Live forensics

Mars 2023

Lors d’une réponse à incidents

La collecte d’information pour analyse se heurte à certaines contraintes:

- La machine peut se trouver sur un autre continent
- Sans personne « technique » pour collecter les données
- La machine en question peut elle être éteinte ou il faut isoler la machine le plus vite possible ?
- Un simple laptop possède aujourd’hui 16Go de RAM et 300 à 500Go de disque dur

Compromis

- Entre temps de collecte et le nombre de données collectées
- Entre taille totale des données collectées et le nombre de données collectées
- Quelles données récupérer en priorité selon la situation ?

Collecte minimale

Utilisateurs, groupes et privilèges

Informations processus, services et réseau:

- Interfaces, adresses IP, connections ouvertes, routage et services réseaux. Caches ARP et DNS/NetBIOS.
  Ports ouverts et en écoute. Etat du pare-feu

Liste de tâches planifiées ou au démarrage

Liste des pilotes, des DLLs non signées (Windows)

Journaux de sécurité, système et applicatifs

Liste des fichiers et répertoires avec les droits

MBR, MFT, Base de registre (Windows)

Empreinte mémoire RAM

Exemple de script (v0.1)

```
REM capture date and time
date /t
time /t

REM system version and variables
ver
systeminfo
set

REM tasks, processes and startup items
tasklist /svc
schtasks
wmic startup list full
wmic process list full

REM drivers
driverquery
driverquery /SI

REM registry
start /w regedit /e %systemroot%\local_machine.txt "HKEY_LOCAL_MACHINE"
REM HKEY_CLASSES_ROOT
REM HKEY_CURRENT_USER
REM HKEY_USERS
REM HKEY_CURRENT_CONFIG
REM files, folders and attr
tree /F /A %systemroot%
wmic fsdir where name="c:\\system32"
wmic datafile where name="c:\\boot.ini"

REM local users accounts and groups
net user
net localgroup

REM sessions, shares, mapped drives
net session
net share
net use

REM windows services
net start
sc query
sc queryex state= all

REM networking
ipconfig /all
netsh int ip show config

REM client DNS cache
ipconfig /displaydns

REM hosts file
Type %systemroot%\system32\drivers\etc\hosts

REM netbios name cache
nbtstat -c

REM ARP table
arp -a

REM routing table
route print
netstat -r

REM windows firewall
netsh firewall show state
netsh advfirewall show allprofiles

REM network connections
netstat -nao
netstat -naob
```

Collecte avancée

MFT et Base de Registre

avec RawCopy

Hashs des fichiers systèmes (coûteux en CPU et temps!)

Empreinte mémoire

- avec DumpIt (MoonSols)
- ou FTK Lite Imager
- LiME et son profil (Linux)

Si l’on veut une analyse en profondeur: collecte de la partition système (et /home sous Linux)

- avec FTK Lite Imager
- ou DD

Analyse locale ou centralisée ?

L'analyse (syntaxique) locale peut permettre de réduire la taille des données collectées.

- Pour la MFT par exemple.
- Quels formats de sortie ? Veiller à l'interopérabilité avec les outils
- Et si l'on découvre de nouveaux artefacts dont la syntaxe n'était pas connu à l'époque de la collecte?

La recherche d'indice de compromission (IOC) en local peut distribuer le coût CPU, mais peut dévoiler à l'intrus notre connaissance sur la compromission recherchée

Conclusion:

- Collection en priorité de données brutes et recherche d'IOC « à l'abri »

DFIR-ORC

Outil de collecte Live

https://github.com/dfir-orc

Par l'ANSSI

« Exécutable valise » embarquant d'autres outils et sa configuration xml

https://www.ssi.gouv.fr/actualite/decouvrez-dfir-orc-un-outil-de-collecte-libre-pour-lanalyse-forensique/

Les EDR