

Lab 05

Cybersecurity 3

Analyse de Mémoire Vive avec Volatility

Objectifs

- Utiliser Volatility pour analyser un dump RAM
- Identifier processus malveillants, injections, rootkits
- Extraire et examiner chaînes de caractères, exécutable, artefacts réseaux

Environnement et Matériel

Docker Image utilisée :

- teamtnt/volatility – contient Volatility 2
- Option : [volatilityfoundation/volatility3](https://github.com/volatilityfoundation/volatility3) (avec adaptation des commandes)

Fichier de travail :

- zeus.vmem (dump mémoire infecté par Zeus, malware bancaire)
- Source directe :
 <https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples>
 Lien direct (Zeus.vmem, 75 MB) :
<https://downloads.volatilityfoundation.org/memory-samples/zeus.vmem.zip>

Etape 1. Préparation de l'environnement Docker

a. Récupération des fichiers

```
mkdir -p ~/memlab/data
```

```
cd ~/memlab/data
```

```
wget https://downloads.volatilityfoundation.org/memory-samples/zeus.vmem.zip
```

```
unzip zeus.vmem.zip
```

b. Lancer Volatility via Docker

```
docker run -it --rm -v $(pwd):/data teamtnt/volatility bash
```

Etape 2. Identification de l'image mémoire

```
volatility -f /data/zeus.vmem imageinfo
```

Cela permet de repérer le bon profil à utiliser (WinXPSP2x86)

Etape 3. Inspection des processus

```
volatility -f /data/zeus.vmem --profile=WinXPSP2x86 pslist
```

```
volatility -f /data/zeus.vmem --profile=WinXPSP2x86 pstree
```

```
volatility -f /data/zeus.vmem --profile=WinXPSP2x86 psscan
```

Chercher :

- Processus sans parent logique
- Anomalies de noms
- PID élevés, noms suspects (svchost.exe, etc.)

Etape 4. Analyse réseau

```
volatility -f /data/zeus.vmem --profile=WinXPSP2x86 netscan
```

Vérifie :

- Connexions actives
- Ports ouverts
- Destinataires IP externes

Etape 5. Analyse de DLL & injections

```
volatility -f /data/zeus.vmem --profile=WinXPSP2x86 malfind
```

```
volatility -f /data/zeus.vmem --profile=WinXPSP2x86 ldrmodules
```

```
volatility -f /data/zeus.vmem --profile=WinXPSP2x86 dlllist
```

Dump de la mémoire d'un processus suspect :

```
mkdir -p /data/dump
```

```
volatility -f /data/zeus.vmem --profile=WinXPSP2x86 memdump -p <pid> -D /data/dump/
```

Etape 6. Extraction & investigation manuelle

```
strings /data/dump/<pid>.dmp | grep -Ei "http|powershell|token|cmd|exe"
```

```
file /data/dump/<pid>.dmp
```

```
md5sum /data/dump/<pid>.dmp
```

Cela permet d'identifier :

- URLs de C2
- Payloads
- Scripts PowerShell embarqués

Livrables attendus

Rapport d'analyse mémoire (.pdf)

Contenu attendu :

- Identification du profil et méthodologie
- Résultats des commandes Volatility
- Screenshots (console)
- Analyse de chaque processus suspect
- Connexions réseau identifiées
- Conclusion : infection confirmée ? Quel vecteur ?