

snort : Système de Détection d'Intrusion

- Objet : Un système de détection d'intrusion
- Niveau requis :
[débutant, avisé](#)
- Commentaires : *Pour analyser le trafic réseau et tenter de détecter une intrusion éventuelle.*
- Débutant, à savoir : [Utiliser GNU/Linux en ligne de commande, tout commence là !](#) 😊
- Suivi :
[obsolete](#)
 - Création par [martinux_qc](#) le 10/12/2012
 - Testé par [oxyz](#) le 16/05/16
- Commentaires sur le forum : [ici](#)¹⁾

Introduction

Le programme snort est considéré comme sniffers, mais il a aussi la fonction de IDS (Intrusion Detection System = détecteur d'intrusion), on va plutôt regarder la fonction IDS que sniffers

Installation

Pour l'installer faite simplement un :

```
apt-get update && apt-get install snort
```

Utilisation

```
snort
```

Pour le démarrer en IDS faite :

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

Ctrl+C pour l'arrêter

Voilà votre système est surveillé, pour voir les logs des attaques et si il y en a aller voir dans :
`/var/log/snort`

¹⁾

N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !

From:

<http://debian-facile.org/> - **Documentation - Wiki**

Permanent link:

<http://debian-facile.org/doc:reseau:snort>



Last update: **03/06/2023 00:38**