Synthèse théorique
Forensics

Troisième Bloc
Sécurité des systèmes
Année académique 2021-2022

Rédigé par Sénéchal Julien

04 Janvier 2022

Table des matières

1 Termes et définitions

- CSIRT :
  Computer Security Incident Response Team = équipe qui s'occupe de la CSIRC.

- CSIRC :
  Computer Security Incident Response Capability = Politique de réponse aux incident.

- Computer security Incident :
  Violation des règles de sécurité ou des règles de sécurité standard.

- Digital Forensics :
  Permet de récupérer des données sous certaines conditions strictes afin de pouvoir les utiliser comme preuve légale de la même manière qu'une preuve physique (peut avoir lieu lors d'un crime hors que la cybercriminalité).

- DFIR :
  Digital Forenscis and Incident Response = Equipe qui regroupe la CSIRT et l'équipe forensics.

- SOC : Security Operation Center

- SIEM : Security Information and Event Management

- BCDR :
  Business continuity and disaster recovery = S'occupe de la mise en place de la stratégie de restauration.

- Imaging vs Copying :
  - Copying : Ne permet pas de récupérer les fichiers cachés, supprimés, les metadatas etc.
  - Imaging : On conserve chaque bit du disque/partition.
- Dead Imaging :
  Récupération de l'image depuis la machine forensic.
- Lvie Imaging :
  Récupération de l'image depuis un système qui tourne toujours.

2 Incident Response Process

2.1 Préparation

- Former une équipe DFIR
- Mettre en place des procédures
- Préparer un laboratoires (des machines etc.) pour le travail forensique
- Exercice régulier
- Sécurisation de l'infrastrucutre

2.2 Détection

- Les outils de SIEM permettent de détecter des comportements anormaux :
  SolarWind, Splunk, Qradar, ...
- IDS, antivirus, monitoring de logs, vérification de l'intégrité des fichiers peuvent compléter le SIEM
- La détection peut provenir de l'extérieur (ex : ISP, antivirus, agences, etc.)
- Souvent découvert par l'utilisateur
- Signes précurseurs :
  Entrée de logs qui montrent l'utilisation d'un scanneur de vulnérabilités, une annonce d'une nouvelle CVE, menace d'un groupe de hacker...

2.3 Analyse

- Retrouver la source de l'incident et toutes ses traces
- Doit respecter des règles en cas d'utilisation d'éventuelles preuves pour des démarches judiciaires
- Beaucoup d'outils (autopsy, FTKImager, ...)

2.4 Endiguement

- Isoler les machines infectées :
  Peut être dangereux car certains malware détectent la mise en quarantaine et profitent pour chiffrer toutes les machines infectées
- Dépend fortement du type de menace détecté et de l'infrastructure à protéger

2.5 Éradication et récupération

- Supprimer la menace et restaurer le système
- Patcher les vulnérabilités
- La stratégie de restauration du système appartient au BCDR

2.6 Post-incident

- Regrouper toutes les informations des étapes précédentes et faire un rapport (peut être fait à l'aide d'une main courante).

3 Mise en place d'un CSIRT

1. Création d'une charte avec ces divers points :
   - Accord écrit de la direction
   - Définir le périmètre que couvre l'équipe
   - Définir la mission du CSIRT
   - Services fournis par le CSIRT (formation, test d'outils, détection, analyse, etc.)
2. Recruter dans la team :
   - Coordinateur (**peut** être le CISO)
   - Analyste CSIRT (collecte et analyse les informations utiles)
   - Personne dédiée au service SOC (Point de contact entre le SOC et la CSIRT)
   - Ingénieur Sécurité IT (responsables des outils, mise en place d'un environnement de prise en charge d'une IR)

4 Digital Forensic Process

4.1 Identification

Tracer l'attaque et identifiant les différents élément qu'elle a laissé derrière elle. Une fois les preuves réunies :

- Isoler la preuve
- Empêcher la modification des logs
- Plus de communication réseaux (sac de faraday pour un téléphone par exemple)
- Faire des snapshots si possible
- Protéger les preuves physiquement
- Si donnée volatile, faire attention à laisser l'appareil sous tension

4.2 Collection

Récupérer les données nécessaires à l'enquête de manière délicate pour s'assurer que les données seront recevable en justice. De plus, certaines de ces données sont volatiles (cache, registre, RAM, fichier tmp,...).

- Les preuves ne doivent pas être altérer (importance du hash)
- Le processus doit être documenté
- Chain of custody :
  - Formulaire à maintenir à jour pour chaque preuve.
  - Permet de garder une histoire du cycle de vie de la preuve

4.3 Examination

Extraire l'information pertinente de la preuve.

4.4 Analyse

Corrélation des différentes données afin de tirer des conclusions

4.5 Présentation

Rédaction d'un rapport :

- Résumé des étapes
- Mise en évidences des données critiques saisies
- Objectif
- Doit identifier la source de l'incident

5 Imager de la mémoire non-volatile

5.1 Préparation

- S'assurer qu'il n'y aie plus rien sur le disque hôte (ex outil : eraser)
- S'assurer que le disque cible soit bloqué en read-only (travail des write-blocker qui peuvent être software et hardware)

5.2 Imaging

Différents outils :

- Sous Linux : Guymager, dc3dd, Paladin, etc.
- Sous Windows : FTK

5.3 Analyse

- Autopsy
- Permet de gagner beaucoup de temps dans l'analyse

6 Imager de la mémoire volatile

6.1 Acquisition

Linux :

— LIME : Permet de créer une image de la mémoire vive (possibilité de faire un hash)

Windows :

— FTK imager

— BelkaSoft RAM Capturer

Limites de l'acquisition :

— Machine toujours allumée

— Accès au compte admin necéssaire

— Peut faire planter la machine

Avantages :

— Offre des informations complémentaires sur l'état d'execution de la machine (processus, kernel, réseaux, ...)

Dans le cas d'une équipe DFIR, il existe F-Response qui va mettre un agent sur les machines, rendant facile la récupération d'une image disque et de la mémoire à distance.

6.2 Analyse

— Volatility

  — Création d'un profil nécessaire pour les machines sous Linux

7 Spécificités de la mémoire flash

- Pas d'overwrite, il faut donc supprimer le contenu avant d'écrire
- Suppression par bloc
- Nombre limité d'accès en écriture
- SATA TRIM :
  - Commande faite par l'OS pour signaler les emplacements à effacer (dans le but d'améliorer la performance car pas besoin de supprimer avant d'écrire car déjà fait)
  - Problème pour l'analyse Forensics et pour le hash d'une image disque
  - Montre l'importance de bloquer l'écriture pendant la collecte d'informations