

Lab 01

Cybersecurity 3

Analyse Forensique d'un poste Windows compromis

Objectifs :

- Monter et analyser une image disque .E01 dans un environnement containerisé
- Identifier les artefacts de compromission
- Construire une timeline d'événements avec The Sleuth Kit
- Documenter les preuves dans un rapport forensique

Environnement & Matériel

Docker Containers Utilisés :

- sleuthkit/tsk: Pour les outils fls, icat, mactime, etc.
- log2timeline/plaso: Pour enrichir l'analyse temporelle si souhaité
- autopsy/autopsy: GUI web dans un container, pour ceux préférant l'interface graphique
- (Optionnel) ubuntu/forensic-tools: image personnalisée avec CAINE-like tools

Fichier source :

- ntfs1-gen2.E01 : image disque compromis

Etape :1. Préparation de l'environnement

a. Récupérer les fichiers

```
mkdir -p ~/cyberlab/data
```

```
cp ntfs1-gen2.E01 ~/cyberlab/data/
```

```
cd ~/cyberlab
```

b. Docker Compose (si GUI souhaitée avec Autopsy)

```
# docker-compose.yml
version: "3.8"

services:
  sleuthkit:
    image: sleuthkit/tsk

    volumes:
      - ./data:/data

    stdin_open: true
    tty: true

  autopsy:
    image: fkiercad/autopsy

    ports:
      - "9999:9999"

    volumes:
      - ./data:/data
```

Lancer :

```
docker compose up -d
```

Etape 2. Analyse initiale

a. Monter l'image .E01 avec ewfmount (via container TSK)

```
docker run -it --rm -v $(pwd)/data:/data sleuthkit/tsk bash
```

Dans le container :

```
ewfmount /data/ewf1.E01 /mnt/ewf
```

b. Identifier les infos système

```
fsstat /mnt/ewf/ewf1.raw
```

c. Identifier l'utilisateur principal :

Rechercher dans Users/ ou via fls :

```
fls -r -m /mnt/ewf/ewf1.raw > /data/bodyfile.txt
```

Etape 3. Analyse des artefacts

- Fichiers récents :

`icat /mnt/ewf/ewfl.raw <inode>`

- Dossiers à inspecter :
 - Identifier les dossiers nécessaire a l'inspection pour identification
- Applications installées :
 - Vérifier si des applications « anormales » ont été installé

Etapes 4. Construction de la timeline

a. Extraire les métadonnées

`fls -r -m /mnt/ewf/ewfl.raw > /data/bodyfile.txt`

b. Créer la timeline avec mactime

`mactime -b /data/bodyfile.txt > /data/timeline.csv`

Option : utiliser log2timeline pour enrichir (Plaso)

Etapes 5. Interprétation

- Point d'entrée : EXE douteux, autorun, clé de registre modifiée ?
- Activités suspectes : accès réseau, exfiltration, programmes en autostart ?
- Corrélation des événements via la timeline ?

Livrables attendus

1. Rapport forensique en PDF

- Résumé des faits et contexte
- Timeline des événements clés
- Indicateurs de compromission (hashs, chemins, timestamps)
- Screenshots des outils (via Autopsy ou console)
- Conclusion et recommandations

2. Fichier de preuves (.csv)

- Dérivé de la timeline
- Colonnes : Type de fichier, Horodatage, Chemin, Hash SHA256, Raison du marquage