Lutte Informatique Défensive
SOC, HIDS et SIEM

TP2 - Introduction à la détection d'intrusion

Objectifs de réalisation

Prise en main d'un IDS réseau, configuration et déploiement d'un Suricata. Mise en oeuvre pour l'analyse de trafic.

Format du TP

Travail en groupe (2 ou 3 personnes par groupe) à réaliser sur 4h.

Pré-requis:

- VirtualBox
- Wireshark

Livrables

Le rapport devra être envoyés par email à l'adresse *georges.bossert@sekoia.fr* **à la fin de la séance de TP.**

Consignes

Chapitre 1 - Installation de votre IDS réseau

1.1 Création d'une machine virtuelle "Jessie 64bits" avec l'outil Vagrant

Vagrant est un logiciel libre et open-source pour la création et la configuration des environnements de développement virtuel. Il peut être considéré comme un *wrapper* autour de logiciels de virtualisation comme VirtualBox.
Dans le cadre de ce TP, nous allons utiliser Vagrant pour obtenir une machine virtuelle "Debian Jessie 64bits" installée et prête à l'emploi.

1.1.1 Installation de Vagrant

Sur une Ubuntu ou une Debian à jour, l'installation de vagrant se résume à l'exécution de la commande suivante :

```
georges@dell-gbo ~ $ sudo apt-get install vagrant
```

Si vous utilisez une autre distribution, utilisez votre package manager pour installer le package officiel Vagrant disponible sur: https://www.vagrantup.com/downloads.html.

Une fois installé, vérifiez le bon fonctionnement de Vagrant en affichant sa version tel qu'illustré ci-dessous.

```
georges@dell-gbo ~ $ vagrant -v
Vagrant 2.1.5
```

1.1.2 Création d'une machine virtuelle Jessie 64

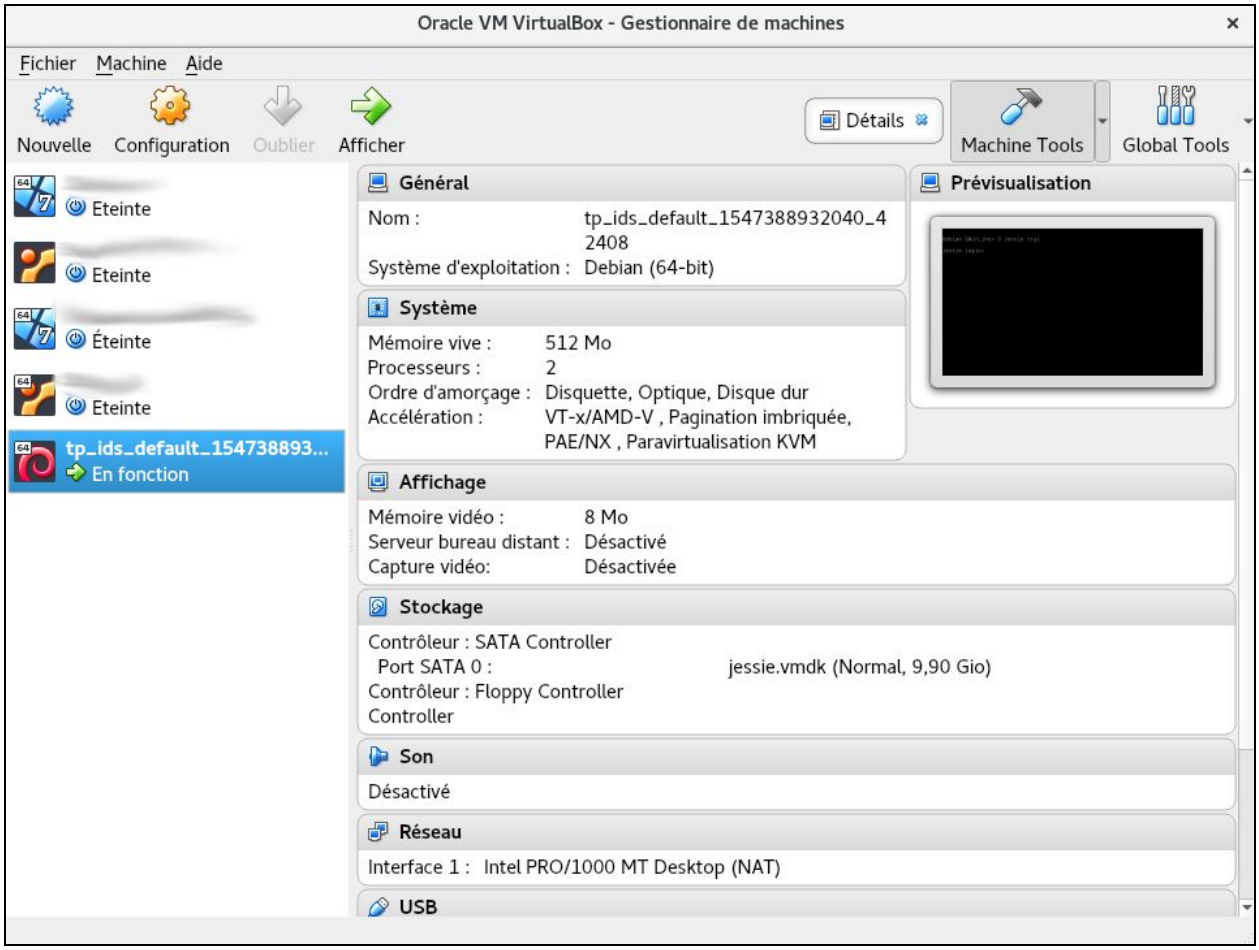
Une fois Vagrant installé, créez un répertoire dédié à votre TP. Nous utiliserons */home/georges/tp_ids* dans la suite du sujet.

```
georges@dell-gbo ~ $ mkdir tp_ids
georges@dell-gbo ~ $ cd tp_ids
georges@dell-gbo ~/tp_ids $ vagrant init debian/jessie64
A `Vagrantfile` has been placed in this directory. You are now
ready to `vagrant up` your first virtual environment! Please read
the comments in the Vagrantfile as well as documentation on
`vagrantup.com` for more information on using Vagrant.
```

```
georges@dell-gbo ~/tp_ids $ vagrant up

Bringing machine 'default' up with 'virtualbox' provider...
==> default: Importing base box 'debian/jessie64'...
[...]
==> default: Machine 'default' has a post `vagrant up` message.
This is a message
==> default: from the creator of the Vagrantfile, and not from
Vagrant itself:
==> default:
==> default: Vanilla Debian box. See
https://app.vagrantup.com/debian for help and bug reports
```

Vous pouvez vérifier que la machine a bien été créé, en ouvrant la GUI de VirtualBox. La capture d'écran ci-dessous illustre la présence d'une machine virtuelle en fonctionnement, nommée "tp_ids_default_…" et créée par Vagrant.



Une fois la machine virtuelle démarrée, l'obtention d'un terminal sur celle-ci se fera par une session ssh telle que configurée par vagrant. Le listing ci-dessous présente l'emploi de la commande *vagrant ssh* pour se connecter en ssh dans la VM courante.

```
georges@dell-gbo ~/tp_ids $ vagrant ssh

The programs included with the Debian GNU/Linux system are free
software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
vagrant@jessie:~$
```

Vous pouvez par exemple vérifiez que vous disposez bien d'une machine virtuelle sous Jessie 64 bits, en affichant ses informations systèmes.

```
vagrant@jessie:~$ uname -a
Linux jessie 3.16.0-6-amd64 #1 SMP Debian 3.16.56-1+deb8u1
(2018-05-08) x86_64 GNU/Linux
```

La suite de ce TP sera réalisé dans cette nouvelle VM et non plus sur votre Host.

1.2 Installation de Suricata

L'installation de Suricata se fait via *apt* à l'aide de la commande suivante

```
vagrant@jessie:~$ sudo apt-get install suricata
```

Si l'installation s'est bien déroulée, vous pouvez vérifier la version installée de Suricata avec la commande suivante:

```
vagrant@jessie:~$ suricata -V
This is Suricata version 2.0.7 RELEASE
```

Les fichiers de configuration de Suricata se trouve dans le répertoire : */etc/suricata/*.
Le principal fichier de configuration est */etc/suricata/suricata-debian.yaml*.

Sans le modifier, analysez le fichier de configuration de Suricata pour répondre aux questions suivantes

- Q1.1: Quel est le répertoire par défaut des journaux d'événements produits ?
- Q1.2: Où seront journalisés toutes les alertes produites ?
- Q1.3: Où seront journalisés tous les événements HTTP capturés ?
- Q1.4: Quelle modification faut-il réaliser dans le fichier de configuration pour
    - journaliser toutes les requêtes DNS capturées par Suricata ?
    - journaliser toutes les alertes en mode "debug" et ainsi obtenir plus d'aide pour la création de signatures
- Q1.5: Quel est le répertoire par défaut des règles ?
- Q1.6: Quels sont les fichiers de règles fourni par défaut par Suricata et en analysant leurs contenu expliquer leurs objectifs de détection respectifs ?

Chapitre 2 - Prise en main de Suricata

2.1 premiere analyse

Utilisez l'outil Wireshark pour étudier le contenu du pcap *`exercice1.pcap`* et répondre aux questions suivantes:

- Q2.1: Quelle est l'adresse IP de la machine à l'initiative de la requête http
- Q2.2: Quelle est l'adresse IP du serveur DNS
- Q2.3: Quelles sont les requêtes HTTP réalisées
- Q2.4: Quelles sont les adresses IP des serveurs associées à chaque requête

Demandez à Suricata d'analyser ce fichier. Pour se faire, utilisez la commande suivante;

```
vagrant@jessie:~$ sudo suricata -c
/etc/suricata/suricata-debian.yaml -r /vagrant/exercice1.pcap
[...]
13/1/2019 -- 15:23:41 - <Notice> - all 4 packet processing threads,
3 management threads initialized, engine started.
13/1/2019 -- 15:23:41 - <Notice> - Signal Received.  Stopping
engine.
13/1/2019 -- 15:23:41 - <Notice> - Pcap-file module read 43
packets, 25091 bytes
```

En analysant les fichiers de journalisations, répondez aux questions suivantes en expliquant la source de votre réponse :

- Q2.5: Combien d'alertes ont été produites par Suricata ?
- Q2.6: Combien de paquets TCP et UDP Suricata a analysés ?
- Q2.7: Combien de sessions TCP ?
- Q2.8: L'analyse de ce pcap a engendré la création de combien d'événements ?

    a. Parmi ces événements, combien sont de type “http”
    b. Parmi ces événements, combien sont de type “dns”
- Q2.9: Quel est le User Agent utilisé par le client http ?
- Q2.10: Quel est le nom de la page web téléchargée en http ?

2.2 Création d’une règle Suricata

Déployer la règle suivante dans le fichier `/etc/suricata/rules/local.rules`:

```
alert http any any -> any any (msg:"UNAUTHORIZED webpage";
flow:established; classtype:policy-violation;
content:"download.html"; http_uri; sid:1;)
```

Puis relancer l’analyse du pcap `exercice1.pcap` après avoir supprimé tous les journaux Suricata avec la commande suivante :

```
vagrant@jessie:~$ sudo rm /var/log/suricata/*
```

En utilisant à minima les sources suivantes:

- l’alerte produite,
- le fichier de configuration de la classification de Suricata `/etc/suricata/classification.config`,
- la documentation officielle de suricata https://suricata.readthedocs.io/en/suricata-4.1.2/rules/index.html,

répondez aux questions suivantes

- Q2.11: À quoi servent les paramètres content et http_uri ?
- Q2.12: Quelle est la différence entre la méthode “sticky buffer” et “content modifier” ?
- Q2.13: Quelle est la catégorie de l’alerte, description complète et sa priorité ?
- Q2.14: Que signifie flow:established ?

En vous inspirant de cette règle, créez une nouvelle règle pour détecter toutes les requêtes DNS contenant le mot “google” et émises vers un serveur DNS n’appartenant pas au réseau `192.168.0.0/16`. Cette alerte devra être de priorité 2 et classifiée en tant que “rogue-dns”. L’alerte produite devra donc ressembler à :

```
05/13/2004-10:17:09.864896  [**] [1:1:0] Unknown DNS server [**]
[Classification: Potential Rogue DNS server spotted] [Priority: 2]
{UDP} 145.254.160.237:3009 -> 145.253.2.203:53
```

2.3. Utilisation du module Eve pour l'analyse DNS

Le module de sortie Eve permet de tracer des événements tels que les alertes, des métadonnées, des informations sur les fichiers ou sur certains protocoles dans un fichier JSON.
La configuration de ce module et plus précisément des différents événements tracés est détaillée dans le fichier `/etc/suricata/suricata-debian.yaml`.

Déclenchez l'analyse du fichier `exercice2.pcap` avec Suricata et observez le contenu du fichier `eve.json`.

1. En utilisant l'outil jq (`sudo apt-get install jq`), identifiez toutes les réponses DNS avec un TTL < 100.
2. Identifiez le top 10 des types de requêtes DNS que l'on peut observer dans ce PCAP (indice: utilisez le champs `dns.rype`)

2.4. Gestion des règles avec Oinkmaster

Il existe plusieurs sources de règles Suricata. Ces sources gratuites ou payantes proposent régulièrement des mises à jours de leurs jeux de règles pour couvrir les dernières menaces. Deux sources de règles Suricata sont souvent citées:

- EmergingThreat
- Cisco VRT

Il est possible de télécharger et d'installer ces jeux de règles manuellement mais il est beaucoup plus simple et rapide d'utiliser un outil dédié. Dans la suite de ce TP, nous utiliserons OinkMaster pour la gestion des règles Suricata.

Pour installer OinkMaster, utilisez le paquet debian officiel:

```
vagrant@jessie:~$ sudo apt-get install oinkmaster
```

Utilisez la documentation officielle proposé sur le site d'EmergingThreats (https://rules.emergingthreats.net/) pour ajouter l'URL du jeux de règles OPEN dans la configuration d'oinkmaster (`/etc/oinkmaster.conf`)

Une fois la configuration de oinkmaster mise-à-jour, il faut utiliser la commande suivante pour déclencher le téléchargement des règles:

```
vagrant@jessie:~$ sudo oinkmaster -C /etc/oinkmaster.conf -o
/etc/suricata/rules
```

Vérifiez ensuite que vous disposez de nouveaux fichiers de règles.

Chapitre 3 - Utilisation de Suricata pour l'analyse

Dans la suite de ce TP, considérez que vous travaillez en tant qu'analyste SOC. Votre travail consiste · entre autres · à analyser les incidents de sécurité qu'ils vous sont remontés.

Chaque analyse doit prendre la forme d'un rapport constitué de trois parties:

1. **Executive Summary:** un résumé de l'incident en quelques lignes destiné à un responsable de votre organisation,
2. **Details of the Incident:** le détail de votre analyse de l'incident, des différentes étapes et des observations réalisées,
3. **Produced IoCs:** la liste des indicateurs de compromissions (IoC) que vous avez identifié pendant votre analyse. Ces IoCs pourront prendre la forme d'indicateurs STIXv2 et de règles Suricata.

3.1. Drive-by

En utilisant votre nouvelle base de règles ré-exécutez une analyse du fichier `exercice2.pcap`. Vous en déduirez qu'il s'agit d'une capture réseau issue d'un réseau disposant · au moins · d'une machine infectée.

Dans votre rapport, identifiez les règles Suricata qui ont levé des alertes et détaillez leurs fonctionnements.

En outre, répondez aux questions suivantes:

- Q3.1: Quel est la date et l'heure de l'activité
- Q3.2: Quelle est l'adresse IP de l'ordinateur de la victime
- Q3.3: Quel est le hostname de l'ordinateur de la victime
- Q3.4: Quelle est l'adresse MAC de l'ordinateur de la victime
- Q3.5: Quelle est l'adresse IP et le nom de domaine associés à l'infection

Cette première analyse doit normalement vous indiquer que l'infection a eu lieu pendant une navigation web:

- Q3.6: Quel site web l'utilisateur a-t-il visité avant que l'on observe le trafic caractéristique de l'infection
- Q3.7: Déterminez si un malware a été envoyé à la victime, la victime est-elle compromise ?

3.2. Braquage à email armé

Utilisez suricata et vos outils préférés pour analyser ce qu'il se passe dans la capture réseau `exercice3.pcap`. Détaillez les règles Suricata qui ont levé des alertes et produisez un rapport d'incident.

3.3 Quel email ?

Utilisez suricata et vos outils préférés pour analyser ce qu'il se passe dans la capture réseau `exercice4.pcap`.

L'analyse de cette capture vous amènera rapidement à comprendre que deux emails malicieux ont été envoyés à la cible. Une illustration de ces deux emails est proposée ci-dessous. Identifiez quel email est la cause de l'infection et produisez un rapport d'incident.