Détection d'intrusions avec SNORT sous Debian 11

1) Installation de snort

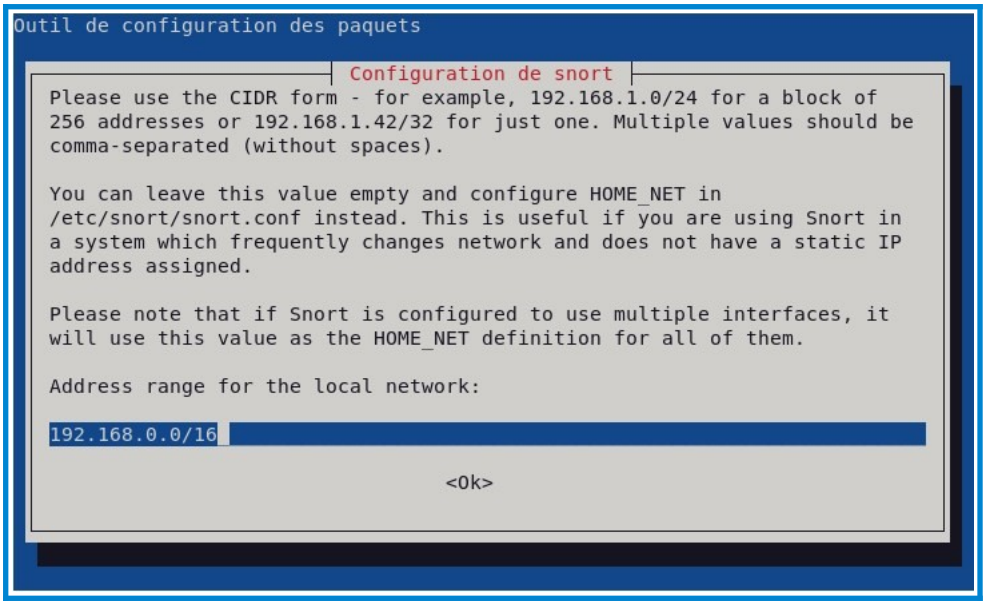
Installer Snort

```
apt-get install snort
```

Les paquets suivants doivent être installés :

```
libdaq2 libdumbnet1 oinkmaster snort snort-common snort-common-libraries
snort-rules-default
```

Définir l'**adresse du réseau** qui sera surveillée



2) Configuration de Snort

Le fichier de configuration initial se trouve dans **/etc/snort/snort.conf**

La démarche et les informations de configuration se trouvent dans le fichier lui-même.

Pendant l'installation, le fichier **/etc/snort/snort.debian.conf** a aussi été créé et modifié avec les paramètres saisis précédemment. Ce fichier est pris en compte dans **snort.conf**.

Pour s'assurer que la configuration ne contient pas d'erreur :

```
sudo snort -T -c /etc/snort/snort.conf
```

qui doit afficher le message **« Snort successfully validated the configuration »**

Snort fonctionne selon deux modes :

- **Analyse en temps réel** : Snort analyse toutes les trames qui circulent sur l'interface réseau configurée et affiche directement les résultats dans la fenêtre de commande. Ce mode est surtout utilisé pour la mise au point des réglages ou pour une vérification ponctuelle.
- **Détection d'intrusion** : le vrai mode de fonctionnement de Snort. Le trafic est analysé sur l'interface configurée et des alertes sont déclenchées si une trame suspecte est identifiée.

2.1) Mode analyse en temps réel

Il suffit d'exécuter la commande :

```
snort -v -c /etc/snort/snort.conf
```

Dans ce mode, les avertissements sont consignés dans **/var/log/snort/snort.log**

Les alertes sont consignées dans **/var/log/snort/snort.alert** et **/var/log/snort/snort.alert.fast**

2.2) Mode détection d'intrusion (IDS)

La commande à exécuter est la suivante :

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

L'analyse perdure tant que la fenêtre ou le processus ne sont pas clôturés.

Dans ce mode, les avertissements sont scindés dans plusieurs fichiers snort.log (ajout d'un suffixe numérique) afin de conserver une performance d'analyse des logs.

Les alertes sont consignées dans **/var/log/snort/snort.alert** et **/var/log/snort/alert** (seul ce fichier est lisible directement)

Lors de vos tests, la commande suivante permet d'afficher les dernières lignes d'un fichier log (ici snort.log). L'affichage est rafraîchi par défaut toutes les 2 secondes.

```
watch tail /var/log/snort.log
```

3) Ecriture de règles personnalisées

3.1) Alerte sur PING ICMP

Nous allons simuler une tentative de découverte du réseau via un ping

Il faut écrire la règle suivante à la fin du fichier **/etc/snort/rules/local.rules**

```
alert icmp any any -> $HOME_NET any (msg:"Découverte PING"; sid:10000001; rev:001;)
```

Cette règle va générer une alerte “Decouverte Ping” dès qu’un paquet ICMP est détecté par l’IDS.

À partir d’un autre machine faire un ping, ici un ping de la machine 192.168.1.50 vers 192.168.1.100 (serveur snort) provoque la détection d’activité :

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
10/12-19:31:21.685153 192.168.1.50 -> 192.168.1.100
ICMP TTL:128 TOS:0x0 ID:19297 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:21  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Dans le fichier log d’alerte, ont obtient :

```
[**] [1:10000001:1] "Découverte PING" [**]
[Priority: 0]
10/12-19:31:21.685153 192.168.1.50 -> 192.168.1.100
ICMP TTL:128 TOS:0x0 ID:19333 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:57  ECHO

[**] [1:10000001:1] "Découverte PING" [**]
[Priority: 0]
10/12-19:31:21.690237 192.168.1.100 -> 192.168.1.50
ICMP TTL:64 TOS:0x0 ID:16151 IpLen:20 DgmLen:60
Type:0  Code:0  ID:1  Seq:57  ECHO REPLY
```

Le comportement a non seulement été détécté, mais classifié par Snort comme étant une alerte de type Découverte PING.

3.2) Explication des paramètres de règle

La forme générale d’une règle Snort est la suivante :

action protocole ipSource portSource direction ipDestination portDestination (options)

action:action à réaliser

Si Snort est en mode passif (IDS) ou inline (IPS)

alert	Génération d’un alerte puis journalisation
log	Journalisation de l’événement uniquement
pass	Ignorance du paquet
activate	Levée d’une alerte et activation d’une autre règle dynamic
dynamic	Règle activée par une autre règle activate, puis journalisation

Si snort est en mode IPS uniquement

drop	Rejet du paquet puis journalisation Pas de retour à l’émetteur

reject	Rejet du paquet puis journalisation
	Envoi d'un paquet TCP reset (si TCP)
	Envoi d'un paquet ICMP port unreachable (si UDP)
sdrop	Rejet du paquet sans journalisation

protocole : le protocole utilisé par le paquet concerné

Valeurs possibles : TCP, UDP, ICMP et IP

ipSource : adresse IP source au format au format CIDR XXX.XXX.XXX.XXX/XX

Exemples de valeurs possibles :

any	N'importe quelle adresse
xxx.xxx.xxx.xxx/xx	Une adresse réseau ou une machine suivant le masque
[xxx.xxx.xxx.xxx/xx,yyy.yyy.yyy.yyy/yy]	Deux adresses réseau
!xxx.xxx.xxx.xxx/xx	Tout sauf l'adresse xxx.xxx.xxx.xxx/xx
$xxxxxxxxxxx	Une variable définie dans les fichiers de configuration de Snort. Par exemple $HOME_NET qui représente l'adresse du réseau local

portSource : numéro de port concerné

Exemples de valeurs possibles :

any	N'importe quel port
xxxxx	Un port
xxxxx:yyyyy	Une étendue de ports
!xxxxx	Tout sauf le port xxxxx

direction : sens de la communication

Valeurs possibles :

->	La règle concerne uniquement le sens source vers destination
<>	La règle concerne les sens source vers destination mais aussi le sens destination vers source (bidirectionnel)

ipDestination : adresse ip de destination (la syntaxe a utiliser est la même que celle d'ipSource)

portDestination : port de destination (la syntaxe à utiliser est la même que celle de portSource)

(options) : options de traitement de la règle

la forme générale des options est :

(msg : « le message » ; sid:xxx;rev:xxx;classtype:nomClasse;content : «signature»)

Explications pour chaque option :

msg : le message qui sera affiché dans la console ou inscrit dans le journal

sid : un numéro d'identifiant de la règle. **Doit être unique**.

rev : un numéro de révision (version) de la règle, si plusieurs versions existent pour un même sid, la règle avec le numéro de révision le plus haut est appliquée, les autres sont ignorées.

Classtype : (facultatif) permet de classer l'événement (utile pour simplifier les recherches futures dans le journal)

Classtype	Description	Priority
attempted-admin	Attempted Administrator Privilege Gain	high
attempted-user	Attempted User Privilege Gain	high
inappropriate-content	Inappropriate Content was Detected	high
policy-violation	Potential Corporate Privacy Violation	high
shellcode-detect	Executable code was detected	high
successful-admin	Successful Administrator Privilege Gain	high
successful-user	Successful User Privilege Gain	high
trojan-activity	A Network Trojan was detected	high
unsuccessful-user	Unsuccessful User Privilege Gain	high
web-application-attack	Web Application Attack	high
attempted-dos	Attempted Denial of Service	medium
attempted-recon	Attempted Information Leak	medium
bad-unknown	Potentially Bad Traffic	medium
default-login-attempt	Attempt to login by a default username and password	medium
denial-of-service	Detection of a Denial of Service Attack	medium
misc-attack	Misc Attack	medium
non-standard-protocol t	Detection of a non-standard protocol or even	medium
rpc-portmap-decode	Decode of an RPC Query	medium
successful-dos	Denial of Service	medium
successful-recon-largescale	Large Scale Information Leak	medium
successful-recon-limited	Information Leak	medium
suspicious-filename-detect	A suspicious filename was detected	medium
suspicious-login	An attempted login using a suspicious username	medium

	was detected	
system-call-detect	A system call was detected	medium
unusual-client-port-connection	A client was using an unusual port	medium
web-application-activity	Access to a potentially vulnerable web application	medium
icmp-event t	Generic ICMP even	low
misc-activity	Misc activity	low
network-scan	Detection of a Network Scan	low
not-suspicious	Not Suspicious Traffic	low
protocol-command-decode	Generic Protocol Command Decode	low
string-detect	A suspicious string was detected	low
unknown	Unknown Traffic	low
tcp-connection	A TCP connection was detected	very low

content : (facultatif) une signature remarquable du paquet, permettant d'identifier le type de menace. Par exemple, la règle suivante permet de détecter une tentative de connexion à un partage distant du serveur 192.168.1.200.

alert tcp any any -> 192.168.1.200/32 111 (content:"|00 01 86 a5|"; msg: "mountd access";)

Si on reprend la règle écrite dans la section 3.1 - Alerte sur PING ICMP, on peut maintenant expliquer le détail :

```
alert icmp any any -> $HOME_NET any (msg:"Découverte PING"; sid:10000001; rev:001;)
```

action	protocole	ipSource	portSource	direction	ipDestination	portDestination
alert Alerter et journaliser	icmp	any N'importe quelle source	any	-> En entrée	$HOME_NET Vers le réseau local	any Sur n'importe quel port destination
(options) (msg:"Découverte PING"; sid:10000001; rev:001;) Message affiché « Découverte PING» Identifiant de règle 10000001 version 001						

4) Exploitation des règles d'analyses pré-écrites

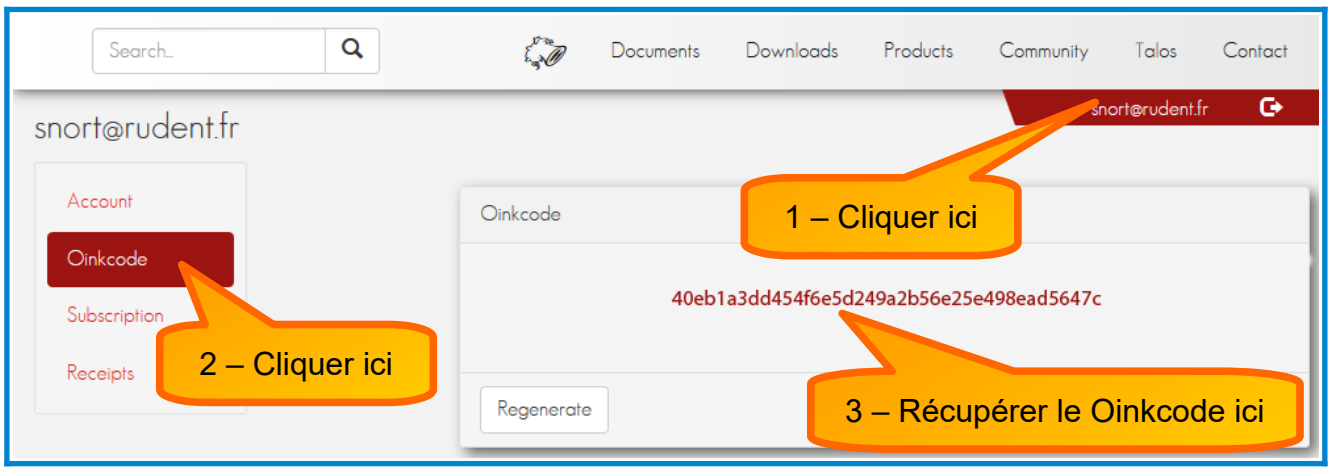
Snort contient des règles par défaut dès l'installation, cependant, afin que le système reste efficace, il est nécessaire de mettre à jour la liste des règles d'analyse.

Pour ce faire, vous devez récupérer les règles d'analyse permettant de détecter les intrusions, il en existe de trois types (vous ne devez en télécharger qu'une seule) :

- les « **Community rules** » sont gratuites. Ce sont les règles de base, les nouveautés n'y sont pas intégrées, elle ne nécessitent pas de compte sur snort.org
- les « **Registered user rules** » sont gratuites, mais l'inscription est obligatoire sur le site snort.org pour les télécharger. Ce sont les règles incluant les dernières attaques du mois (ces règles ne détectent pas les attaques découvertes durant les 30 derniers jours)
- le « **Suscribers rules** » sont payantes. Ce sont les règles incluant toutes les attaques connues jusqu'à ce jour (ces règles ne détectent pas les attaques de type 0-day)

Dans la suite nous utiliserons les «Registered User rules »

Le Oinkcode utilisé pour les téléchargements est disponible sur le site snort.org, dans les préférences du profil utilisateur



Sur le site web, les règles à télécharger sont disponibles à l'adresse https://www.snort.org/downloads/registered/snortrules-snapshot-29181.tar.gz

Vous pouvez télécharger les règles en utilisant la ligne de commande suivante :

```
wget https://www.snort.org/rules/snortrules-snapshot-29181.tar.gz?oinkcode=<votrecode>
```

<votrecode> correspond au Oinkcode associé à votre compte web snort

Ce qui donnerait avec l'exemple ci-dessus :

```
wget https://www.snort.org/rules/snortrules-snapshot-29181.tar.gz?oinkcode=40eb1a3dd454f6e5d249a2b56e25e498ead5647c -O snortrules.tar.gz
```

Il suffit ensuite d'installer les règles dans le répertoire de snort

```
tar -xvf snortrules.tar.gz -C /etc/snort/
```

puis redémarrer Snort.

L'automatisation de la mise à jour des règles est possible via le script PulletPork (https://github.com/shirkdog/pulledpork). Procédure non documentée ici.