

Home Lab - IDS/IPS : Short



Auteur : Ismaël Baby

Période : Automne 2025

Étudiant en Cybersécurité

Rédigé le 18 Mai 2025

Home Lab - IDS/IPS : Snort

Partie 1 : Installation de Snort

L'installation de l'outil de détection d'intrusion (IDS) Snort a été réalisée sur l'environnement de la machine virtuelle Linux Mint :

Commande utilisée :

```
mint@mint:~$ sudo apt install snort -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdaq2t64 libdumbnet1 liblua5.1-2 liblua5.1-common libnetfilter-queue1 libpcrc3 oinkmaster snort-common snort-common-libraries
  snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2t64 libdumbnet1 liblua5.1-2 liblua5.1-common libnetfilter-queue1 libpcrc3 oinkmaster snort snort-common snort-common-libraries
  snort-rules-default
0 upgraded, 11 newly installed, 0 to remove and 382 not upgraded.
Need to get 2666 kB of archives.
After this operation, 11.4 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble/universe amd64 liblua5.1-2 amd64 2.1.0+git20231223.c525bcb+dfsg-1 [49.2 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/universe amd64 liblua5.1-common all 2.1.0+git20231223.c525bcb+dfsg-1 [275 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble/universe amd64 libpcrc3 amd64 2:8.39-15build1 [248 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble/universe amd64 snort-common-libraries amd64 2.9.20-0+deb11ubuntu1 [899 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble/universe amd64 snort-rules-default all 2.9.20-0+deb11ubuntu1 [144 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble/universe amd64 snort-common all 2.9.20-0+deb11ubuntu1 [47.7 kB]
Get:7 http://archive.ubuntu.com/ubuntu noble/universe amd64 libdumbnet1 amd64 1.17.0-1ubuntu2 [30.7 kB]
Get:8 http://archive.ubuntu.com/ubuntu noble/universe amd64 libnetfilter-queue1 amd64 1.0.5-4build1 [15.1 kB]
Get:9 http://archive.ubuntu.com/ubuntu noble/universe amd64 libdaq2t64 amd64 2.0.7-5.1build3 [92.9 kB]
Get:10 http://archive.ubuntu.com/ubuntu noble/universe amd64 snort amd64 2.9.20-0+deb11ubuntu1 [791 kB]
Get:11 http://archive.ubuntu.com/ubuntu noble/universe amd64 oinkmaster all 2.0-4.2 [71.9 kB]
Fetched 2666 kB in 1s (2380 kB/s)
Preconfiguring packages ...
Snort configuration: interface default not set, using 'enp0s3'
Selecting previously unselected package liblua5.1-common.
(Reading database ... 490682 files and directories currently installed.)
Preparing to unpack .../00-liblua5.1-common-2.1.0+git20231223.c525bcb+dfsg-1.all.deb ...
Unpacking liblua5.1-common (2.1.0+git20231223.c525bcb+dfsg-1) ...
Selecting previously unselected package liblua5.1-2:amd64.
Preparing to unpack .../01-liblua5.1-2-2.1.0+git20231223.c525bcb+dfsg-1_amd64.deb ...
Unpacking liblua5.1-2:amd64 (2.1.0+git20231223.c525bcb+dfsg-1) ...
```

Partie 2 : Configuration de Snort

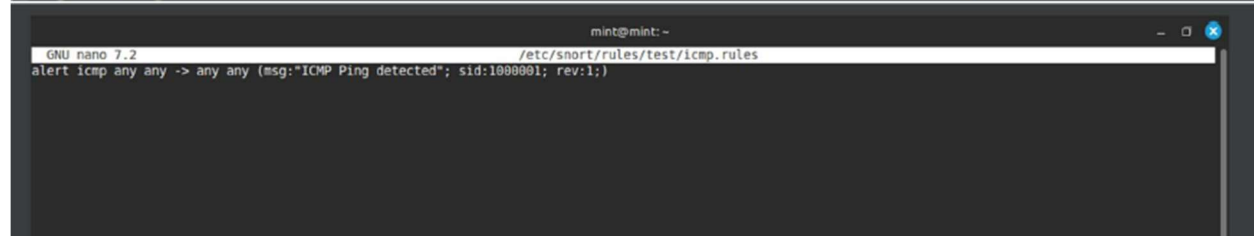
Pour tester la fonctionnalité de détection d'intrusion, une règle personnalisée visant à détecter le trafic ICMP (notamment les pings) a été créée.

Commandes utilisées pour la création de la règle :

1. Création du répertoire pour la règle : `sudo mkdir -p /etc/snort/rules/test`
2. Création et édition du fichier de règle : `sudo nano /etc/snort/rules/test/icmp.rules`

Règle personnalisée créée (icmp.rules) :

```
mint@mint:~$ sudo mkdir -p /etc/snort/rules/test
mint@mint:~$ sudo nano -p /etc/snort/rules/test
mint@mint:~$ sudo nano /etc/snort/rules/test/icmp.rules
```



Home Lab - IDS/IPS : Snort

Partie 3 : Exécution et Test de Snort

Snort a été lancé pour écouter le trafic sur l'interface réseau spécifique et appliquer la règle personnalisée. Un test de connectivité (ping) a ensuite été initié à partir d'une autre machine (Windows) pour vérifier si Snort générait correctement une alerte.

Commande utilisée pour lancer Snort :

```
sudo snort -A console -q -c /etc/snort/rules/test/icmp.rules -i enp0s3
```

- -A console : Afficher les alertes sur la console.
- -q : Mode silencieux (supprime le splash screen de démarrage).
- -c <fichier> : Utiliser le fichier de configuration/règles spécifié.
- -i <interface> : Écouter sur l'interface réseau enp0s3.

```
mint@mint:~$ sudo snort -A console -q -c /etc/snort/rules/test/icmp.rules -i enp0s3
^C*** Caught Int-Signal
C [REDACTED]
C [REDACTED] ping 192.168.0.107

Envoi d'une requête 'Ping' 192.168.0.107 avec 32 octets de données :
Réponse de 192.168.0.107 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.0.107 : octets=32 temps<1ms TTL=64
Réponse de 192.168.0.107 : octets=32 temps<1ms TTL=64
Réponse de 192.168.0.107 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.0.107:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
  Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C [REDACTED]
```

Conclusions : Rôle de Snort comme IDS

Snort joue le rôle de **Système de Détection d'Intrusion (IDS)** libre qui analyse le trafic réseau en temps réel.

- **Fonctionnement** : Snort compare les paquets de données qui transitent sur le réseau aux signatures d'attaques connues (ou aux règles personnalisées).
- **Résultat** : Lorsqu'un comportement suspect ou correspondant à une règle est détecté (comme le ping ICMP dans ce lab), Snort est capable de générer des alertes.

Home Lab - IDS/IPS : Snort

- **Importance** : Ceci permet de surveiller efficacement et de manière proactive la sécurité d'un réseau informatique.

Ce laboratoire a démontré avec succès l'installation, la configuration d'une règle personnalisée, et l'efficacité de Snort à détecter un trafic réseau simple mais pertinent (ICMP), confirmant ainsi son utilité en tant qu'outil de surveillance de sécurité.