TD SYSTEMES DE DETECTION D'INTRUSION

04/10/2022

Sadry FIEVET
sadry.fievet@etu.univ-cotedazur.fr

Orange Cyberdefense

UNIVERSITÉ CÔTE D'AZUR

Université Nice Sophia Antipolis

TABLE DES MATIÈRES

Vue d'ensemble

Le but de ce TD est de vous familiariser avec les systèmes de détection d'intrusion.

Pour ce faire nous utiliserons deux machines :

- votre propre OS qui sera la machine d'attaque (Kali par exemple)
- une image docker d'un serveur Apache qui tourne sur Ubuntu et qui héberge deux sites vulnérables. Cette machine sera le serveur à protéger (cible)

Objectifs

1. Acquérir les notions de fonctionnement des systèmes de détection d'intrusion (IDS) abordées lors du cours précédent en l'illustrant avec des exemples pratiques.
2. Savoir comment et pourquoi on écrit une règle de filtrage.
3. Connaître les commandes basiques de Snort, Docker, Nmap, Scapy, Hping3.

Rappel

Les systèmes de détection d'intrusion sont des outils qui permettent l'analyse du trafic réseau et/ou machine dans le but de déceler toutes activités suspectes.

Il existe 3 types d'IDS :

NIDS > détection au niveau du réseau
HIDS > détection au niveau d'une machine
Hybrides > les deux

Les IDS sont classés en deux catégories :

- détecteur de signatures
- détecteur d'anomalies

Dans ce TP nous allons étudier le fonctionnement de l'IDS Snort qui est de type NIDS et appartient à la catégorie des détecteurs de signatures.

Présentation de Snort

I. Les différents composants

Snort est constitué de plusieurs composants qui ont chacun un rôle précis.

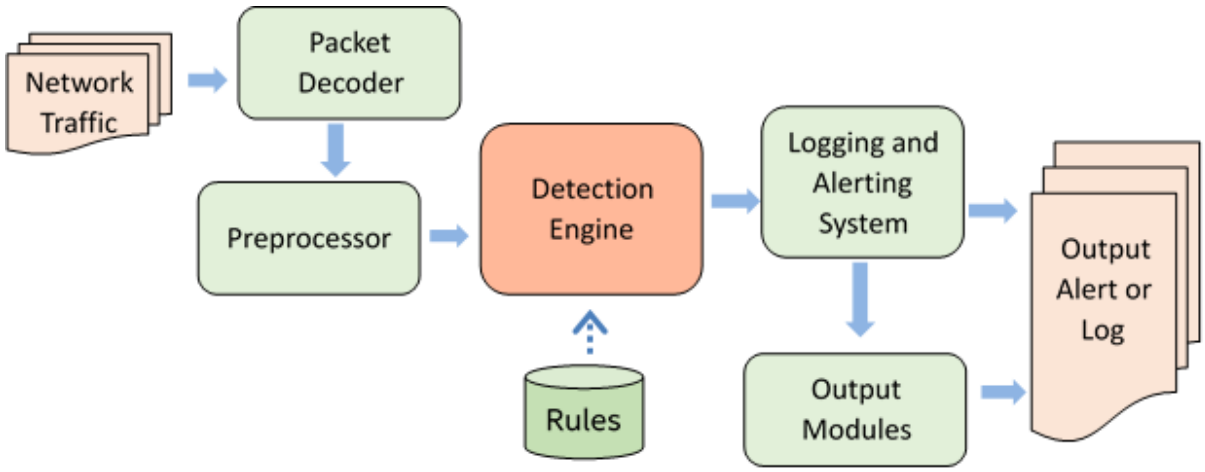


Figure 1 architecture Snort

Décodeur de paquet

Le décodeur est le premier composant de Snort, il récupère les paquets qui proviennent des interfaces et les prépare pour les préprocesseurs. Il est composé de plusieurs sous décodeurs organisés par protocole (Ethernet, TCP, IP...)
Ces décodeurs vont écrire et structurer les informations contenues dans les paquets avant de les envoyer aux préprocesseurs.

Préprocesseurs

Leur rôle principal est de préparer les paquets pour le moteur de détection. Ils permettent d'arranger ou de modifier les données avant que le moteur de détection agisse.
Ils peuvent ainsi parer certaines attaques.

Exemple 1 :
> Vous avez créé une règle afin d'être alerté si un paquet contient la chaîne de caractères : « CASPAR »
Un attaquant peut légèrement changer cette valeur et par exemple envoyer : « C.ASPAR »

Exemple 2 :
>L'attaquant utilise la technique de fragmentation (https://www.incapsula.com/ddos/attack-glossary/ip-fragmentation-attack-teardrop.html) pour envoyer son payload (script d'attaque)

Un préprocesseur doit être capable d'assembler les données fragmentées avant que cela ne soit fait par la machine ciblée.

Les préprocesseurs de Snort sont donc capables de défragmenter des paquets, de les réassembler, de décoder des URI en hexadécimales, d'assembler des flux TCP....

De plus Snort nous permet d'écrire nos propres préprocesseurs.
Quelques exemples de préprocesseurs installés par défaut dans Snort :

Frag3 >> contre les attaques de type fragmentation
SfPortscan >> détecte les scans de ports et balayages d'IPs utilisés dans la phase de reconnaissance par les attaquants.
Http_inspect >> normalise les requêtes http afin de déjouer les injections de caractères hexadécimaux par exemple
Arpspoof >> détecte les attaques d'ARP spoofing
Ssh >> détecte les attaques sur le protocole SSH en contrant les exploits Challenge- Response Buffer Overflow, Secure CRT ou Protocol Mismatch

Moteur de détection

C'est le cœur du dispositif de détection de Snort. Il fonctionne en appliquant les règles prédéfinies sur les paquets. Si un paquet correspond à une règle, une action est déclenchée (journalisation, déclenchement d'une alerte)

Système de journalisation et d'alerte

En fonction des règles appliquées par le moteur de détection, les paquets seront journalisés ou bien ils déclencheront des alertes.

Modules de sortie

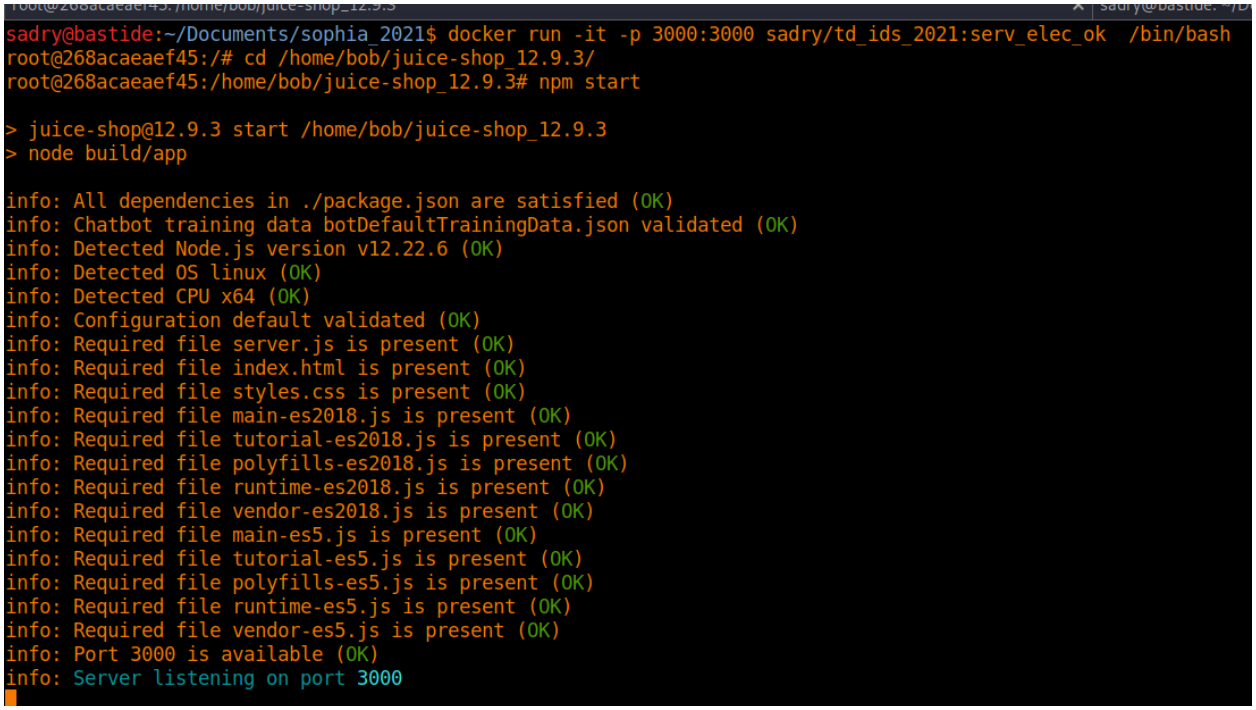
Les modules de sorties permettent de configurer les paramètres de stockage pour la journalisation (fichier textes, format binaire, format Tcpdump) Ils permettent également de configurer le stockage et les actions des alertes (enregistrement dans une base de données, envois d'email, de sms...)

Installation du serveur à défendre

Comme je vous l'ai demandé dans mon document sur les pré requis à ce TD, vous devez avoir installé Docker.
Nous allons donc simplement télécharger à partir du docker hub puis lancer sur notre host une image Docker que je vous ai préparée.
docker pull sadry/td_ids_2021:serv_caspar_ok

Vous avez désormais l'image du serveur vulnérable sur votre machine. Lancez-la dans un conteneur et demandez une invite de commande bash.

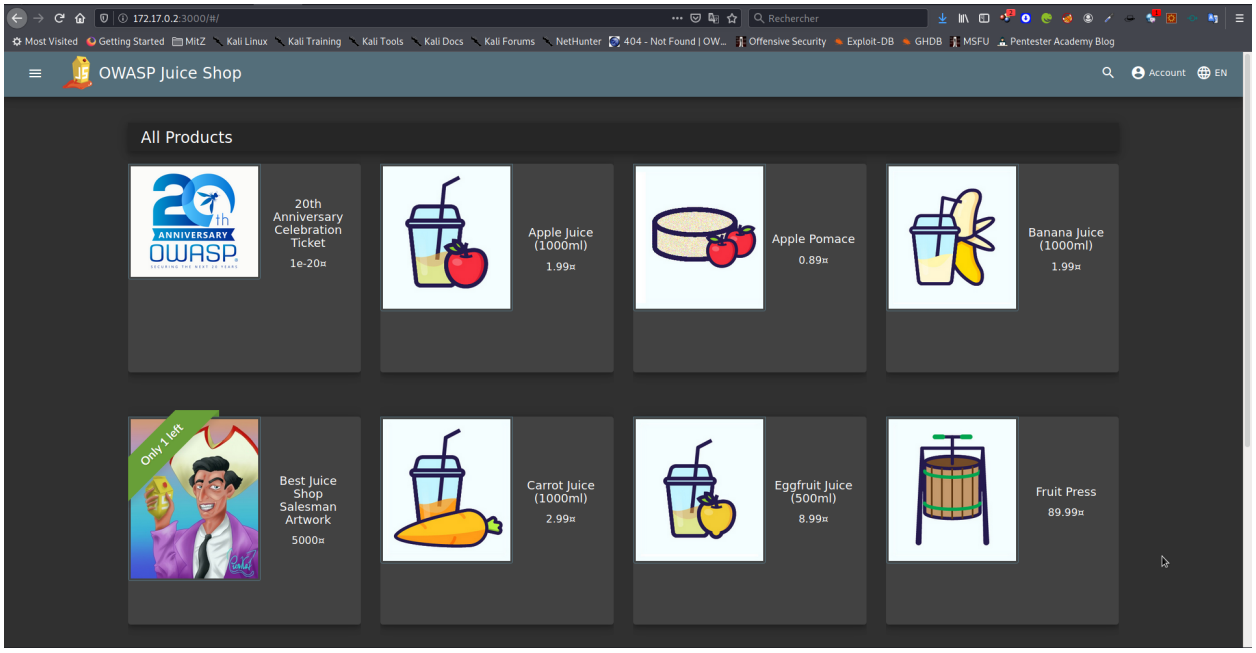
Une fois sur le conteneur, déplacez-vous dans le dossier **/home/bob/webstore/**, puis lancez le serveur "Juice-shop" avec la commande **npm start.**



Ouvrez un navigateur et allez à l'adresse suivante (ipduserveurcible:3000) :

http://172.17.0.2:3000

Vous devriez voir le site OWASP Juice Shop comme sur la capture suivante



OWASP JUICE SHOP

Le site Juice Shop ressemble à une petite boutique en ligne qui vend des jus de fruits & légumes et des produits associés.

À l'exception de l'aspect paiement et livraison, Juice Shop est entièrement fonctionnel.

Le Juice Shop contient 100 défis de difficultés variables où vous êtes censé(e)s exploiter les vulnérabilités de sécurité sous-jacentes.

Ces vulnérabilités ont été intentionnellement implantées dans l'application exactement à cette fin, mais d'une manière qui peut également se produire dans le développement Web « réel » !

OWASP MUTILLIDAE

Comme je vous l'ai indiqué en introduction, le serveur Apache que nous allons protéger avec l'IDS Snort héberge 2 sites web qui contiennent de nombreuses vulnérabilités. Ce site est, comme Juice Shop, un excellent outil d'entraînement pour le pentesting car il contient la quasi-totalité des vulnérabilités recensées par OWASP.

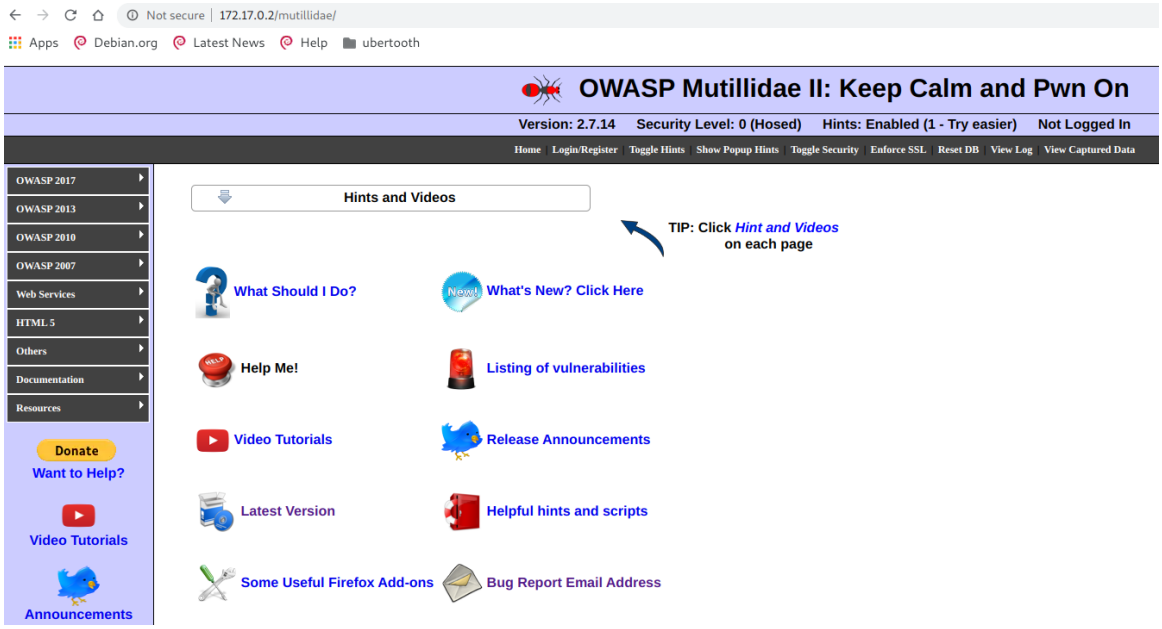
Afin d'y accéder il faut d'abord lancer votre serveur Apache ainsi que le daemon mysqld.

```
root@f3beae8db76f:/# service apache2 start & service mysql start
[1] 1753
 * Starting Apache httpd web server apache2
 * Starting MySQL database server mysqld
su: warning: cannot change directory to /nonexistent: No such file or directory
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.17.0.
2. Set the 'ServerName' directive globally to suppress this message
 *                                                                                    [ OK ]
[1]+  Done                    service apache2 start
```

Vous pouvez maintenant ouvrir un navigateur sur votre machine hôte et tapez l'url suivante

http://172.17.0.2/mutillidae

Vous devriez voir ceci.



Vous pouvez vous enregistrer en créant un compte et commencer à explorer les différentes pages du site.

NMAP

Nmap est un scanner de ports libre créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant. Ce logiciel est devenu une référence pour les administrateurs réseaux car l'audit des résultats de Nmap fournit des indications sur la sécurité d'un réseau. Il est disponible sous Windows, Mac OS X, Linux, BSD et Solaris.

https://nmap.org/

SCAPY

Scapy est un outil de manipulation de paquets réseau écrit en python par Philippe Biondi.

Il est capable, entre autres, d'intercepter le trafic sur un segment réseau, de générer des paquets dans un nombre important de protocoles, de réaliser une prise d'empreinte de la pile TCP/IP, de faire un traceroute, d'analyser le réseau informatique...

https://scapy.net/

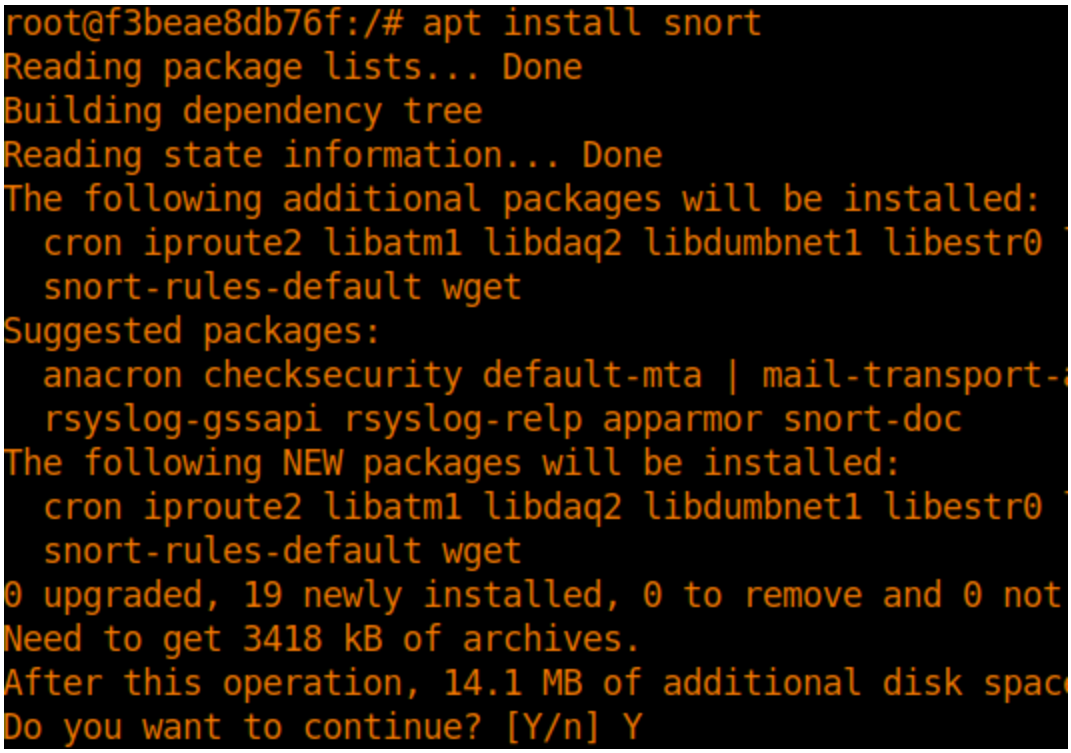
HPING3

Hping3 est un logiciel en ligne de commande créé par Salvatore Sanfilippo qui fonctionne en envoyant des paquets TCP à un port de destination puis en signalant les paquets qu'il reçoit en retour.

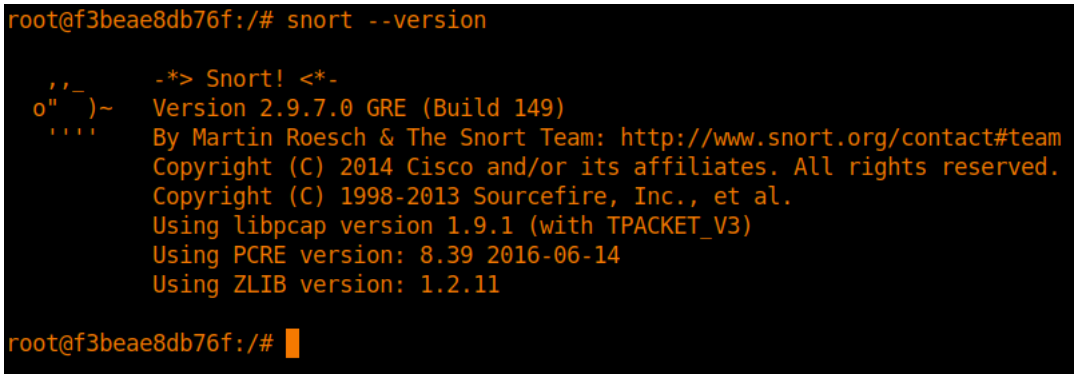
http://www.hping.org/

II. Installation et lancement de Snort

Installez simplement Snort en utilisant le gestionnaire de paquets de votre distribution.



Vérifiez votre installation en demandant la version.



EXERCICES

Nous allons dans un premier temps utiliser Snort en mode sniffeur et faire le tour des commandes classiques. En mode sniffeur Snort n'a pas besoin qu'on lui indique un fichier de configuration.

1 - Lancez Snort sur votre serveur avec les options **-vde**

Explorez les sites Mutillidae et Juice Shop à partir de votre machine hôte et remplissez des champs afin d'envoyer des données. Que se passe-t-il ?

2 - Arrêtez Snort, faites une capture d'écran et décrivez là.

3 - Expliquez à quoi servent les options -d, -e, -v en les illustrant avec des avec des captures d'écrans

4 - Créez un répertoire log, lancez Snort pour qu'il enregistre les logs ICMP dans un fichier, puis envoyez des pings depuis votre machine hôte vers le serveur. Que se passe-t-il ? Décrivez les fichiers enregistrés.

5 - Recommencez l'exercice précédent en enregistrant les données au format binaire. Selon vous quel est l'avantage de la sauvegarde au format binaire ?

6 - Donnez 2 manières pour visualiser les captures binaires (capture d'écran). Lisez avec Snort le fichier que vous venez d'enregistrer.

SNORT MODE IDS : CRÉATION D'ALERTES

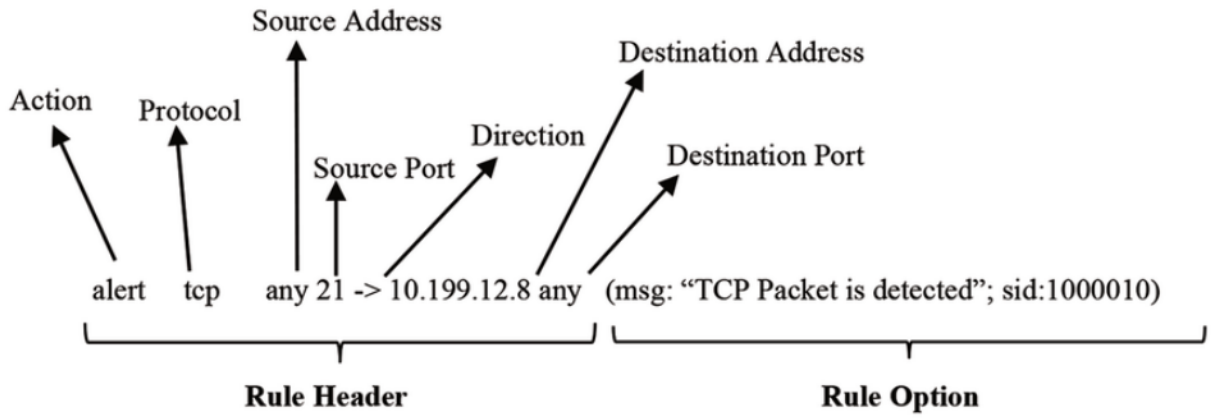
En mode IDS Snort n'enregistre plus tous les paquets comme on l'a vu en mode sniffeur, il va désormais appliquer les règles que l'on a configurées pour chacun d'eux. Cela se fait en éditant le fichier de configuration de Snort et en précisant son chemin au niveau de la commande :

snort -dev -l log -c /etc/snort/snort.conf -i interface_name

Faites une copie du fichier /etc/snort/snort.conf avant de l'éditer

Les règles de Snort

Les règles s'écrivent sur une seule ligne et se composent ainsi :



Entête de la Règle

Comme on le voit dans la figure précédente, c'est dans la règle de l'entête que l'on définit les actions à prendre. Snort propose 5 actions :

- alert : génère une alerte définie et journalise le paquet
- log : journalise le paquet
- pass : ignore le paquet
- activate : fait une alerte et active une règle dynamique
- dynamic : reste passif jusqu'à avoir été activé par une règle activate et puis agit comme une règle log.

Options de la Règle

C’est dans cette partie que va s’effectuer la détection grâce aux options indiquées et qui peuvent être combinées afin d’affiner au mieux la règle.

Liste des options :

msg > affiche un message dans les alertes et journalise les paquets

logto > journalise le paquet dans un fichier nommé par l'utilisateur au lieu de la sortie standard

content > recherche un motif dans la charge d'un paquet

offset > modifie l'option content, fixe le décalage du début de la tentative de correspondance de motif

depth > modifie l'option content, fixe la profondeur maximale de recherche pour la tentative de correspondance de motif

nocase > correspond à la procédure de chaîne de contenu sans sensibilité à la casse

session > affiche l'information de la couche applicative pour la session donnée

ip_proto > permet de définir un protocole au-dessus de IP

classtype > assigne une classification à l’attaque (virus, cheval de Troie)

flow > permet de fixer le sens d’un flux

react > réponse active

Etudiez la manière d’écrire et de sauvegarder les règles Snort.

EXERCICES

Vous allez maintenant écrire des règles afin de détecter différentes attaques. Afin d'optimiser la vitesse de fonctionnement de Snort vous allez tout d'abord mettre en commentaire toutes les lignes qui correspondent aux paramétrage des préprocesseurs dans votre fichier snort.conf.

1 – Écrivez une règle qui déclenche une alerte contenant le message « Tentative de connexion **SSH** » lorsqu'une tentative de connexion **SSH** provenant de n'importe quelle IP est détectée. Lancez Snort en mode IDS puis essayez d'établir une connexion SSH à partir de votre machine physique vers votre serveur. Expliquer le fonctionnement de cette règle avec un schéma.

2 – Écrivez une règle qui déclenche une alerte contenant le message « Tentative de scan **XMAS** » lorsqu'un attaquant utilise la technique de scan XMAS avec NMAP. Lancez Snort en mode IDS puis, avec Nmap faites un scan de type **XMAS** sur votre serveur. Que se passe-t-il ? Écrivez un script python qui utilise la Scapy pour faire un nouveau scan XMAS.

3 - Allez sur le site Juice Shop et visitez la page "about you". Analysez attentivement cette page et vous allez découvrir un lien vers un répertoire qui contient des données confidentielles qui ne devraient normalement pas être accessibles. Récupérer ensuite le fichier : **acquisitions.md**. Ecrivez maintenant une règle Snort qui alerte si on essaie de récupérer ce fichier. Lancez Snort et essayez à nouveau de récupérer le fichier.

4 – Sur le site Mutilidae :
Choisissez 2 vulnérabilités et pour chacune d'elles :

- Lancer une attaque sans règle de détection.
- Écrire une règle de détection et vérifier son efficacité en jouant l'attaque à nouveau.

5 - Pour cet exercice vous allez devoir vous connecter à la place de l'administrateur du site et prendre ainsi le contrôle total sur cette boutique en ligne ! Commencez par lancer Snort.

Dans un premier temps vous devez trouver l'adresse email de l'administrateur du site. Essayez ensuite de découvrir le mot de passe en vous aidant de cette liste : **/usr/share/seclists/Passwords/Common-Credentials/best1050.txt**

Une fois que vous avez réussi à vous connecter à la place de l'administrateur, observez les sorties de Snort et écrivez une règle qui alerte en cas d'attaque de ce type. Testez ensuite cette règle en jouant à nouveau votre attaque.

6 - Les attaques de type DOS (déni de service) ciblent la disponibilité des données en surchargeant les serveurs de requêtes. Vous allez utiliser l'outil **Hping3** afin d'attaquer le serveur et observer la sortie de Snort.

Lancez dans un premier temps une attaque DOS avec Hping3 et décrivez ce qui se passe. Écrivez une règle qui détecte cette attaque et vérifiez-la.

Avez-vous pu neutraliser cette attaque ? Expliquez.

Faites l'exercice précédent avec une attaque DDOS en répondant à toutes ses questions.

Donnez une manière d'échapper au filtrage de la règle DOS avec une attaque DOS.

RECOMMANDATIONS

Les TDs sont également notés sur la présentation. Vous devez expliquer vos commandes et les compléter avec des captures d'écrans. La rédaction et la mise en forme sont donc importantes. Vous êtes libres d'écrire en anglais ou en français et vous avez la possibilité de faire ce TD en binôme.

IMPORTANT

Vous devez envoyer vos rapports à :
sadry.fievet@etu.univ-cotedazur.fr en précisant dans l'objet **[TD-IDS-NOM1_NOM2-PARCOURS]**

Vos documents doivent avoir un titre comportant vos noms ex: **tp_ids_Nom1-Nom2.pdf**

FIN DU TD