504447
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 96
Root Directory: 5
```

CONTENT INFORMATION

```
-----
Sector Size: 512
Cluster Size: 512
Total Cluster Range: 0 - 1008894
Total Sector Range: 0 - 1008894
```

```
$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)  Size: 48-72  Flags: Resident
$ATTRIBUTE_LIST (32)        Size: No Limit  Flags: Non-resident
$FILE_NAME (48)             Size: 68-578  Flags: Resident,Index
$OBJECT_ID (64)             Size: 0-256    Flags: Resident
$SECURITY_DESCRIPTOR (80)    Size: No Limit  Flags: Non-resident
$VOLUME_NAME (96)           Size: 2-256    Flags: Resident
$VOLUME_INFORMATION (112)    Size: 12-12    Flags: Resident
$DATA (128)                 Size: No Limit  Flags:
$INDEX_ROOT (144)           Size: No Limit  Flags: Resident
$INDEX_ALLOCATION (160)       Size: No Limit  Flags: Non-resident
$BITMAP (176)               Size: No Limit  Flags: Non-resident
$REPARSE_POINT (192)         Size: 0-16384  Flags: Non-resident
$EA_INFORMATION (208)        Size: 8-8      Flags: Resident
$EA (224)                   Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256) Size: 0-65536   Flags: Non-resident
```

4.2. Analyse de l'arborescence à la racine du volume

Le parcours de la racine du système de fichiers (**fls**) a immédiatement mis en évidence une structure inhabituelle. Plutôt qu'une arborescence système classique, le volume semble dédié au stockage de données protégées, avec la présence de dossiers spécifiques (RAW, Compressed, Encrypted) et de plusieurs certificats liés à la technologie EFS (Encrypting File System) stockés en clair.

```
fls -o 0 /mnt/ewf/ewf1
r/r 4-128-4:  $AttrDef
r/r 8-128-2:  $BadClus
r/r 8-128-1:  $BadClus:$Bad
r/r 6-128-1:  $Bitmap
r/r 7-128-1:  $Boot
d/d 11-144-4: $Extend
r/r 2-128-1:  $LogFile
r/r 0-128-1:  $MFT
r/r 1-128-1:  $MFTMirr
r/r 9-128-8:  $Secure:$SDS
r/r 9-144-11: $Secure:$SDH
r/r 9-144-5:  $Secure:$SII
r/r 10-128-1: $UpCase
r/r 3-128-3:  $Volume
d/d 28-144-8: Compressed
r/r 46-128-1: EFS-key-info.txt
r/r 43-128-4: EFS-key-no-password.pfx
r/r 45-128-4: EFS-key-password-strong-protection.pfx
r/r 44-128-4: EFS-key-password.pfx
d/d 29-144-10: Encrypted
d/d 27-144-7: RAW
d/d 30-144-1: System Volume Information
V/V 96: $OrphanFiles
```

4.3. Extraction d'informations critiques et d'indices

La présence du fichier **EFS-key-info.txt** à la racine (inode 46) constituait une compromission potentielle majeure. Son extraction a révélé le stockage en clair du mot de passe maître permettant de déverrouiller la clé EFS.

```
icat /mnt/ewf/ewf1 46
> The password for the EFS key is "password" (no quotes).
```

Récupération des artefacts cryptographiques et vérification de l'intégrité

L'ensemble des fichiers de clés et de certificats (.pfx) présents à la racine ont été extraits vers l'environnement d'analyse. Des empreintes cryptographiques (SHA-256) ont été générées immédiatement afin de sceller ces preuves numériques.

```
icat /mnt/ewf/ewf1 46 > /data/EFS-key-info.txt
icat /mnt/ewf/ewf1 43 > /data/EFS-key-no-password.pfx
icat /mnt/ewf/ewf1 44 > /data/EFS-key-password.pfx
icat /mnt/ewf/ewf1 45 > /data/EFS-key-password-strong-protection.pfx

sha256sum /data/EFS-key*
```

Inspection de la zone de stockage chiffrée

L'inspection du dossier **Encrypted** (inode 29) a permis de lister les fichiers que l'utilisateur tentait de protéger. On y retrouve des documents de nature administrative, des normes de sécurité (NIST), et surtout, un fichier journal (**logfile1.txt**) qui pourrait contenir des traces d'activités système ou utilisateur.

```
> fls /mnt/ewf/ewf1 29
r/r 41-128-1: 20076517123273.pdf
r/r 49-128-7: logfile1.txt
r/r 35-128-1: NISTSP800-88_rev1.pdf
r/r 32-128-1: NIST_logo.jpg
r/r 38-128-1: report02-3.pdf
```

Extraction globale des preuves documentaires

L'intégralité du contenu du dossier chiffré a été extraite et hachée cryptographiquement en vue d'une analyse ultérieure et pour garantir la traçabilité des éléments versés au dossier.

```
icat /mnt/ewf/ewf1 49 > /data/logfile1.txt
icat /mnt/ewf/ewf1 41 > /data/20076517123273.pdf
icat /mnt/ewf/ewf1 35 > /data/NISTSP800-88_rev1.pdf
icat /mnt/ewf/ewf1 32 > /data/NIST_logo.jpg
icat /mnt/ewf/ewf1 38 > /data/report02-3.pdf
```

```
> sha256sum /data/*.pdf /data/*.jpg /data/*.txt /data/*.pfx
ef35e4c7ffb1befe4b605149a2dbd97e3fac67b809c387cab549a8de03c6930d /data/20076517123273.pdf
8646b073ff05f8a6c0af300b49995cabfd557d8090964eb24af042618ad54ef6 /data/NISTSP800-88_rev1.pdf
f0f97ac2e3b56e628b9f128d3972652596f340aac5834d24d8e45640221708ab /data/report02-3.pdf
5d793e1cbbbcc9ca474aa4925870b6e2018e4ecdec19dc6837b74d2bb5bb43fc /data/NIST_logo.jpg
89b04b0ed76d440379aa8914c3769c2d14e936e2d18a5de9525f6131c0298d07 /data/EFS-key-info.txt
f8a03d238825e0cce7168fec663447ec821d781837987b2ce2694b702dea9890 /data/logfile1.txt
bb939b30a08c51aee28c1d7ad1e31e8592059206cfa58a6bcd1ef3e10292943 /data/EFS-key-no-password.pfx
2d7297b6ee4708a169c3d5694b733df88f5c0ddfb98f3605452de8a602bae04d /data/EFS-key-password-strong-
protection.pfx
7c41ec33d24e704ace50d5b617100458dc2e1a12bd1b13fed46c1988d23debcc /data/EFS-key-password.pfx
```

5. Chronologie des événements

Afin de contextualiser l'apparition des clés de chiffrement et la manipulation du fichier de journalisation, une timeline globale a été générée en extrayant les métadonnées MACB (Modified, Accessed, Changed, Born) de l'ensemble du volume.

```
fls -r -m / /mnt/ewf/ewf1 > /data/bodyfile.txt
mactime -b /data/bodyfile.txt > /data/timeline.csv
```

Un filtrage ciblé sur les événements liés au système de chiffrement (**EFS**) et au journal système (**logfile**) a produit le résultat suivant :

```
> grep -e "EFS" -e "logfile" timeline.csv
Mon Jan 05 2009 21:44:06      1730 ...b r/rrwxrwxrwx 0 0 43-128-4 /EFS-key-no-password.pfx
                             112 ...b r/rrwxrwxrwx 0 0 43-48-2 /EFS-key-no-password.pfx ($FILE_NAME)
Mon Jan 05 2009 21:44:09      1730 m.c. r/rrwxrwxrwx 0 0 43-128-4 /EFS-key-no-password.pfx
                             112 mac. r/rrwxrwxrwx 0 0 43-48-2 /EFS-key-no-password.pfx ($FILE_NAME)
Mon Jan 05 2009 21:44:36      1730 .a.. r/rrwxrwxrwx 0 0 43-128-4 /EFS-key-no-password.pfx
Mon Jan 05 2009 21:44:42      1730 ...b r/rrwxrwxrwx 0 0 44-128-4 /EFS-key-password.pfx
                             106 ...b r/rrwxrwxrwx 0 0 44-48-2 /EFS-key-password.pfx ($FILE_NAME)
Mon Jan 05 2009 21:44:44      1730 mac. r/rrwxrwxrwx 0 0 44-128-4 /EFS-key-password.pfx
                             106 mac. r/rrwxrwxrwx 0 0 44-48-2 /EFS-key-password.pfx ($FILE_NAME)
Mon Jan 05 2009 21:45:10      1734 ...b r/rrwxrwxrwx 0 0 45-128-4 /EFS-key-password-strong-
protection.pfx
                             142 ...b r/rrwxrwxrwx 0 0 45-48-2 /EFS-key-password-strong-
protection.pfx ($FILE_NAME)
Mon Jan 05 2009 21:45:12      1734 mac. r/rrwxrwxrwx 0 0 45-128-4 /EFS-key-password-strong-
protection.pfx
                             142 mac. r/rrwxrwxrwx 0 0 45-48-2 /EFS-key-password-strong-
protection.pfx ($FILE_NAME)
Mon Jan 05 2009 21:45:47         57 ...b r/rrwxrwxrwx 0 0 46-128-1 /EFS-key-info.txt
                             98 ...b r/rrwxrwxrwx 0 0 46-48-2 /EFS-key-info.txt ($FILE_NAME)
Mon Jan 05 2009 21:45:48         57 m.c. r/rrwxrwxrwx 0 0 46-128-1 /EFS-key-info.txt
                             98 mac. r/rrwxrwxrwx 0 0 46-48-2 /EFS-key-info.txt ($FILE_NAME)
                             21888890 ...b r/rrwxrwxrwx 0 0 47-128-5 /RAW/logfile1.txt
                             90 macb r/rrwxrwxrwx 0 0 47-48-2 /RAW/logfile1.txt ($FILE_NAME)
                             21888890 ...b r/rrwxrwxrwx 0 0 48-128-6 /Compressed/logfile1.txt
                             90 macb r/rrwxrwxrwx 0 0 48-48-2 /Compressed/logfile1.txt ($FILE_NAME)
                             21888890 ...b r/rrwxrwxrwx 0 0 49-128-7 /Encrypted/logfile1.txt
                             90 macb r/rrwxrwxrwx 0 0 49-48-2 /Encrypted/logfile1.txt ($FILE_NAME)
Mon Jan 05 2009 22:01:23 21888890 mac. r/rrwxrwxrwx 0 0 47-128-5 /RAW/logfile1.txt
Mon Jan 05 2009 22:01:25 21888890 mac. r/rrwxrwxrwx 0 0 48-128-6 /Compressed/logfile1.txt
Mon Jan 05 2009 22:01:26 21888890 mac. r/rrwxrwxrwx 0 0 49-128-7 /Encrypted/logfile1.txt
Tue Jan 06 2009 19:44:13         57 .a.. r/rrwxrwxrwx 0 0 46-128-1 /EFS-key-info.txt
```

L'analyse détaillée de cette chronologie démontre que les actions de création et de configuration des clés de chiffrement se sont succédé très rapidement dans la soirée du **5 janvier 2009**. Le tableau ci-dessous synthétise la séquence logique des opérations :

Horodatage (UTC)	Action / Événement identifié	Fichier / Chemin concerné	Inode	Métadonnées MACB
05/01/2009 21:44:06	Création du certificat EFS vierge de protection	/EFS-key-no-password.pfx	43	...b (Born)
05/01/2009 21:44:42	Création du certificat EFS chiffré basique	/EFS-key-password.pfx	44	...b (Born)
05/01/2009 21:45:10	Création du certificat EFS à protection forte	/EFS-key-password-strong-protection.pfx	45	...b (Born)
05/01/2009 21:45:47	Génération du fichier texte d'indice contenant le secret	/EFS-key-info.txt	46	...b (Born)
05/01/2009 22:01:23	Altération du journal d'événements brut	/RAW/logfile1.txt	47	mac. (Mod/Acc/Chg)
05/01/2009 22:01:25	Opération de compression appliquée sur le journal	/Compressed/logfile1.txt	48	mac. (Mod/Acc/Chg)
05/01/2009 22:01:26	Chiffrement effectif et enregistrement du journal protégé	/Encrypted/logfile1.txt	49	mac. (Mod/Acc/Chg)
06/01/2009 19:44:13	Preuve de lecture du fichier contenant le secret	/EFS-key-info.txt	46	.a.. (Accessed)

6. Indicateurs de compromission (IoC) & Faiblesses structurelles

6.1. Fichiers clés et certificats EFS identifiés

L'investigation a permis d'isoler plusieurs artefacts cryptographiques dont la simple présence constitue une vulnérabilité sévère :

Nom du fichier	Hash SHA256	Emplacement	Inode	Description
EFS-key-info.txt	89b04b0ed76d440379aa8914c3769c2d14e936e2d18a5de9525f6131c0298d07	/	46	Fichier contenant le secret en clair.
EFS-key-no-password.pfx	bb939b30a08c51aee28c1d7ad1e31e8592059206cfa58a6bcd1ef3e10292943	/	43	Certificat EFS exporté sans protection par mot de passe.
EFS-key-password.pfx	7c41ec33d24e704ace50d5b617100458dc2e1a12bd1b13fed46c1988d23debcc	/	44	Clé EFS (protégée par le mot de passe trivial "password").
EFS-key-password-strong-protection.pfx	2d7297b6ee4708a169c3d5694b733df88f5c0ddfb98f3605452de8a602bae04d	/	45	Clé EFS implémentant une protection renforcée.
logfile1.txt	f8a03d238825e0cce7168fec663447ec821d781837987b2ce2694b702dea9890	/Encrypted/	49	Fichier de journalisation volumineux (~21.8 MB).

6.2. Manquements aux politiques de sécurité relevés

L'analyse forensique met en exergue des défaillances critiques dans l'hygiène de sécurité du système :

- **Stockage de secrets en texte clair** : La présence du fichier `EFS-key-info.txt` à la racine rend la compromission immédiate et triviale pour tout attaquant accédant au volume.
- **Complexité des mots de passe inexistante** : Le verrouillage d'un conteneur cryptographique (`.pfx`) avec la chaîne de caractères "password" annule toute l'efficacité du mécanisme de protection.
- **Exposition injustifiée de matériel cryptographique privé** : Les certificats et clés d'agent de récupération EFS n'ont pas vocation à être stockés sur la racine d'un volume système accessible.

7. Évaluation de la compromission

L'état des lieux du système de fichiers dresse un bilan alarmant quant à la confidentialité des données hébergées.

Élément	Présence / Statut	Commentaire analytique
Stockage illégal de clés de chiffrement	Confirmé	Le matériel cryptographique privé est librement accessible à la racine.
Exposition volontaire de mots de passe	Confirmé	Le secret d'accès a été délibérément documenté dans <code>EFS-key-info.txt</code> .
Absence de protection sur les certificats	Confirmé	Le fichier <code>EFS-key-no-password.pfx</code> a été extrait et peut être importé sans restriction.
Analyse du cycle de vie des données (RAW > Compressed > Encrypted)	Confirmé	La timeline démontre une tentative de dissimulation et de traitement de logs confidentiels avant leur chiffrement.

Conclusion de l'investigation : Bien que les éléments analysés ne démontrent pas formellement l'exécution d'un code malveillant distant, le système souffre d'un défaut de conception critique. La mauvaise gestion du chiffrement EFS a induit un état de compromission permanent : tout individu (ou processus) disposant de droits de lecture sur le volume était en mesure d'usurper les clés privées et de déchiffrer l'ensemble du contenu du répertoire `/Encrypted`.

8. Préconisations de remédiation

Suite aux conclusions de cette analyse, les mesures suivantes doivent être appliquées afin de restaurer l'intégrité de l'environnement de travail :

Court terme (Immédiat)

- Procéder à la suppression sécurisée des certificats et clés de chiffrement (.pfx) actuellement stockés en clair sur la racine des volumes.
- Engager une procédure de révocation pour les clés EFS compromises (EFS-key-no-password.pfx et EFS-key-password.pfx).
- Détruire le fichier compromettant EFS-key-info.txt (purge des secteurs associés).

Moyen terme

- Appliquer informatiquement une politique de robustesse de mot de passe lors de la génération ou de l'exportation de clés PKCS#12 et EFS.
- Implémenter une solution de gestion des secrets centralisée (ex: HashiCorp Vault, KeepassXC) pour proscrire définitivement le stockage de mots de passe dans des fichiers textes locaux.
- Réviser les permissions d'accès (ACLs NTFS) sur la racine des disques et les dossiers sensibles afin d'appliquer le principe du moindre privilège.

Long terme

- Intégrer la gestion du cycle de vie des certificats et des agents de récupération EFS directement via les services de domaine Active Directory (PKI d'entreprise et stratégies de groupe GPO).
- Organiser une campagne de sensibilisation ciblée envers les équipes techniques et de développement sur les risques associés au stockage de matériel cryptographique et de secrets en clair.

9. Annexes

Annexe 1 : Extrait du registre des preuves (preuves.csv)

Le fichier complet preuves.csv a été joint au présent rapport. Il consigne l'ensemble des artefacts extraits selon le format exigé :

```
Type de fichier,Horodatage,Chemin,Hash SHA256,Raison du marquage
Texte Indice,2009-01-05 21:45:47 UTC,/EFS-key-info.txt,89b04b0ed76d440379aa8914c3769c2d14e936e2d18a5de9525f6131c0298d07,Contient le mot de passe de chiffrement en clair
Certificat PFX,2009-01-05 21:44:06 UTC,/EFS-key-no-password.pfx,bb939b30a08c51aee28c1d7ad1e31e8592059206cfa58a6bcd1ef3e10292943,Clé EFS privée sans mot de passe
Certificat PFX,2009-01-05 21:44:42 UTC,/EFS-key-password.pfx,7c41ec33d24e704ace50d5b617100458dc2e1a12bd1b13fed46c1988d23debcc,Clé EFS protégée par un mot de passe faible
Certificat PFX,2009-01-05 21:45:10 UTC,/EFS-key-password-strong-protection.pfx,2d7297b6ee4708a169c3d5694b733df88f5c0ddfb98f3605452de8a602bae04d,Clé EFS à protection forte
Fichier Log,2009-01-05 22:01:26 UTC,/Encrypted/logfile1.txt,f8a03d238825e0cce7168fec663447ec821d781837987b2ce2694b702dea9890,Fichier de log volumineux stocké en zone chiffrée
Document PDF,2009-01-05 21:45:00 UTC,/Encrypted/20076517123273.pdf,ef35e4c7fffb1befe4b605149a2dbd97e3fac67b809c387cab549a8de03c6930d,Document extrait du dossier chiffré
Document PDF,2009-01-05 21:45:00 UTC,/Encrypted/NISTSP800-88_rev1.pdf,8646b073ff05f8a6c0af300b49995cabfd557d8090964eb24af042618ad54ef6,Document NIST sur la destruction sécurisée de données
Document PDF,2009-01-05 21:45:00 UTC,/Encrypted/report02-3.pdf,f0f97ac2e3b56e628b9f128d3972652596f340aac5834d24d8e45640221708ab,Rapport d'analyse extrait du dossier chiffré
Image JPG,2009-01-05 21:45:00 UTC,/Encrypted/NIST_logo.jpg,5d793e1cbbbcc9ca474aa4925870b6e2018e4ecdec19dc6837b74d2bb5bb43fc,Logo NIST extrait de la zone chiffrée
```