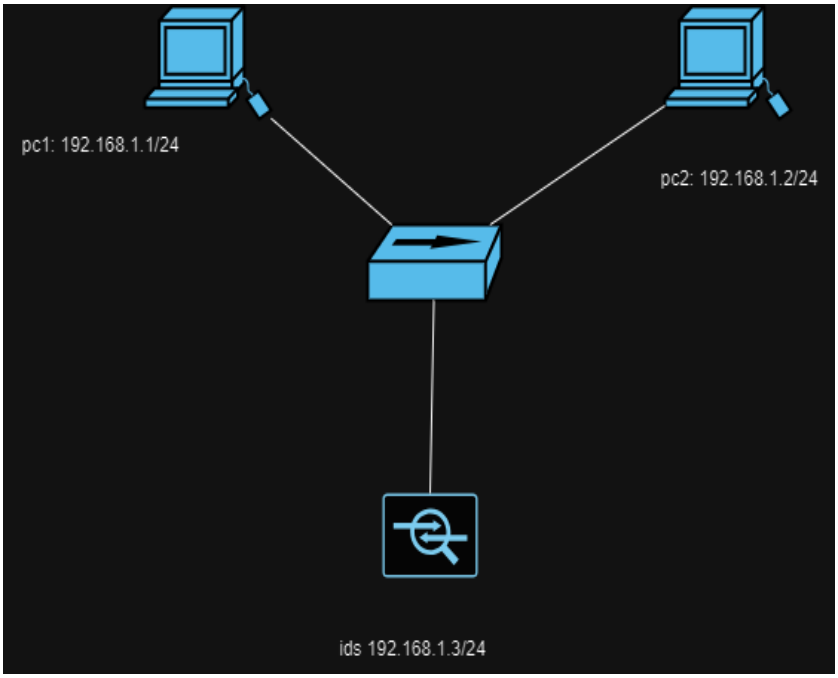
Nous allons donc suivre exactement la méthodologie préconisée dans la présentation. La première phase consiste à identifier la solution de sécurité, ce qui est déjà fait dans notre cas car nous voulons intégrer l'IDS open-source Suricata. En ce qui concerne la deuxième phase nous supposons qu'elle est déjà faite et si vous souhaitez en savoir plus sur l'installation de suricata vous pouvez consulter la documentation officielle ou suivre ce tuto qui donne un aperçu éclair et assez explicite de l'installation et de la configuration de Suricata. Dans exercice pratique, nous allons donc nous concentrer sur la dernière phase qui consiste à intégrer la solution de sécurité à notre réseau virtuel.

Cette phase est subdivisée en trois étapes.

Première étape : Installation de la solution sur un équipement

Pour rappel voici une représentation de l'architecture du réseau virtuel dont vous avez cloné le répertoire depuis GitHub.



Un équipement nommé "ids" fait partir du réseau et sur cet équipement nous allons installer suricata.

1. Création de l'image personnalisée kathara/suricata

La première chose à faire est donc de construire une nouvelle image Docker contenant le package suricata car il n'est pas directement intégré à l'image Docker par défaut utilisé par Kathara pour construire les conteneurs.

Veuillez-vous assurer que vous êtes dans le répertoire « ***install_suricata_lab*** ». En ligne de commande ou via l'interface graphique de Windows, créez un fichier nommé Dockerfile, ouvrez-le puis coller le lignes ci-dessous à l'intérieur :

```
#specify the docker image from the customized image will be build

FROM kathara/base:latest

#update and upgrade

RUN apt-get update && apt-get upgrade -y

#Install suricata and clean cache

RUN apt-get install -y suricata && apt-get clean
```

Enregistrer le fichier puis fermez-le.

Accéder à la ligne de commande puis assurez-vous d'être dans le répertoire « ***install_suricata_lab »*** en exécutant la commande "pwd". Si nous n'êtes pas dans ledit répertoire, déplacez-vous-y alors. Une fois, dans le répertoire « ***install_suricata_lab »,*** exécutez la commande :

```
docker buildx build -t kathara/suricata
```

Cette commande construit une nouvelle image docker nommé ***kathara/suricata*** en utilisant le fichier Dockerfile contenu dans le répertoire courant "."

Après la construction de l'image exécutez la commande ci-dessous et vérifiez que l'image kathara/suricata est bien présente :

```
docker image ls
```

2. Test

Nous devons maintenant vérifier que le package suricata s'est bel et bien installé convenablement. Pour cela nous allons exécuter un conteneur de test en exécutant la commande ci-dessous :

```
docker run --rm -it kathara/suricata /bin/bash
```

Une fois dans le conteneur exécuter la commande :

```
suricata -v
```

La commande devrait retourner la version de suricata et son usage, la preuve que l'installation s'est bien déroulée. Déconnectez-vous ensuite du conteneur en exécutant la commande "exit"

3.Installer suricata sur l'équipement ids

En ligne de commande ou via l'interface graphique ouvrez le fichier ***lab.conf*** et en dessous de la ligne ***"#specific config"*** écrivez la ligne ci-dessous :

```
ids[image]="kathara/suricata"
```

Enregistrez le fichier lab.conf, quittez puis démarrer le réseau virtuel en exécutant la commande:

kathara lstart

Connectez-vous ensuite à l'équipement ids en exécutant la commande :

kathara connect ids

Une fois connecté, exécutez la commande ci-dessous pour vérifier une fois de plus que suricata est installé et que vous avez bien fait les configurations qu'il faut :

suricata -v

Deuxième étape : Configuration manuelle de la solution

Nous supposons que vous maitrisez l'installation et la configuration de Suricata et donc, nous allons définir l'objectif de sécurité de cet IDS. L'IDS doit détecter tous les trafics ICMP. C'est à dire qu'à chaque fois qu'un ping sera effectué sur le réseau, suricata générera une alerte automatiquement.

1. Modification des fichiers appropriés

En étant connecté à l'équipement ids via la commande ***"kathara connect ids"***, ouvrez le fichier ***/etc/suricata/rules/suricata.rules*** en éxecutant la commande :

nano /etc/suricata/rules/suricata.rules

Ecrivez à l'intérieur la règle ci-dessous :

alert icmp qny qny -> any any (msg:"Ping detecter"; flow:stateless; sid:1000001; rev:1;)

Enregistrez le fichier puis quittez.

2. Exécution des commandes requises

Tester vos configurations en éxecutant :

suricata -T -c /etc/suricata/suricata.yaml -v

Démarrer ensuite le service suricata en exécutant la commande ci-dessous :

systemctl start suricata

Vérifiez l'état du service en exécutant la commande ci-dessous :

systemctl status suricata

3. Tester les configurations

Pour afficher les alertes en temps réel exécutez la commande ci-dessous :

tail -f /var/log/suricata/fast.log

Ouvrez ensuite un autre terminal puis connectez-vous à l'équipement pc1 via la commande ***« kathara connect pc1 »*** puis exécutez :

ping 192.168.1.2 -c 4 && ping 192.168.1.3 -c 4

Accéder maintenant au précédant terminal. Vous devez alors voir les alertes s'afficher.

<u>Troisième étape :</u> Automatisation et persistance des configurations

Récapitulons.

Pour configurer notre IDS suricata nous avons modifié un seul fichier nommé ***/etc/suricata/rules/suricata.rules*** puis nous avons exécuter la commande :

```
systemctl suricata start
```

Nous allons donc faire en sorte que ces configurations soient automatisées. En étant connecté à l'équipement "ids" exécutez la commande :

```
cp /etc/suricata/rules/suricata.rules  /shared
```

Vérifiez ensuite la copie en exécutant :

```
ls shared
```

Déconnectez-vous de l'équipement ids en exécutant la commande :

```
exit
```

Ouvrez le fichier ***ids.startup***, écrivez la commande ci-dessous, enregistrez-le, puis fermez-le:

```
systemctl start suricata
```

Créer ensuite l'arborescence de répertoire ***ids/etc/suricata/rules*** en exécutant la commande ci-dessous (il s'agit d'une commande exécuter sous Windows) :

```
mkdir ids\etc\suricata\rules
```

Copier le fichier ***suricata.rules*** vers le répertoire créé précédemment :

```
copy shared\suricata.rules ids\etc\suricata\rules
```

Redémarrez le réseau virtuel via la commande :

```
kathara lrestart
```

Connectez-vous à l'équipement "ids" via la commande :

```
kathara connect ids
```

Recommencer les tests faits au 3. de la deuxième étape.