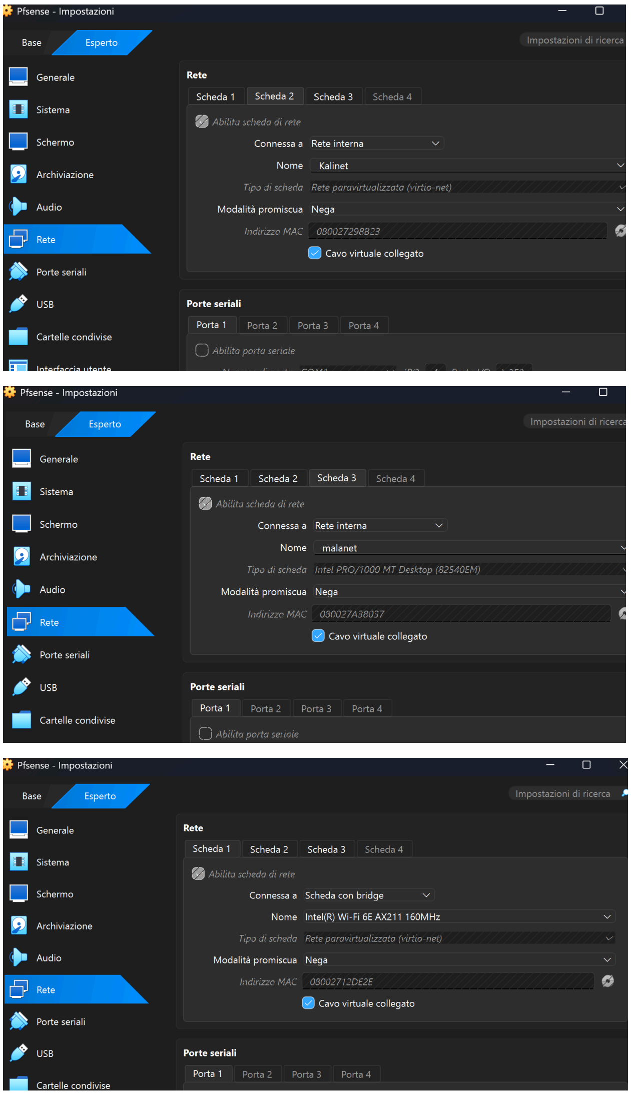
REPORT S3/L5

Creazione policy Pfsense

L’esercizio di oggi ci chiede di sperimentare l’utilizzo del firewall creando una regola: Dobbiamo bloccare l’accesso alla ***DVWA***(*Application vulnerable web application*) (della Metasploitable) dalla macchina *Kali* e ne impedisca lo scan. Ci viene richiesto, fondamentale per lo svolgimento dell’esercizio, che le macchine Kali e Metasploitable siano su reti diverse, pertanto prima di iniziare questo esercizio dovremo configurare La macchina *Pfsense* con 3 interfaccia di rete *di cui 2 già configurate per la Kali in precedenza*

Firewall: Possiamo dire che il Firewall è il nostro guardiano rete interna e mondo esterno. è un componente di sicurezza progettato per monitorare e controllare il traffico di rete entrata e uscita.

Pfsense: distribuzione software open-source progettata per essere utilizzata come un potente firewall e router



Pfsense - Impostazioni

Rete — Scheda 2

Abilita scheda di rete
Connessa a: Rete interna
Nome: Kalinet
Tipo di scheda: Rete paravirtualizzata (virtio-net)
Modalità promiscua: Nega
Indirizzo MAC: 080027298B23
☑ Cavo virtuale collegato

Porte seriali — Porta 1
□ Abilita porta seriale

Pfsense - Impostazioni

Rete — Scheda 3

Abilita scheda di rete
Connessa a: Rete interna
Nome: malanet
Tipo di scheda: Intel PRO/1000 MT Desktop (82540EM)
Modalità promiscua: Nega
Indirizzo MAC: 080027A38037
☑ Cavo virtuale collegato

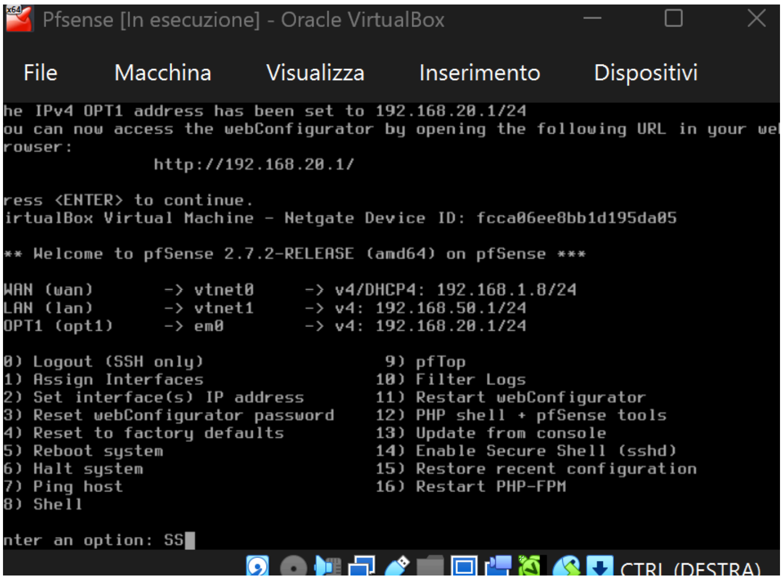
Porte seriali — Porta 1
□ Abilita porta seriale

Pfsense - Impostazioni

Rete — Scheda 1

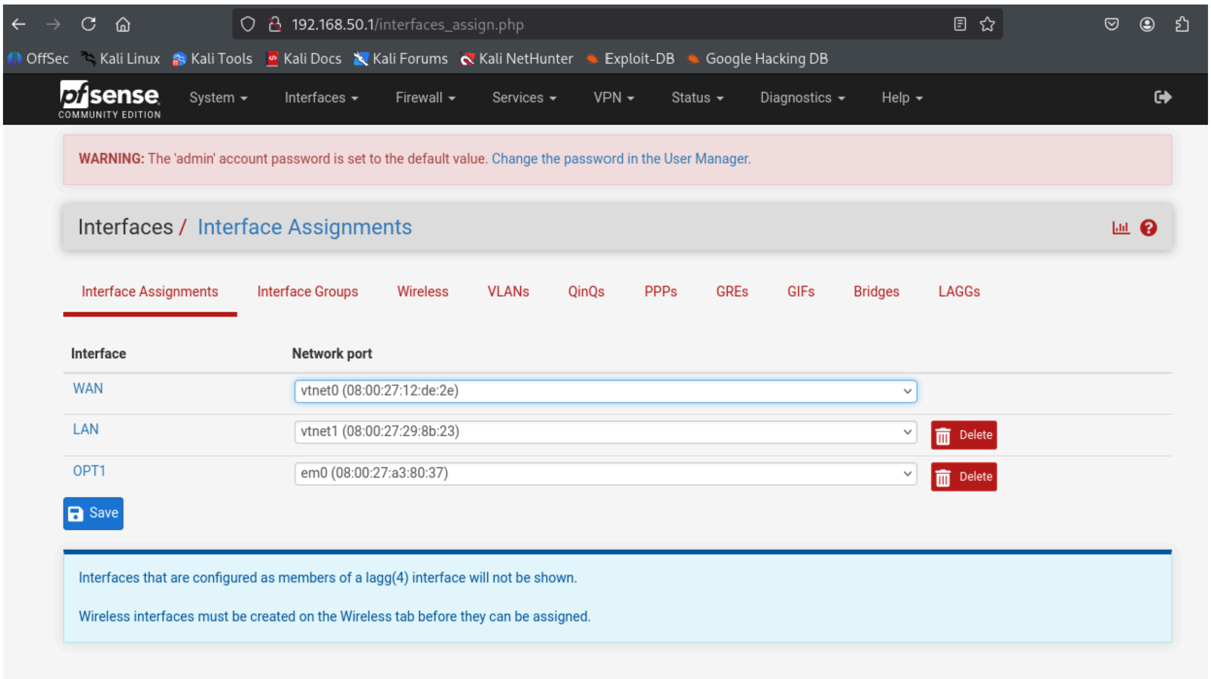
Abilita scheda di rete
Connessa a: Scheda con bridge
Nome: Intel(R) Wi-Fi 6E AX211 160MHz
Tipo di scheda: Rete paravirtualizzata (virtio-net)
Modalità promiscua: Nega
Indirizzo MAC: 08002712DE2E
☑ Cavo virtuale collegato

Configurazione Pfsense dalle impostazioni generali di Pfsense su Oracle Virtual Box



```
he IPv4 OPT1 address has been set to 192.168.20.1/24
ou can now access the webConfigurator by opening the following URL in your we
rowser:
               http://192.168.20.1/

ress <ENTER> to continue.
irtualBox Virtual Machine - Netgate Device ID: fcca06ee8bb1d195da05

** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)       -> vtnet0     -> v4/DHCP4: 192.168.1.8/24
LAN (lan)       -> vtnet1     -> v4: 192.168.50.1/24
OPT1 (opt1)     -> em0        -> v4: 192.168.20.1/24

0) Logout (SSH only)                  9) pfTop
1) Assign Interfaces                 10) Filter Logs
2) Set interface(s) IP address       11) Restart webConfigurator
3) Reset webConfigurator password    12) PHP shell + pfSense tools
4) Reset to factory defaults         13) Update from console
5) Reboot system                     14) Enable Secure Shell (sshd)
6) Halt system                       15) Restore recent configuration
7) Ping host                         16) Restart PHP-FPM
8) Shell

nter an option: SS
```

Vm di PfSense con 3 schede di rete e gli ip associati



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

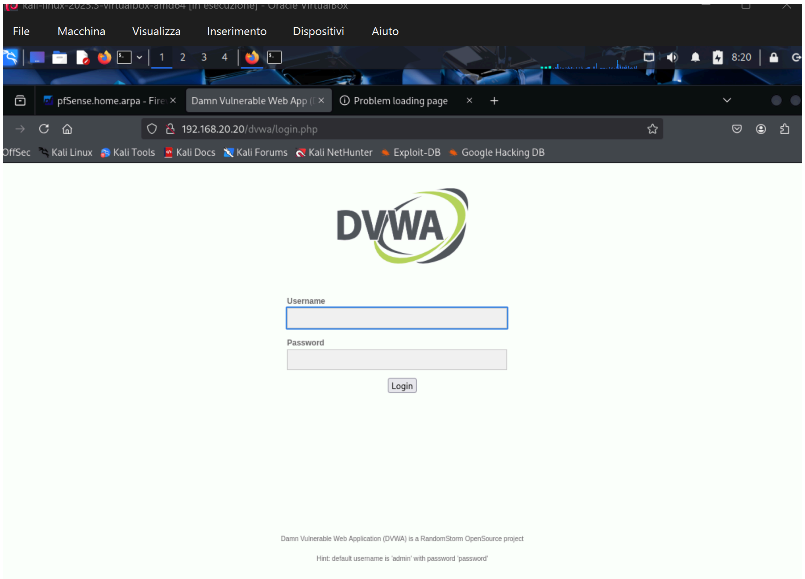
Interfaces / Interface Assignments

Interface	Network port
WAN	vtnet0 (08:00:27:12:de:2e)
LAN	vtnet1 (08:00:27:29:8b:23)
OPT1	em0 (08:00:27:a3:80:37)

Interfaces that are configured as members of a lagg(4) interface will not be shown.

Wireless interfaces must be created on the Wireless tab before they can be assigned.

Dal broswer di *Kali* andiamo su pfsense e andiamo nella sezione ***interfaces / interfaces assignments*** per impostare la configurazione di rete:

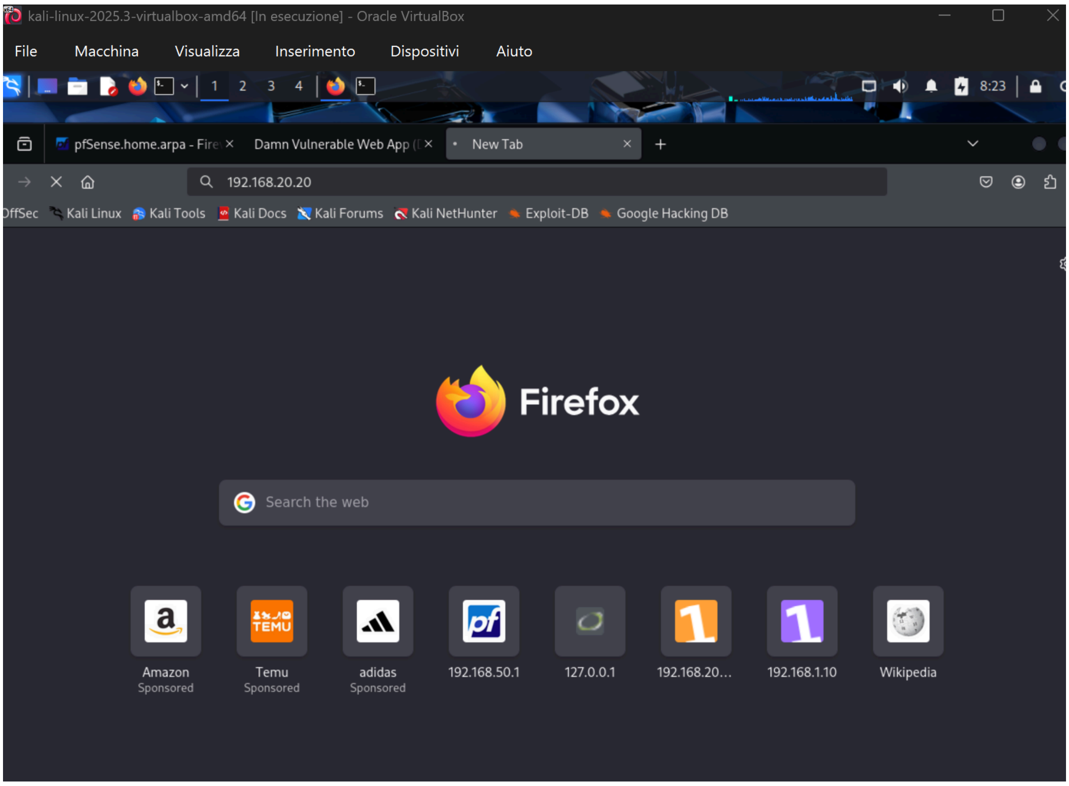


Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

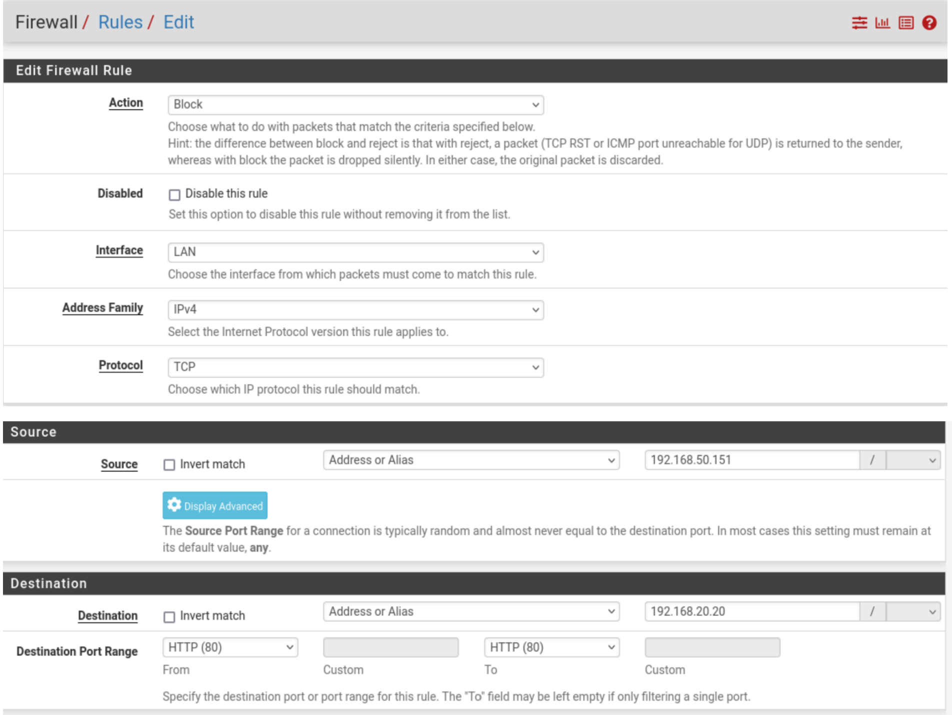
Hint: default username is 'admin' with password 'password'

Prima fase: Browser della Kali che apre la pagina servita della Metasploitable2 senza prima aver applicato la regola. La prima fase è terminata.

Seconda fase: Browser della *Kali* che non riesce più ad aprire la pagina servita dalla *Metasploitable2* dopo l'applicazione della regola (***come vedete in alto la rotellina è in fase di caricamento***)



Impostazione regola firewall:



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 | Address or Alias | 192.168.50.151 | /

Display Advanced

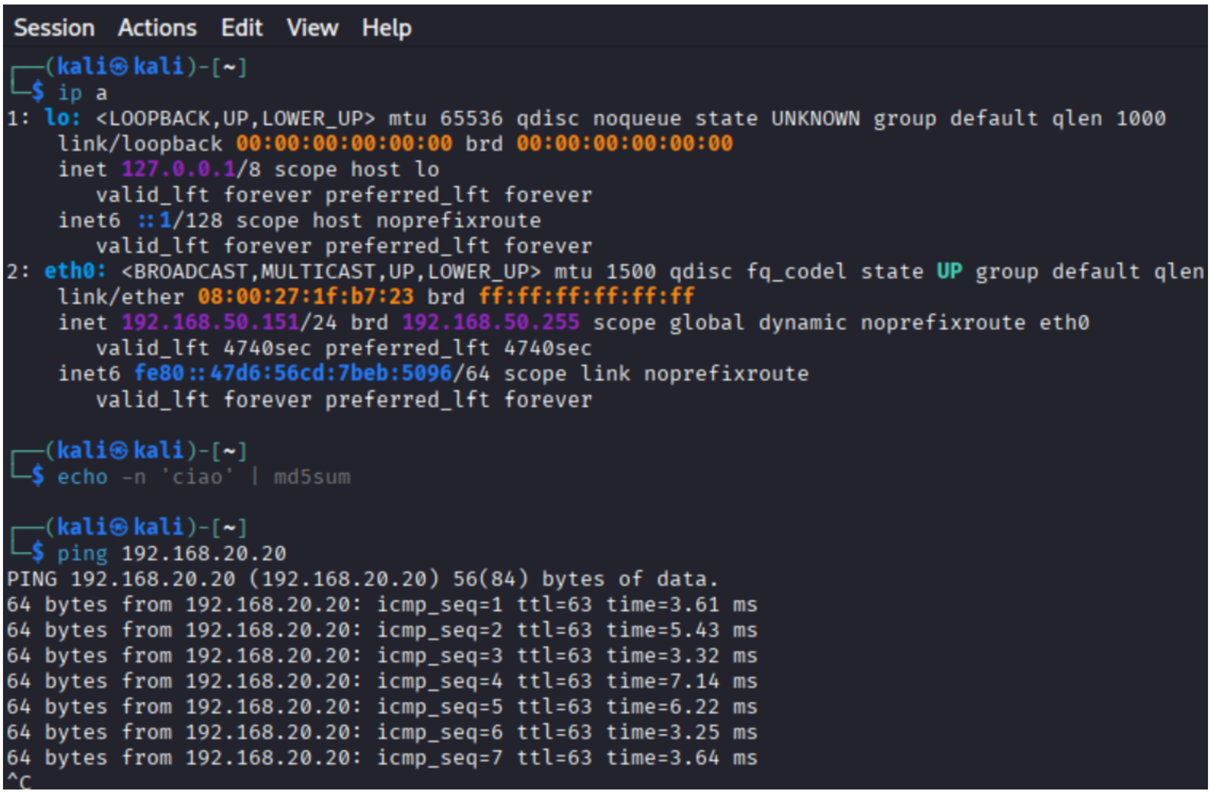
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination: □ Invert match | Address or Alias | 192.168.20.20 | /

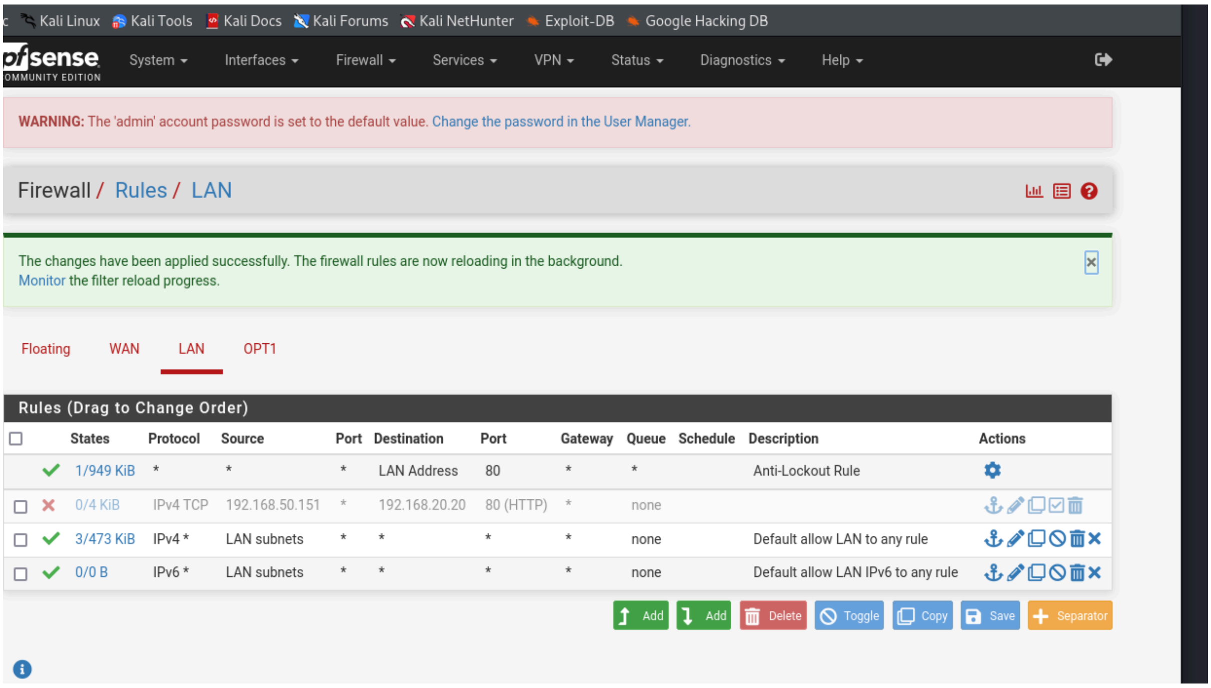
Destination Port Range: HTTP (80) From | Custom | HTTP (80) To | Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Nota: nella Pfsense una volta configurato bisogna scorrere giù e cliccare “Save” dopodiché, in alto a destra, bisogna cliccare “Apply Changes”.



```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.151/24 brd 192.168.50.255 scope global dynamic noprefixroute eth0
       valid_lft 4740sec preferred_lft 4740sec
    inet6 fe80::47d6:56cd:7beb:5096/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ echo -n 'ciao' | md5sum

┌──(kali㉿kali)-[~]
└─$ ping 192.168.20.20
PING 192.168.20.20 (192.168.20.20) 56(84) bytes of data.
64 bytes from 192.168.20.20: icmp_seq=1 ttl=63 time=3.61 ms
64 bytes from 192.168.20.20: icmp_seq=2 ttl=63 time=5.43 ms
64 bytes from 192.168.20.20: icmp_seq=3 ttl=63 time=3.32 ms
64 bytes from 192.168.20.20: icmp_seq=4 ttl=63 time=7.14 ms
64 bytes from 192.168.20.20: icmp_seq=5 ttl=63 time=6.22 ms
64 bytes from 192.168.20.20: icmp_seq=6 ttl=63 time=3.25 ms
64 bytes from 192.168.20.20: icmp_seq=7 ttl=63 time=3.64 ms
^C
```

Terza Fase: Adesso dal terminale della Kali effettuiamo un ping per vedere se raggiunge la Metasploitable2.
Test riuscito (Dopo applicazione della regola)



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

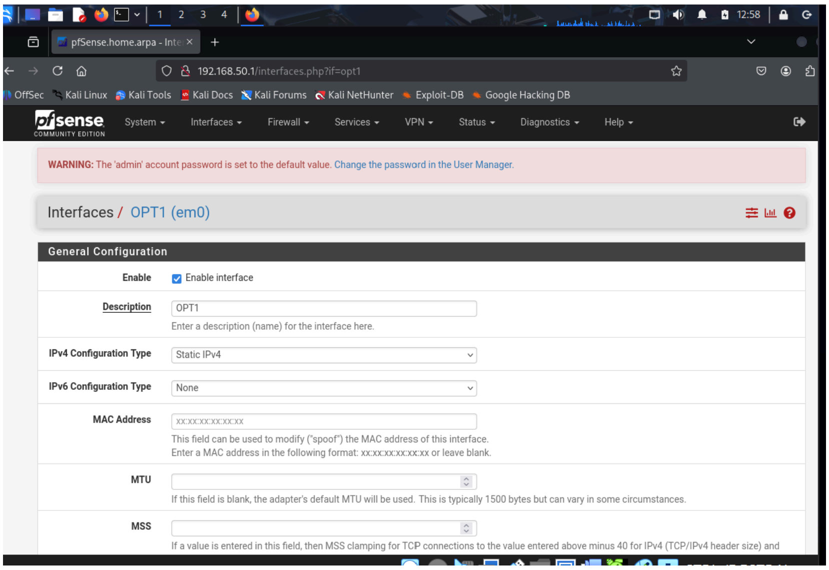
Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	1/949 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙
□	✗	0/4 KiB	IPv4 TCP	192.168.50.151	*	192.168.20.20	80 (HTTP)	*	none			
□	✓	3/473 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Interfaccia generale delle regole



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Interfaces / OPT1 (em0)

General Configuration

Enable ☑ Enable interface

Description OPT1
Enter a description (name) for the interface here.

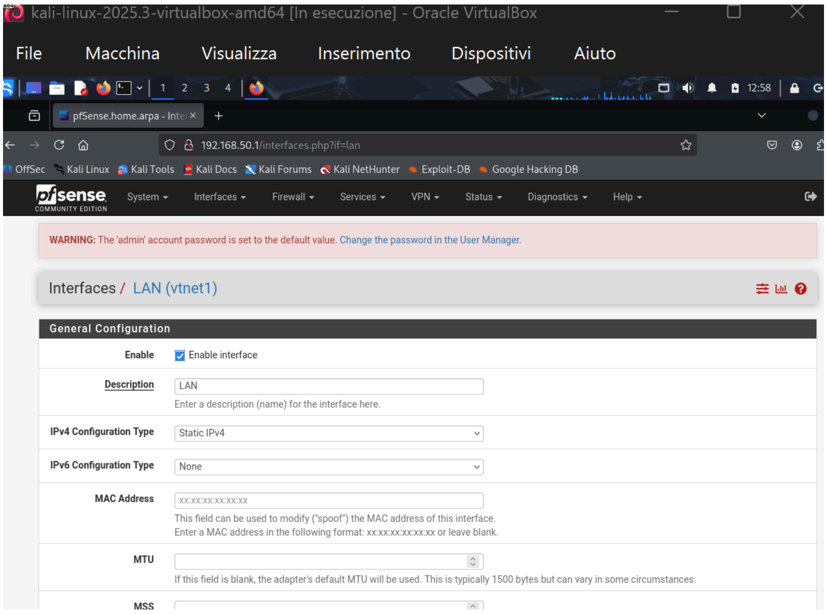
IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Interfaces / LAN (vtnet1)

General Configuration

Enable ☑ Enable interface

Description LAN
Enter a description (name) for the interface here.

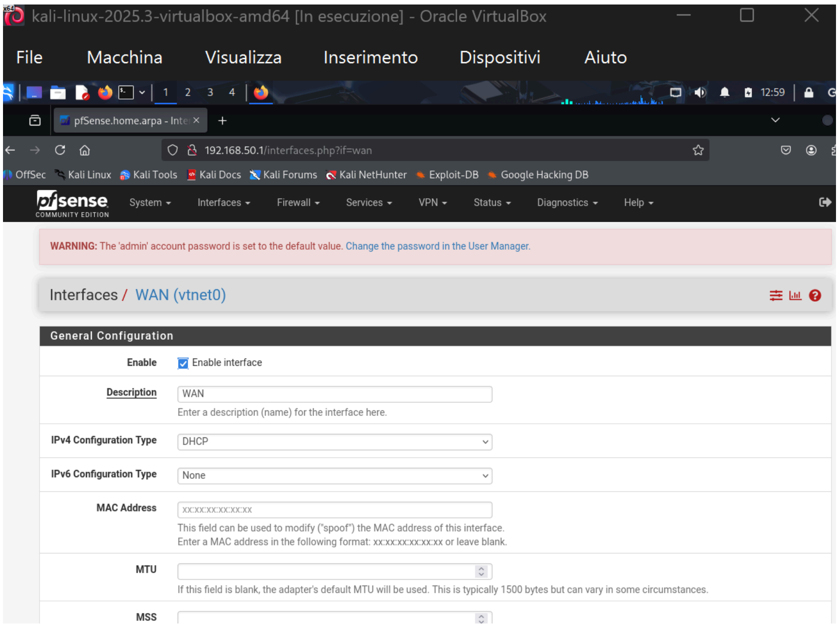
IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Interfaces / WAN (vtnet0)

General Configuration

Enable ☑ Enable interface

Description WAN
Enter a description (name) for the interface here.

IPv4 Configuration Type DHCP

IPv6 Configuration Type None

MAC Address xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS