

Implémentation d'un IDS basé sur les signatures à l'aide de Suricata

1. Préparer la liste des hashes de Ransomware

On utilise la plateforme **MalwareBazaar**, c'est un service en ligne gratuit développé par **Abuse.ch**. Il s'agit d'une plateforme qui centralise les échantillons de malwares (fichiers malveillants) pour aider les chercheurs en cybersécurité, les professionnels de la sécurité et les analystes à étudier, détecter et contrer les cybermenaces. Ses principales caractéristiques :

- **Répertoire de malwares**
MalwareBazaar permet aux utilisateurs de soumettre et de télécharger des échantillons de malwares, tels que des exécutables Windows, des documents infectés ou des fichiers associés à des familles de ransomwares.
- **Classification par famille de malwares**
Les échantillons sont catégorisés par type de malware (ransomware, botnet, trojan, etc.) et par famille spécifique (par exemple : **LockBit**, **Emotet**, **TrickBot**).
- **Hashes et métadonnées**
Chaque fichier malveillant est accompagné de plusieurs informations :
 - Hashes (MD5, SHA1, SHA256).
 - Famille ou catégorie.
 - Nom du fichier et type (exécutable, document, etc.).
 - Date de soumission.
- **Téléchargement sécurisé**
Les fichiers sont disponibles pour téléchargement dans un environnement contrôlé, mais nécessitent un compte pour éviter une mauvaise utilisation.
- **Intégration avec des outils de sécurité**
 - MalwareBazaar propose des **APIs** pour automatiser la récupération d'informations et d'échantillons.
 - Les données peuvent être intégrées dans des systèmes de détection comme des IDS (Intrusion Detection Systems) ou des solutions SIEM (Security Information and Event Management).
- **Recherche avancée**
Les utilisateurs peuvent rechercher des échantillons via :
 - Le nom du malware ou de sa famille.
 - Des mots-clés ou tags (ex. : "ransomware").
 - Des hashes spécifiques.

on extrait les MD5 hashes des ransomware à partir de la plateforme :

Plain text files

The following data exports exists in plain text format:

- SHA256 hashes: Recent additions ([download](#))
- SHA256 hashes: Full data dump ([download](#) - zip compressed)
- MD5 hashes: Recent additions ([download](#))
- MD5 hashes: Full data dump ([download](#) - zip compressed)
- SHA1 hashes: Recent additions ([download](#))
- SHA1 hashes: Full data dump ([download](#) - zip compressed)

On sauvegarde le fichier sous nom : **hashes.txt**

```
1 #####
2 # MalwareBazaar full malware samples dump (MD5 hashes) #
3 # Last updated: 2024-11-08 20:39:35 UTC #
4 # #
5 # Terms Of Use: https://bazaar.abuse.ch/faq/#tos #
6 # For questions please contact bazaar [at] abuse.ch #
7 #####
8 #
9 # md5_hash
10 f6ec1671cbe2aea689a7bfcc3ba9f7b3
11 cd45ab127a5ad0327cadffb89238cb09
12 bdc6432b365c256c5d0efe8d66122e8f
13 c1b2e76883510b828947e99b9a74f618
14 a32bc0032323cd52755394c24d79fa86
15 2cf1757ffddf7be24efa99c137d5fdf6
16 ad8a3ff974e2f2eac64acfb7ae8dd30c
17 27ca3e985916dfc28bd8095903cf21ba
18 399d3cb161c65b7cfa1412af587747ad
19 8fca666ce48bed2b7a0b474aab486201
20 603cab183e5c75c8b5f4f426245fffc6
21 951a32aa2dc318f958f6343a90520b9a
22 7b48de772acb4f632429a89bcf8cb58b
23 e18509f0de1d1dc4967c8d1d1dc222e9
24 713bbf6e9521194e53a845417ae70178
25 d259c61b387fcd39b3ab83dd9ee1fc26
26 c5b2cfc7315961dc239c70061d5664dc
27 9f2fc27c4942545a6430deb1c126712d
28 71f0c1101306ebd89735b734b500fe10
29 ff6dabf0905fffd7626e9adc12418e979
30 9429ed343b923d08cb76b46b89be9663
31 3b73e06f137fe1776adde3f01965ce72
```

2. Configurer le fichier de recherche des hashes dans Suricata

Suricata peut rechercher des hashes dans un fichier local. Pour ce faire, on va placer le fichier contenant une liste de hashes MD5 que Suricata utilisera pour comparer les fichiers entrants, dans le répertoire **/etc/suricata/**

```
(kali@kali)-[/etc/suricata/rules]
$ ls -l /etc/suricata
total 27724
-rw-r--r-- 1 root root 3327 Oct 1 02:11 classification.config
-rw-r--r-- 1 root root 28279326 Nov 9 11:17 hashes.md5
-rw-r--r-- 1 root root 1375 Oct 1 02:11 reference.config
drwxr-xr-x 2 root root 4096 Nov 9 11:47 rules
-rw-r--r-- 1 root root 86075 Nov 9 11:46 suricata.yaml
-rw-r--r-- 1 root root 1643 Oct 1 02:11 threshold.config
```

3. Activer le hashing des fichiers dans la configuration de Suricata

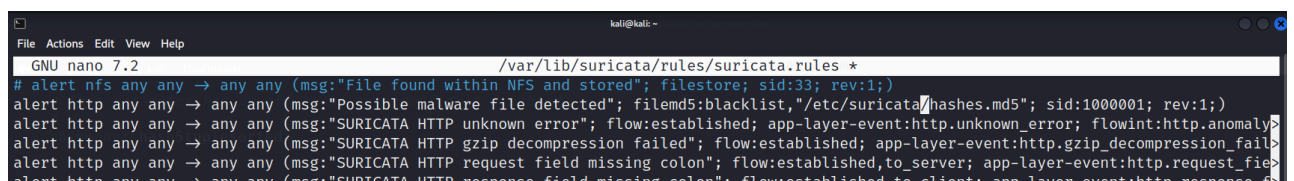
On ouvre le fichier **suricata.yaml** (généralement situé dans **/etc/suricata/**).

Sous la section **files**, on fait activer l'algorithme de hashing et on configure Suricata pour surveiller les types de fichiers pertinents (ex. : exécutables).

```
- files:
  enabled: yes
  force-magic: yes # force logging magic on all logged files
  # force logging of checksums, available hash functions are md5,
  # sha1 and sha256
  force-hash: [md5]
  force-md5: yes
  magic: [document, archive, executable]
```

4. Ecrire la règle Suricata

On écrit la règle Suricata pour lancer une alerte quand les fichiers dont les hashes MD5 figurent dans la liste **hashes.md5** :

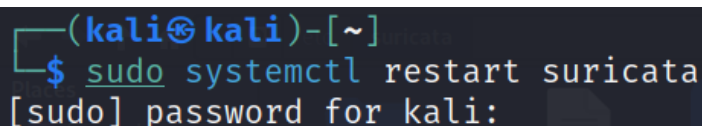


```
GNU nano 7.2 /var/lib/suricata/rules/suricata.rules *
# alert nfs any any -> any any (msg:"File found within NFS and stored"; filestore; sid:33; rev:1;)
alert http any any -> any any (msg:"Possible malware file detected"; filemd5:blacklist,"/etc/suricata/hashes.md5"; sid:1000001; rev:1;)
alert http any any -> any any (msg:"SURICATA HTTP unknown error"; flow:established; app-layer-event:http.unknown_error; flowint:http.anomaly;
alert http any any -> any any (msg:"SURICATA HTTP gzip decompression failed"; flow:established; app-layer-event:http.gzip_decompression_fail;
alert http any any -> any any (msg:"SURICATA HTTP request field missing colon"; flow:established,to_server; app-layer-event:http.request_fie;
alert http any any -> any any (msg:"SURICATA HTTP response field missing colon"; flow:established,to_client; app-layer-event:http.response_fie;
```

Explication des composants de la règle :

- **msg** : Définit le message d'alerte.
- **filemd5:blacklist,"/etc/suricata/hashes.md5"** : Indique à Suricata de comparer les hashes MD5 des fichiers entrants avec ceux de **hashes.md5**.
- **sid** : Un identifiant unique pour cette règle.
- **rev** : Numéro de révision de la règle.

5. Redémarrez Suricata pour charger la nouvelle règle



```
(kali@kali)-[~]
$ sudo systemctl restart suricata
[sudo] password for kali:
```

6. Surveillance :

Consultez les logs de Suricata, généralement dans

- **/var/log/suricata/fast.log** ou

- `/var/log/suricata/alerts.log`

pour vérifier s'il y a des fichiers qui ont été détectés comme ransomware.

7. Mettre à jour la liste des hashes régulièrement

La mise à jour régulière de la liste des hashes est une étape cruciale pour assurer une détection efficace des ransomwares et renforcer la posture de sécurité globale.

Dans un environnement où les menaces évoluent rapidement, cette pratique constitue une défense proactive essentielle contre les cyberattaques. Ignorer cette étape expose les systèmes à des risques accrus, compromettant ainsi la confidentialité, l'intégrité et la disponibilité des données.

AMAHROUK Asmae

Cyber Security Engineering Student