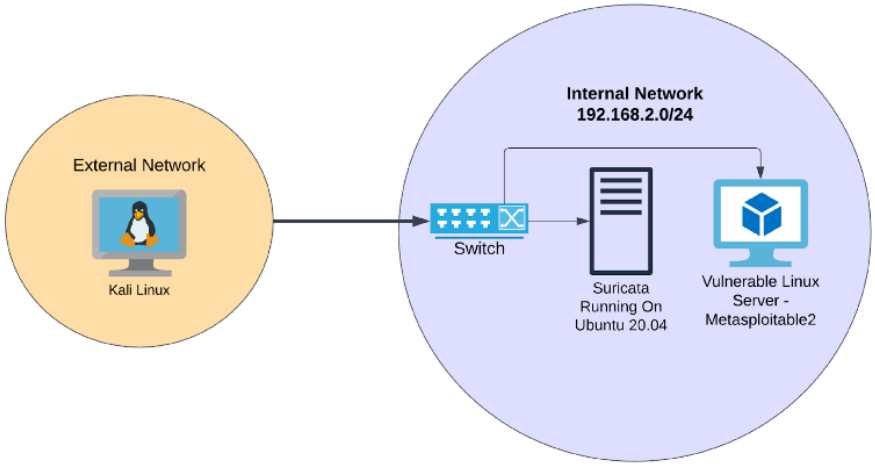
Installation et Configuration : Suricata

I-Environnement

Un réseau externe : VM (OS : Kali linux)

Un réseau interne : VM-1 (Serveur vulnérable (Linux Metasploitable-2))

VM-2 (NIDS) (OS : Suricata sur Ubuntu 20.04)



II-Installation

Appliquer les commandes suivantes pour installer les dépendances nécessaires pour la dernière version de SURICATA :

```
$ sudo apt-get install software-properties-common
$ sudo add-apt-repository ppa:oisf/suricata-stable
$ vsudo apt-get update
```

Puis, taper la commande suivante pour installer la dernière version stable de SURICATA :

```
$ sudo apt-get install suricata -y
```

Après l'installation, vous pouvez tester la version, les options et le status en tapant les commandes suivantes :

```
$ sudo suricata --build-info
$ sudo systemctl status suricata
```

Lancer le service SURICATA :

```
$ sudo systemctl enable  suricata.service
```

Pour arrêter le service SURICATA :

```
$ sudo systemctl stop  suricata
```

Examiner les différentes composantes du service SURICATA :

```
$ ls  -al /etc/suricata
```

III- Configuration

Le fichier **/etc/suricata/suricata.yaml** est le fichier de configuration principal de Suricata. Il est structuré en sections YAML pour configurer divers aspects du fonctionnement de Suricata. Voici une explication des champs les plus courants :

```
$ sudo nano /etc/suricata/suricata.yaml
```

1. Global

Configure les paramètres globaux de Suricata.

```
vars:

  address-groups: {}

  port-groups: {}
```

- **vars** : Définit des groupes d'adresses IP et de ports pour simplifier les règles.
- **address-groups / port-groups** : Permet de définir des regroupements d'adresses IP et de ports.

2. Logging

Définit la manière dont Suricata gère les journaux.

```
logging:

  default-log-level: info

  outputs:

    - console:

        enabled: yes

        level: info

    - file:

        enabled: yes

        filename: /var/log/suricata/suricata.log

        level: info
```

- **default-log-level** : Niveau de journalisation global (ex. info, error, debug).
- **outputs** :
- **console** : Active/désactive les journaux affichés dans la console.
- **file** : Configure l'emplacement et le niveau de détail des journaux dans les fichiers.

3. Network Settings

Configure le mode d'écoute réseau et les interfaces surveillées.

```
af-packet:

  - interface: eth0

    threads: auto

    cluster-id: 99

    cluster-type: cluster_flow

    defrag: yes
```

af-packet : Configure l'interface réseau.

- **interface** : Nom de l'interface à surveiller (ex. eth0).
- **threads** : Nombre de threads utilisés (peut être auto pour s'adapter au matériel).
- **cluster-id** / **cluster-type** : Utilisé pour le traitement multithreadé.
- **defrag** : Active la reconstitution des paquets fragmentés.

4. Capture Settings

Configure la capture des paquets résea

```
pcap:

  enabled: yes

  filename: /path/to/file.pcap
```

pcap : Permet de lire des fichiers PCAP au lieu de surveiller en temps réel.

- **enabled** : Active/désactive la capture à partir de fichiers PCAP.
- **filename** : Chemin vers le fichier PCAP à analyser.

5. Rule Management

Configure les règles IDS/IPS.

```
rule-files:
  - /etc/suricata/rules/local.rules
  - /etc/suricata/rules/emerging-threats.rules
```

rule-files : Liste des fichiers de règles à charger.

- **local.rules** : Règles définies localement.
- **emerging-threats.rules** : Règles téléchargées de sources externes (par exemple, Emerging Threats).

6. Detection

Configure les paramètres de détection des menaces.

```
detect:
  profile: medium
  sgh-mpm-context: auto
  inspection-recursion-limit: 3000
```

- **profile** : Définit le niveau de performance pour la détection (low, medium, high).
- **sgh-mpm-context** : Configure l'algorithme de correspondance des motifs pour l'analyse des signatures.
- **inspection-recursion-limit** : Limite le nombre d'étapes dans l'inspection récursive (protection contre les attaques Evasion).

7. Outputs

Configure les fichiers de sortie pour les journaux et les alertes.

```
outputs:
 - eve-log:
     enabled: yes
     filetype: json
     filename: /var/log/suricata/eve.json
     types:
       - alert
```

```
    - http
    - dns
    - tls
```

eve-log : Principal fichier journal (souvent utilisé pour l'intégration avec SIEM).

- **enabled** : Active/désactive le fichier.
- **filetype** : Format des journaux (par ex. json ou plain).
- **filename** : Emplacement du fichier.
- **types** : Types d'événements à inclure (ex. alert, dns, http).

8. App Layer Protocols

Configure la détection des protocoles d'application.

```
app-layer:
  protocols:
    http:
      enabled: yes
      libhtp:
        default-config:
          personality: IDS
          request-body-limit: 100kb
          response-body-limit: 100kb
```

http : Configure l'analyse des protocoles HTTP.

- **enabled** : Active l'analyse des flux HTTP.
- **request-body-limit** / **response-body-limit** : Limite la taille des corps des requêtes/réponses HTTP à analyser.

9. IPS Mode

Configure Suricata comme un système de prévention des intrusions (IPS).

```
outputs:
  - drop:
      enabled: yes
      filename: /var/log/suricata/drop.log
```

- **drop** : Active l'enregistrement des paquets bloqués dans le mode IPS.

Pour activer le mode IPS, il faut également configurer les interfaces réseau et activer le mode **NFQUEUE** (Netfilter Queue) ou autre.

10. Performance

Configure l'optimisation des ressources.

```
engine-analysis:
  - rule-reload-rate: unlimited
```

rule-reload-rate : Définit à quelle fréquence les règles peuvent être rechargées (unlimited ou une valeur spécifique).

Mise à jour nécessaire

Appliquer les mises à jour du service (les sources)

```
$ sudo suricata-update
$ sudo suricata-update list-sources

$ sudo suricata-update enable-sources malsilo/win-malware
$ sudo suricata-update
```

Tester la configuration du service :

```
$ sudo suricata  -T -c /etc/suricata/suricata.yaml  -v
```

Démarrer le service

```
 $ sudo systemctl start suricata.service
```

Puis vérifier

```
$ sudo systemctl status suricata.service
```

Accèder au fichier fast.log

```
$ sudo cat /var/lib/suricata/fast.log
```

Pour éditer des « rules » il faut stopper le service

```
$ sudo systemctl stop suricata.service
```

A- Gestion des Rules

Puis, ajouter « rule » dans le fichier **/etc/suricata/rules/local.rules**

```
$ sudo nano /etc/suricata/rules/local.rules
```

Un règle prend la forme suivante (exemple) :

```
1 alert icmp any any -> $HOME_NET any (msg : '' ICMP Ping'' ;sid :1 ;rev ;1 ; )
```

Ajouter la règle au fichier de cobfiguration

```
$ sudo nano /etc/suricata/suricata.yaml
```

Puis ajouter **/etc/suricata/rules/local.rules** au champ **rule-files**

Recompiler le service

```
$ sudo suricata -T -c /etc/suricata/suricata.yaml -v
```

Puis redémarrer le service suricata :

```
$ sudo systemctl start suricata.service
```