UVSQ- Master SECRETS – IDS – TD Snort

1. Installer snort sur une machine virtuelle

Ne pas oublier d'installer les règles (*snort-rules-default* généralement dans les distributions classiques), et éventuellement la documentation.

Les extensions avec base de données ne sont pas nécessaires pour ce TD.

2. Premiers pas avec snort

▪ Mode “sniffer”

Snort peut se comporter en simple sniffer : pour cela, les options à utiliser sont :

-v : verbeux

-d : affiche les infos des couches données

-e : affiche les infos des couches basses

Créez du trafic réseau entre la machine virtuelle et la machine hôte ou une autre machine virtuelle et observez les informations fournies par snort.

Vous pouvez spécifiez l'interface avec l'option **-i** ou un fichier de capture, comme le fichier **test.pcap** fourni, avec l'option **-r** :

sudo snort -r test.pcap -dev

■ Mode “logger”

Pour enregistrer les informations fournies, on utilisera :

-l <dir> : logger dans le répertoire spécifié ; celui-ci doit exister.

Comme précédemment générez du trafic et lisez les fichiers dans le répertoire spécifié avec tcpdump ou wireshark :

sudo snort -r test.pcap -devl -l /var/log/snort

■ Mode “IDS”

Cette partie met en oeuvre la détection d'intrusion.

Pour cela, on utilise snort avec l'option **-c <fichier de configuration>**.

On utiliser également l'option **-k none** pour désactiver la vérification des checksums sur les paquets.

Snort enregistre ses alertes au format texte ou au format unified2 dans le

répertoire **/var/log/snort/**, selon les arguments passés sur la ligne de commande et selon les paramètres du fichier de configuration.

Dans le fichier de configuration **/etc/snort/snort.conf**, vous modifierez la section 6 (*Configure output plugins*) comme suit:

output unified2: filename snort_merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types

output alert_unified2: filename snort_alert.log, limit 128, nostamp

output log_unified2: filename snort_standard.log, limit 128, nostamp

Pour lever des alertes dans un fichier texte :

**sudo snort -eIr test.pcap -k none -l /var/log/snort **

-A full -c /etc/snort/snort.conf

On pourra alors lancer snort dans un terminal et superviser le fichier de logs en parallèle via la commande **tail -f /var/log/snort/alert**.

Quelles sont les alertes levées ?

Retrouvez les règles associées (répertoire **/etc/snort/rules**) et comprenez leur fonctionnement.

Lever ensuite les alertes dans un fichier au format unified2 :

**sudo snort -eIr test.pcap -k none -l /var/log/snort **

-c /etc/snort/snort.conf

Pour visualiser le contenu des fichiers au format unified2, on utilisera l'outil **u2spewfoo** ; il n'est pas fourni dans le package Ubuntu, il faut donc le compiler à partir des sources de **snort**. NB : pour compiler ceci, vous aurez certainement besoin d'installer **daq** et **libdnet**.

Lisez ensuite les différents fichiers de log snort au format unified2 se trouvant dans **/var/log/snort/** :

sudo u2spewfoo snort_standard.log

sudo u2spewfoo snort_alert.log

sudo u2spewfoo snort_merged.log

Depuis votre station hôte ou une autre machine virtuelle, déclenchez les mêmes alertes que celles observées dans le fichier de log, en écoutant sur l'interface

réseau.

Enfin, rédigez une nouvelle règle (dans le fichier **/etc/snort/rules/local.rules**) qui lèvera une alerte lorsqu'un paquet vérifiera les conditions suivantes :

- le paquet appartient à une connexion TCP sur le port 4567 ;
- il est envoyé par le client au serveur ;
- il contient le motif *UVSQmasterSECRETS* : celui-ci est situé après les 8 premiers octets de données et on ne différenciera pas les minuscules des majuscules (*uVsQmasTerseCReTS* marchera, ainsi que *UVSQMASTERsecrets*) ;
- le TTL du paquet est inférieur à 10 ;

Vous la testerez enfin en émettant le paquet en question vers la machine qui fait tourner snort.

Pour tester vos règles, il est plus efficace d'ajouter les différents paramètres l'un après l'autre. Notez bien qu'une règle snort doit inclure un intitulé et un identifiant uniquer (vous vous référerez à la documentation).