

Projet "Sécurité des réseaux et du web"

Sous thème :

Système De Détection Et De Prevention D'intrusion : IDS /IPS (SNORT)



Réaliser par :
HIDSI Elmahdi

Encadrée par :
Mr. SADQI Yassine

Année Universitaire : **2022/2023**

Sommaire

Objectifs:	- 4 -
Tache 1 : installation et configuration de Pfsense	- 4 -
1.Téléchargement de Pfsense :	- 4 -
2.installation Pfsense comme virtuel machine :	- 4 -
3.Modification sur les paramètres réseaux du Pfsense pour ajouter un réseaux LAN :	- 5 -
4.installation un autre système d'exploitation sur le virtuel machine pour faire les tests (kali linux) :	- 5 -
5. Sélection du réseaux LAN sur les paramètres réseaux du kali linux sur le virtuel machine pour connecter à Pfsense :	- 6 -
6.Test de ping sur l'adresse LAN :	- 6 -
7.Pfsense authentification :	- 7 -
Tache 2 : Configuration SNORT sur Pfsense :	- 7 -
1.Package Manager Pfsense :	- 7 -
2.Installation du SNORT :	- 7 -
3.Configuration SNORT :	- 8 -
3.1 Pour Snort oinkmaster code	- 8 -
3.2 Pour les cases coucher :	- 8 -
3.3 configurations de la mise à jour :	- 8 -
4.Mise à jour des différentes règles du SNOTR :	- 9 -
5.Configurations d'interfaces :	- 9 -
5.1 Interface WAN :	- 9 -
5.2 Interface LAN :	- 11 -
6.Activation des interfaces :	- 11 -
Tache 3 : Attaques pour tester :	- 12 -
1.Attaque sur LAN :	- 12 -
1.1 nmap via Kali Linux.....	- 12 -
1.2 les alertes reçus sur LAN :	- 13 -
2.Attaque sur WAN :	- 13 -
2.1 Tester avec des sites web malveillantes :	- 13 -
2.2 Alertes sur WAN :	- 14 -

Liste des figures

Figure 1 : Téléchargement du Pfsense	- 4 -
Figure 2 : L'accueil Pfsense.....	- 4 -
Figure 3 : Ajouter un réseaux LAN	- 5 -
Figure 4 : Kali Linux	- 5 -
Figure 5 : Sélection du réseaux LAN.....	- 6 -
Figure 6 : Ping sur L'adresse LAN	- 6 -
Figure 7 : Pfsense Sign in.....	- 7 -
Figure 8 : Pfsense Packet Manager	- 7 -
Figure 9 : installation SNORT sur Pfsense	- 7 -
Figure 10 : SNORT global settings	- 8 -
Figure 11 : SNORT global settings	- 8 -
Figure 12 : SNORT oinkmaster code	- 8 -
Figure 13 : SNORT global settings	- 9 -
Figure 14 : SNORT update	- 9 -
Figure 15 : Interfaces WAN Settings	- 10 -
Figure 16 : Interfaces WAN Settings	- 10 -
Figure 17 : Interface WAN catégories	- 11 -
Figure 18 : Snort Interfaces.....	- 11 -
Figure 19 : Attaque sur l'interface LAN.....	- 12 -
Figure 20 : Alerts de l'interface LAN	- 13 -
Figure 21 : Sites web malveillantes.....	- 13 -
Figure 22 : Alerts de l'interface WAN.....	- 14 -

Objectifs:

L'objectif d est de mettre en place un système de détection d'intrusion en se basant sur le logiciel libre **Snort**. C'est un système de détection d'intrusion libre qui est capable d'effectuer en temps réel des analyses de trafic et de logger les paquets sur un réseau IP. Il peut effectuer des analyses de protocoles, recherche/correspondance de contenu et peut être utilisé pour détecter une grande variété d'attaques.

Tache 1 : installation et configuration de Pfsense

1.Téléchargement de Pfsense :

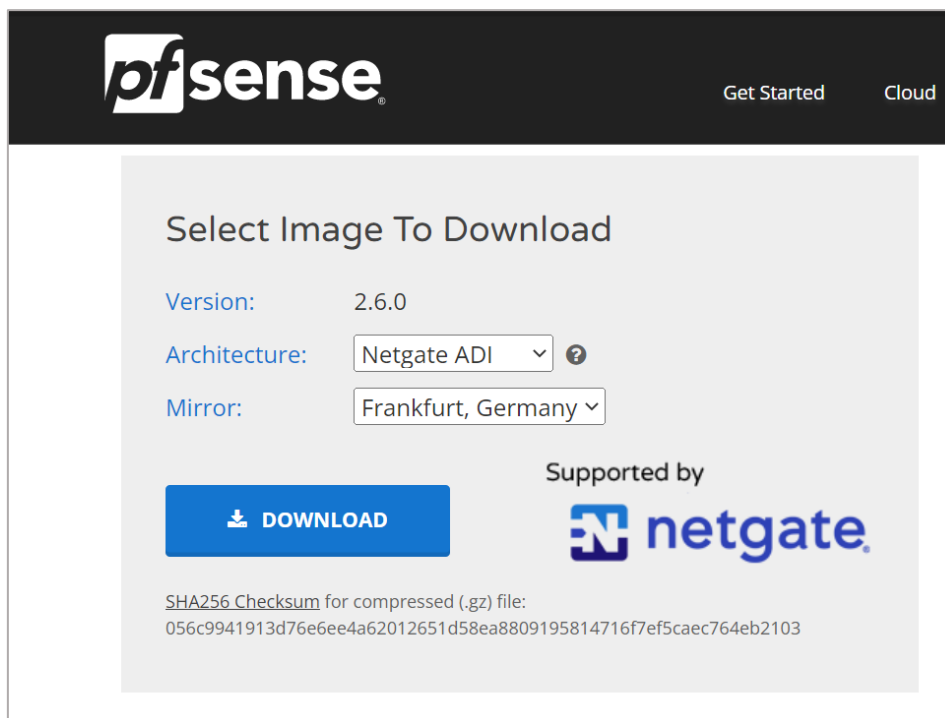


Figure 1 : Téléchargement du Pfsense

2.installation Pfsense comme virtuel machine :

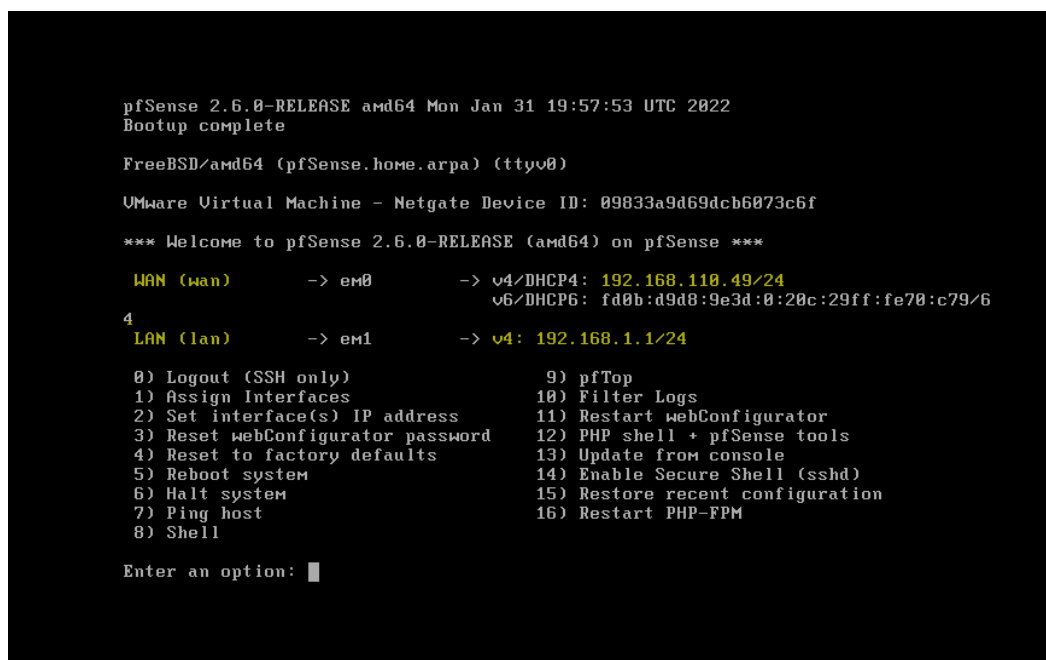


Figure 2 : L'accueil Pfsense

3.Modification sur les paramètres réseaux du Pfsense pour ajouter un réseaux LAN :

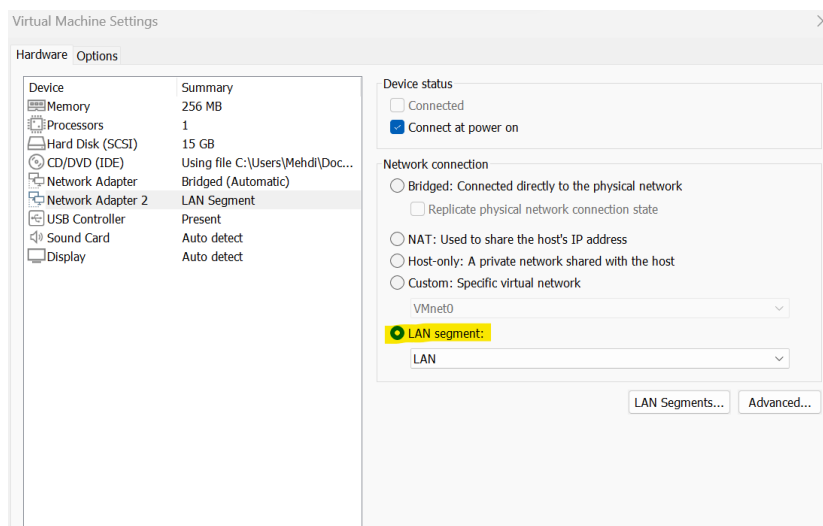


Figure 3 : Ajouter un réseaux LAN

4.installation un autre système d'exploitation sur le virtuel machine pour faire les tests (kali linux) :

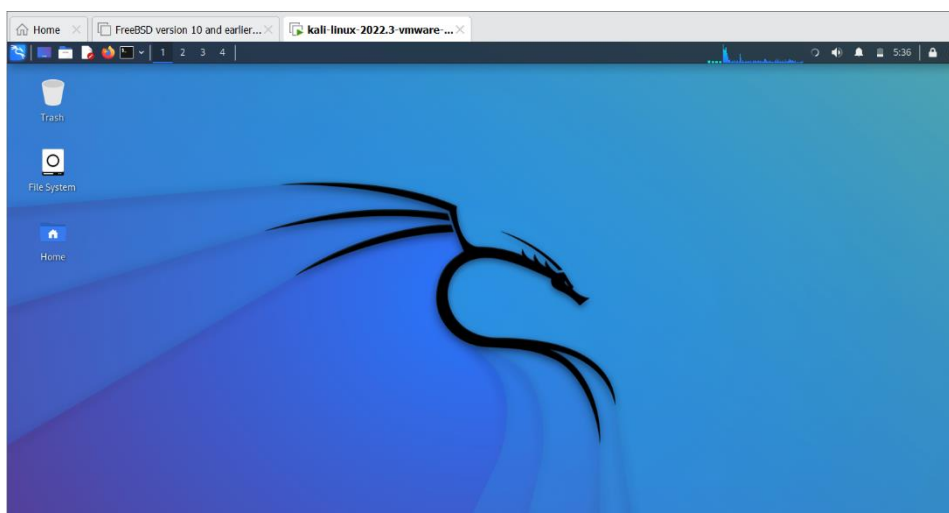


Figure 4 : Kali Linux

5. Sélection du réseaux LAN sur les paramètres réseaux du kali linux sur le virtuel machine pour connecter à PfSense :

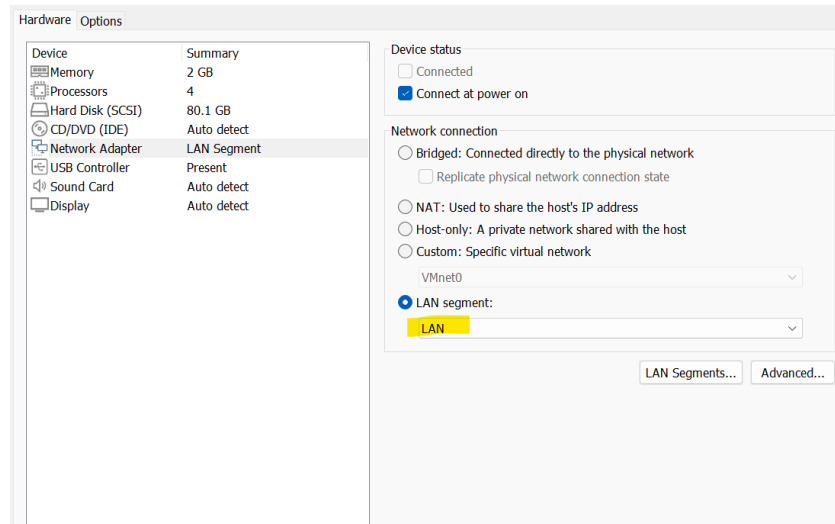


Figure 5 : Sélection du réseaux LAN

6. Test de ping sur l'adresse LAN :

Un ping sur l'adresse LAN (192.168.1.1/24) pour tester la connexion entre kali linux et PfSense :

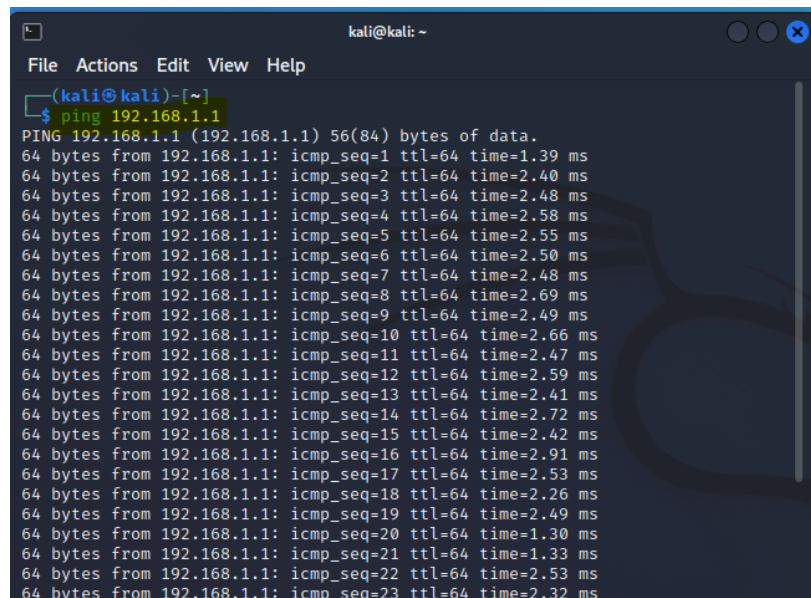


Figure 6 : Ping sur L'adresse LAN

7. Pfsense authentication :

Maintenant la saisie d'adresse **LAN (192.168.1.1/24)** sur un navigateur pour connecter à Pfsense :

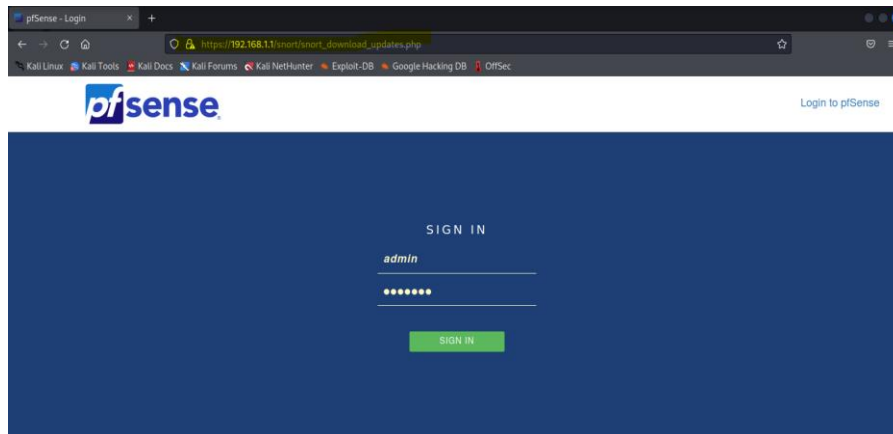


Figure 7 : Pfsense Sign in

Tache 2 : Configuration SNORT sur Pfsense :

1. Package Manager Pfsense :

Maintenant en note que notre **pfSense** installé et configuré, nous nous rendons dans le **Packet Manager** :

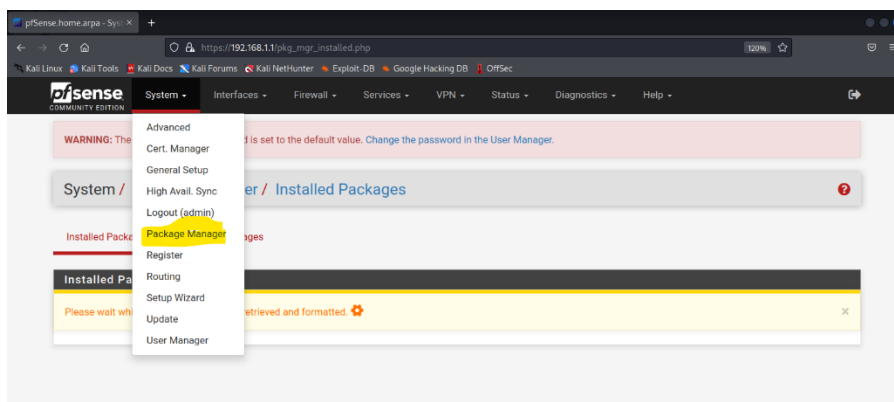


Figure 8 : Pfsense Packet Manager

2. Installation du SNORT :

On clique ensuite sur **Install** puis **Confirmé** et l'installation se lance :

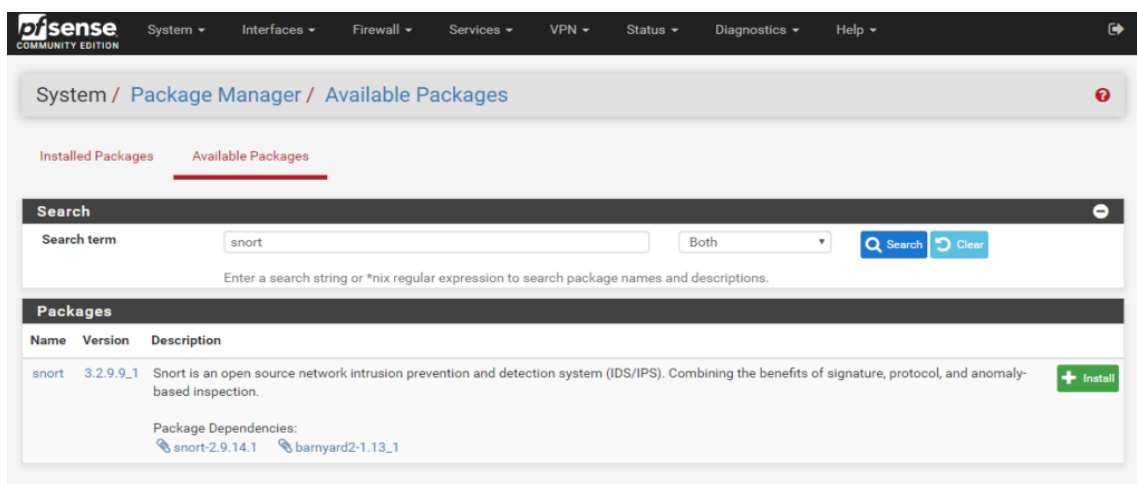
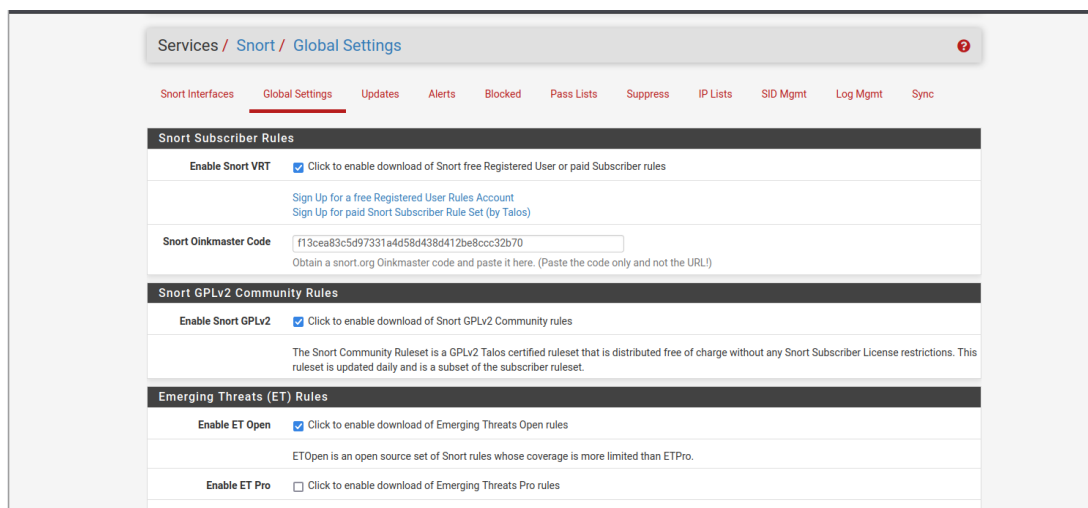


Figure 9 : installation SNORT sur Pfsense

3.Configuration SNORT :

Une fois installé, **SNORT** apparaîtra dans l'onglet **Services**. Une fois rendu dessus, nous allons dans un premier temps aller sur l'onglet **Global Settings** :



Services / Snort / Global Settings

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Snort Subscriber Rules

Enable Snort VRT ☒ Click to enable download of Snort free Registered User or paid Subscriber rules

[Sign Up for a free Registered User Rules Account](#)
[Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)

Snort Oinkmaster Code
Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL)

Snort GPLv2 Community Rules

Enable Snort GPLv2 ☒ Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

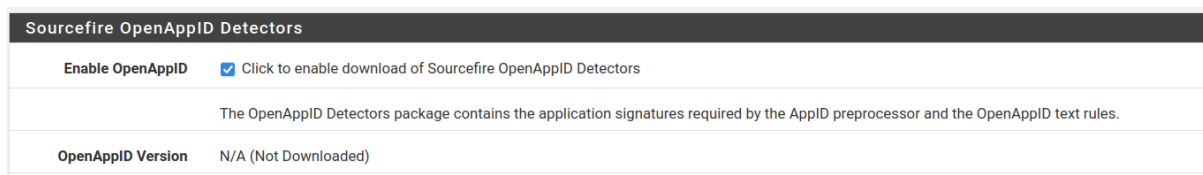
Enable ET Open ☒ Click to enable download of Emerging Threats Open rules

ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

Enable ET Pro ☐ Click to enable download of Emerging Threats Pro rules

[Sign Up for an ETPro Account](#)

Figure 10 : SNORT global settings



Sourcefire OpenAppID Detectors

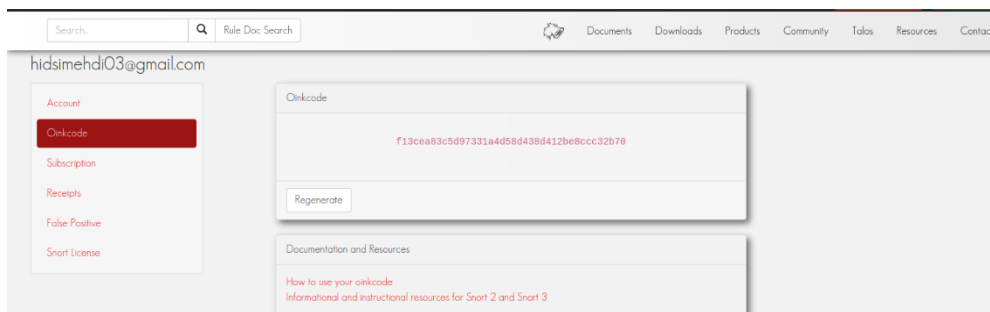
Enable OpenAppID ☒ Click to enable download of Sourcefire OpenAppID Detectors

The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.

OpenAppID Version N/A (Not Downloaded)

Figure 11 : SNORT global settings

3.1 Pour Snort oinkmaster code



Search Rule Doc Search

Documents Downloads Products Community Talos Resources Contact

hidsimehdi03@gmail.com

Account

Oinkcode

Subscription

Receipts

False Positive

Snort License

Oinkcode

f13cea83c5d97331a4d58d438d412be8ccc32b70

Regenerate

Documentation and Resources

How to use your oinkcode
Informational and instructional resources for Snort 2 and Snort 3

Figure 12 : SNORT oinkmaster code

3.2 Pour les cases cocher :

- **Enable Snort GPLv2**, pour les règles communautaires.
- **Enable ET Open**, qui sont des règles proposées par la société ET.
- **Enable OpenAppID**, éventuellement, qui est une autre société.

3.3 configurations de la mise à jour :

Pour les derniers paramètres il convient simplement de configurer l'update pour les différentes règles, c'est-à-dire le délai avant de vérifier **les mises à jour** pour les différentes règles ou pour de nouvelles :

Rules Update Settings

Update Interval

12 HOURS

Please select the interval for rule updates. Choosing NEVER disables auto-updates.

Update Start Time

00:05

Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.

Hide Deprecated Rules Categories

☐

Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.

Disable SSL Peer Verification

☐

Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

General Settings

Remove Blocked Hosts Interval

1 HOUR

Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.

Remove Blocked Hosts After Deinstall

☐

Click to clear all blocked hosts added by Snort when removing the package. Default is checked.

Keep Snort Settings After Deinstall

☒

Click to retain Snort settings after package removal.

Startup/Shutdown Logging

☐

Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

Figure 13 : SNORT global settings

4.Mise à jour des différentes règles du SNOTR :

Maintenant on clique sur l'onglet **Updates** et manuellement mettre à jour les différentes règles que nous avons cochées juste avant :

Services / Snort / Updates

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	3dc0bc9a5c3ed3eb63894fdb1f8ae14	Monday, 14-Nov-22 15:00:28 UTC
Snort GPLv2 Community Rules	a9e5168ae8dbc35b4a43ca049feb1b5a	Monday, 14-Nov-22 15:00:29 UTC
Emerging Threats Open Rules	12529ae31968ae7c33a513d387c70aca	Monday, 14-Nov-22 15:00:37 UTC
Snort OpenAppID Detectors	fba164dfe992d6022740a6b390d51765	Monday, 14-Nov-22 15:00:28 UTC
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Monday, 14-Nov-22 15:00:28 UTC
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last Update

Nov-14 2022 15:00

Result: Success

Update Rules

☒ Update Rules

Force Update

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

Manage Rule Set Log

View Log

Clear Log

Figure 14 : SNORT update

5.Configurations d'interfaces :

Après Rendons-nous donc sur **Snort interfaces** pour choisir l'interface (ou les interfaces) sur laquelle **Snort** va écouter et analyser le trafic :

5.1 Interface WAN :

Premièrement nous choisissons l'**interface WAN**, puis une courte description, et ensuite nous cochons simplement le fait d'envoyer les alertes sur le système de log interne, ce qui est toujours bien.

Services / Snort / WAN - Interface Settings

Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync

WAN Settings
WAN Categories
WAN Rules
WAN Variables
WAN Preprocs
WAN IP Rep
WAN Logs

General Settings

Enable

☒ Enable interface

Interface

WAN (em0)

Choose the interface where this Snort instance will inspect traffic.

Description

WAN

Enter a meaningful description here for your reference.

Snap Length

1518

Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings

Send Alerts to System Log

☒ Snort will send Alerts to the firewall's system log. Default is Not Checked.

System Log Facility

LOG_AUTH

Select system log Facility to use for reporting. Default is LOG_AUTH.

Figure 15 : Interfaces WAN Settings

Et enfin pour le reste nous n'allons pas nous y attarder, il s'agit de l'algorithme pour la recherche d'intrusion ainsi que les options avancées :

Detection Performance Settings

Search Method

AC-BNFA

Choose a fast pattern matcher algorithm. Default is AC-BNFA.

Split ANY-ANY

☐ Enable splitting of ANY-ANY port group. Default is Not Checked.

Search Optimize

☐ Enable search optimization. Default is Not Checked.

Stream Inserts

☐ Do not evaluate stream inserted packets against the detection engine. Default is Not Checked.

Checksum Check Disable

☐ Disable checksum checking within Snort to improve performance. Default is Not Checked.

Choose the Networks Snort Should Inspect and Whitelist

Home Net

default

View List

Choose the Home Net you want this interface to use.

Default Home Net adds only local networks, WAN IPs, Gateways, VPNs and VIPs.

Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.

External Net

default

View List

Choose the External Net you want this interface to use.

External Net is networks that are not Home Net. Most users should leave this setting at default.

Create a Pass List and add an Alias to it, and then assign the Pass List here for custom External Net settings.

Choose a Suppression or Filtering List (Optional)

Alert Suppression and Filtering

default

View List

Choose the suppression or filtering file you want this interface to use.

Custom Configuration Options

Figure 16 : Interfaces WAN Settings

Après en activer toutes les règles précédemment téléchargées en nous rendant dans **WAN Catégories**, sur **Snort Interfaces**, **WAN** en cochant l'option **Use IPS Policy** :

The screenshot shows the 'WAN Categories' configuration page. The top navigation bar includes 'Snort Interfaces', 'Global Settings', 'Updates', 'Alerts', 'Blocked', 'Pass Lists', 'Suppress', 'IP Lists', 'SID Mgmt', 'Log Mgmt', and 'Sync'. Below this, a sub-navigation bar shows 'WAN Settings', 'WAN Categories' (selected), 'WAN Rules', 'WAN Variables', 'WAN Preprocs', 'WAN IP Rep', and 'WAN Logs'. The main content area is divided into two sections: 'Automatic Flowbit Resolution' and 'Snort Subscriber IPS Policy Selection'. In the first section, 'Resolve Flowbits' is checked, and 'Auto-Flowbit Rules' has a 'View' button. In the second section, 'Use IPS Policy' is checked, and 'IPS Policy Selection' is set to 'Security'.

Automatic Flowbit Resolution

Resolve Flowbits ☒ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.
 Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

Auto-Flowbit Rules [View](#)
 Disabling auto-flowbit rules is strongly discouraged for security reasons. Auto-enabled flowbit rules that generate unwanted alerts should have their GID:SID added to the Suppression List for the interface instead of being disabled.

Snort Subscriber IPS Policy Selection

Use IPS Policy ☒ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.
 Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

IPS Policy Selection Security
 Snort IPS policies are: Connectivity, Balanced, Security or Max-Detect.
 Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file. Max-Detect is a policy created for testing network traffic through your device. This policy should be used with caution on production systems!

Figure 17 : Interface WAN catégories

5.2 Interface LAN :

Deuxièmement nous choisissons l'interface **LAN**, puis c'est la même configuration que **WAN**.

6.Activation des interfaces :

On retourne à la liste des interfaces de **Snort** pour cliquer sur **Start** :

The screenshot shows the 'Snort Interfaces' configuration page. The top navigation bar is the same as in Figure 17. Below it, a sub-navigation bar shows 'Snort Interfaces' (selected), 'Global Settings', 'Updates', 'Alerts', 'Blocked', 'Pass Lists', 'Suppress', 'IP Lists', 'SID Mgmt', 'Log Mgmt', and 'Sync'. The main content area is titled 'Interface Settings Overview' and contains a table with the following data:

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input checked="" type="checkbox"/> WAN (em0)	✓ ↺ ⊕	AC-BNFA	DISABLED	WAN	Edit Delete
<input type="checkbox"/> LAN (em1)	✓ ↺ ⊕	AC-BNFA	DISABLED	LAN	Edit Delete

At the bottom right of the table, there is a 'Delete' button. At the bottom left, there is an information icon.

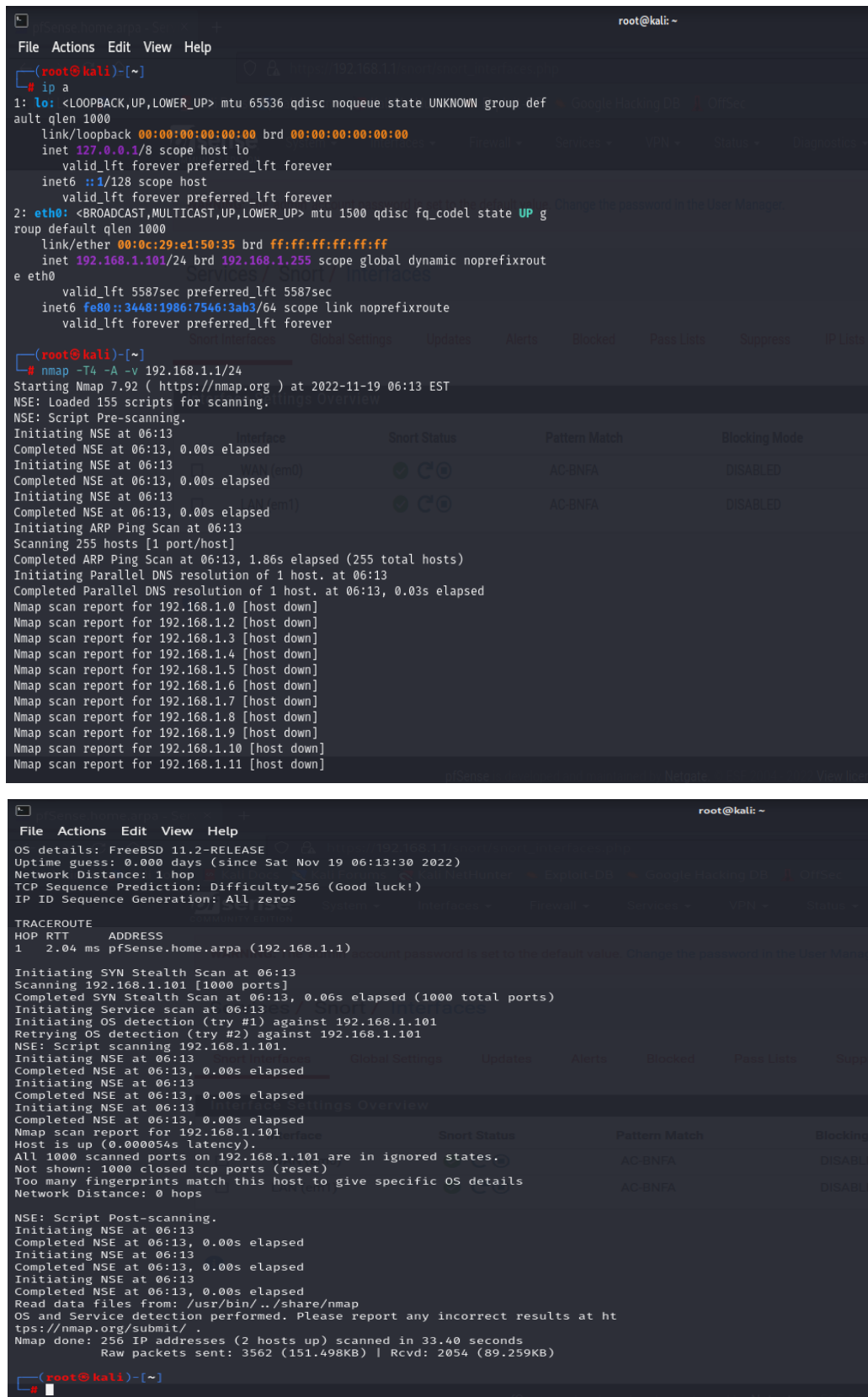
Figure 18 : Snort Interfaces

Tache 3 : Attaques pour tester :

1. Attaque sur LAN :

1.1 nmap via Kali Linux

Maintenant en peu de lancer un petit **nmap** via **Kali Linux** sur l'interface LAN pour vérifier que **Snort** fonctionne bien :



```
(root@kali)-[~]
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
    link/ether 00:0c:29:e1:50:35 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.101/24 brd 192.168.1.255 scope global dynamic noprefixrou
        valid_lft 5587sec preferred_lft 5587sec
    inet6 fe80::3448:1986:7546:3ab3/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(root@kali)-[~]
# nmap -T4 -A -v 192.168.1.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-19 06:13 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:13
Completed NSE at 06:13, 0.00s elapsed
Initiating NSE at 06:13
Completed NSE at 06:13, 0.00s elapsed
Initiating NSE at 06:13
Completed NSE at 06:13, 0.00s elapsed
Initiating ARP Ping Scan at 06:13
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 06:13, 1.86s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:13
Completed Parallel DNS resolution of 1 host. at 06:13, 0.03s elapsed
Nmap scan report for 192.168.1.0 [host down]
Nmap scan report for 192.168.1.2 [host down]
Nmap scan report for 192.168.1.3 [host down]
Nmap scan report for 192.168.1.4 [host down]
Nmap scan report for 192.168.1.5 [host down]
Nmap scan report for 192.168.1.6 [host down]
Nmap scan report for 192.168.1.7 [host down]
Nmap scan report for 192.168.1.8 [host down]
Nmap scan report for 192.168.1.9 [host down]
Nmap scan report for 192.168.1.10 [host down]
Nmap scan report for 192.168.1.11 [host down]

OS details: FreeBSD 11.2-RELEASE
Uptime guess: 0.000 days (since Sat Nov 19 06:13:30 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT ADDRESS
1 2.04 ms pfSense.home.arpa (192.168.1.1)

Initiating SYN Stealth Scan at 06:13
Scanning 192.168.1.101 [1000 ports]
Completed SYN Stealth Scan at 06:13, 0.06s elapsed (1000 total ports)
Initiating Service scan at 06:13
Initiating OS detection (try #1) against 192.168.1.101
Retrying OS detection (try #2) against 192.168.1.101
NSE: Script scanning 192.168.1.101.
Initiating NSE at 06:13
Completed NSE at 06:13, 0.00s elapsed
Initiating NSE at 06:13
Completed NSE at 06:13, 0.00s elapsed
Initiating NSE at 06:13
Completed NSE at 06:13, 0.00s elapsed
Nmap scan report for 192.168.1.101
Host is up (0.000054s latency).
All 1000 scanned ports on 192.168.1.101 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

NSE: Script Post-scanning.
Initiating NSE at 06:13
Completed NSE at 06:13, 0.00s elapsed
Initiating NSE at 06:13
Completed NSE at 06:13, 0.00s elapsed
Initiating NSE at 06:13
Completed NSE at 06:13, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/
Nmap done: 256 IP addresses (2 hosts up) scanned in 33.40 seconds
Raw packets sent: 3562 (151.498KB) | Rcvd: 2054 (89.259KB)
```

Figure 19 : Attaque sur l'interface LAN

1.2 les alertes reçus sur LAN :

Maintenant on clique sur l'onglet **Alerts** :

The screenshot shows the Snort Alerts interface. At the top, there's a breadcrumb trail: Services / Snort / Alerts. Below this is a navigation bar with tabs: Snort Interfaces, Global Settings, Updates, Alerts (selected), Blocked, Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync. The main content area is divided into three sections: Alert Log View Settings, Alert Log Actions, and Alert Log View Filter. The Alert Log View Settings section has a dropdown menu for 'Interface to Inspect' set to 'LAN (em1)', an 'Auto-refresh view' checkbox, and a text input for 'Alert lines to display' set to '250'. The Alert Log Actions section has 'Download' and 'Clear' buttons. The Alert Log View Filter section shows '1 Entries in Active Log'. Below this is a table with columns: Date, Action, Pri, Proto, Class, Source IP, SPort, Destination IP, DPort, GID:SID, and Description. The table contains one entry: 2022-11-19 11:13:33, a warning icon, priority 3, TCP, Unknown Traffic, Source IP 192.168.1.101, SPort 37626, Destination IP 192.168.1.1, DPort 80, GID:SID 119:31, and Description (http_inspect) UNKNOWN METHOD.

Figure 20 : Alerts de l'interface LAN

2. Attaque sur WAN :

En lance une attaque sur l'interface WAN :

2.1 Tester avec des sites web malveillantes :

The screenshot shows a news article titled 'Top 100 virus-infected websites exposed'. The article is dated August 20, 2009, and was first published at 12:03pm. The article text states: 'The 100 websites most affected by viruses each have about 18,000 nasties to attack net users' computers, an internet security company says.' Below the text, there is a list of websites that made the list, including 17ebook.co, aladel.net, bpwhamburgorchardpark.org, clicnews.com, dfwdiesel.net, divineenterprises.net, fantasticfilms.ru, gardensrestaurantandcatering.com, ginedis.com, gncr.org, hdvideoforums.org, hihanin.com, kingfamilyphotoalbum.com, and likaraoke.com. To the right of the list, there is a 'RELATED ARTICLE' section titled 'The internet's most dangerous celebrities'.

Figure 21 : Sites web malveillantes

2.2 Alertes sur WAN :

Maintenant on clique sur l'onglet **Alerts** :

Services / Snort / Alerts

Snort InterfacesGlobal SettingsUpdatesAlertsBlockedPass ListsSuppressIP ListsSID MgmtLog MgmtSync

Alert Log View Settings

Interface to InspectWAN (em0)Auto-refresh view250Save

Choose interface..Alert lines to display.

Alert Log Actions

DownloadClear

Alert Log View Filter

206 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2022-11-19 11:22:51	⚠	2	TCP	Potentially Bad Traffic	192.168.110.48	57107	104.18.191.9	443	137:1	(spp_ssl) Invalid Client HELLO after Server HELLO Detected
2022-11-19 09:56:14	⚠	3	TCP	Unknown Traffic	45.33.18.44	80	192.168.110.49	62594	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2022-11-19 09:56:14	⚠	3	TCP	Unknown Traffic	45.33.18.44	80	192.168.110.49	2442	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2022-11-19 09:55:12	⚠	3	TCP	Unknown Traffic	64.190.63.111	80	192.168.110.49	20688	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE
2022-11-19 09:55:11	⚠	3	TCP	Unknown Traffic	64.190.63.111	80	192.168.110.49	2784	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE

Figure 22 : Alerts de l'interface WAN