TP SNORT

Table des matières

1. Qu'est-ce que SNORT ? 2
   1. Introduction 2
   2. Historique 2
   3. Fonctionnement et architecture 2
   4. Principaux cas d'utilisation 2
   5. Conclusion 2
2. Installation de SNORT 3
   1. Mettre à jour le système 3
   2. Installer les dépendances 3
   3. Récupérer le code source 3
   4. Configurer et compiler 3
   5. Vérifier l'installation 3
   6. Activer Snort au démarrage 4

1. Qu'est-ce que SNORT ?

1. Introduction

Snort fonctionne sur Linux et Windows et se présente comme un outil léger, gratuit et open source pour la surveillance de traffic réseau. Il offre trois principaux modes d'utilisation :

- Mode Sniffer : capture et affiche les paquets au fil de l'eau.
- Mode Logger : enregistre les paquets dans des fichiers pour analyse ultérieure.
- Mode IDS/NIPS : compare le flux réseau à un ensemble de règles pour générer des alertes ou agir en prévention.

2. Historique

Le projet Snort a démarré en 1998 sous l'impulsion de Martin Roesch, à l'origine pour remplacer des solutions propriétaires coûteuses. En 2001, Roesch fonde Sourcefire pour commercialiser une version professionnelle de Snort tout en maintenant la version communautaire gratuite. En 2013, Cisco acquiert Sourcefire, intégrant Snort à sa suite de sécurité et renforçant ainsi son adoption dans les environnements d'entreprise

3. Fonctionnement et architecture

Le cœur de Snort repose sur un moteur d'analyse en temps réel capable de :

1. Analyse de protocoles : déchiffrement des entêtes et vérification de la conformité aux standards.
2. Recherche et correspondance de contenu : détection de motifs malveillants dans les paquets.
3. Préprocesseurs : modules modulaires qui prétraitent le traffic (recomposition de flux TCP, détection de scan, etc.). Avec Snort 3, une nouvelle architecture améliore la performance, la scalabilité et intègre un langage de règles en Lua pour une meilleure lisibilité et vérifiabilité.

4. Principaux cas d'utilisation

Snort est largement déployé pour :

- Détection d'intrusions : alertes en temps réel sur tentatives d'attaques (buffer overflow, scans de ports, injections CGI…)
- Prévention d'intrusions : bloquer automatiquement le trafic malveillant en mode IPS.
- Intégration dans les routeurs Cisco ISR : Snort IPS/IDS peut être embarqué sur les routeurs Cisco 4000 Series pour protéger des succursales.
- Analyse forensique : journalisation détaillée des flux pour enquête post-incident.

5. Conclusion

Grâce à sa communauté active et aux mises à jour régulières, Snort reste la référence des IDS open source, avec des millions de téléchargements et un vaste écosystème de règles partagées. Son adoption dans des solutions embarquées, sa modularité et son langage de règles puissant continuent de répondre aux besoins de détection et de prévention des menaces réseau.

2. Installation de SNORT

1. Mettre à jour le système

```
linuxclient@linuxclient:~$ sudo apt update
[sudo] Mot de passe de linuxclient :
Réception de :1 http://security.debian.org/debian-security bookworm-security InRelease [48,0 kB]
Réception de :2 http://security.debian.org/debian-security bookworm-security/main Sources [153 kB]
Réception de :3 http://security.debian.org/debian-security bookworm-security/main amd64 Packages [255 kB]
Atteint :4 https://repo.zabbix.com/zabbix-tools/debian-ubuntu bookworm InRelease
Atteint :5 https://repo.zabbix.com/zabbix/7.0/debian bookworm InRelease
Réception de :6 http://security.debian.org/debian-security bookworm-security/main Translation-en [152 kB]
Atteint :7 http://deb.debian.org/debian bookworm InRelease
Réception de :8 http://deb.debian.org/debian bookworm-updates InRelease [55,4 kB]
664 ko réceptionnés en 5s (122 ko/s)
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
```

```
linuxclient@linuxclient:~$ sudo apt upgrade
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

2. Installer les dépendances

```
linuxclient@linuxclient:~$ sudo apt install -y build-essential libpcap-dev libpcre3-dev bison flex
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
```

3. Récupérer le code source

```
linuxclient@linuxclient:~$ sudo git clone https://github.com/snort3/snort3.git
Clonage dans 'snort3'...
remote: Enumerating objects: 120892, done.
remote: Counting objects: 100% (13425/13425), done.
remote: Compressing objects: 100% (2321/2321), done.
Réception d'objets:   0% (371/120892), 60.00 Kio | 81.00 Kio/s
```

4. Configurer et compiler

Configurez les options de compilation (réglage des préprocesseurs, chemins d'installation…) :
./configure

Compilez Snort 3 :
make

Installez le binaire et les fichiers de configuration :
sudo make install

Cette séquence génère les exécutables et place les configurations par défaut dans `/usr/local/etc/snort/`

5. Vérifier l'installation

Contrôlez la version de Snort pour vous assurer que tout fonctionne :
snort -V

On doit obtenir une sortie de ce type :
,,_ -*> Snort++ <*-

o")~ Version 3.x.x.x

...

Using DAQ version x.x.x

Cette commande confirme l'installation réussie de Snort 3 et du module DAQ

6. Activer Snort au démarrage

sudo systemctl enable snort

Et pour finir, il faut lancer Snort comme service :

sudo systemctl start snort.

Avec toutes ces configurations, l'IDS Snort est opérationnel dès le démarrage de la machine !