

TEST S3/L5

CONSEGNA:

Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan.

Per prima cosa ho acceso il server di pf sense, configurato in precedenza.

Poi ho aperto metasploitable e ho configurato il nuovo indirizzo di rete.

```
GNU nano 2.0.7      File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.2.100
    netmask 255.255.255.0
    gateway 192.168.2.1

[ Read 14 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text ^T To Spell
```

Con il comando `sudo nano /etc/network/interfaces` ho configurato un ip statico (prima in dhcp), ovviamente una rete diversa da kali.

Kali:

IP: 192.168.1.5

Subnet: 255.255.255.0

Gateway: 192.168.1.1

Metasploitable:

IP: 192.168.2.100

Subnet: 255.255.255.0

Gateway: 192.168.2.1

```
[ Read 14 lines ]



msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f8:62:dc
          inet addr:192.168.2.100  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fd00::a00:27ff:fe8:62dc/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe8:62dc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:158 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4486 (4.3 KB)  TX bytes:18721 (18.2 KB)
          Interrupt:9 Base address:0xd020

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:188 errors:0 dropped:0 overruns:0 frame:0
          TX packets:188 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:63409 (61.9 KB)  TX bytes:63409 (61.9 KB)



msfadmin@metasploitable:~$
```

Salvato il file modificato ho riavviato i servizi di rete con il comando
sudo /etc/init.d/networking restart
dopo ho verificato che i cambiamenti siano stati applicati con ifconfig.

A questo punto siamo pronti a iniziare a configurare pfsense dalla dashboard web.






 COMMUNITY EDITION 


WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Interfaces / **Interface Assignments**  

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges

LAGGs

Interface	Network port
WAN	em0 (08:00:27:87:af:d1) 
LAN	vtnet0 (08:00:27:48:59:e3)  
LAN2	VLAN 10 on vtnet0 - lan  



Per prima cosa ho creato una nuova LAN per metasploitable,ciò è stato possibile creando una nuova VLAN e configurandola in LAN(no WAN).

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

192.168.1.5

/



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

Address or Alias

192.168.2.100

/

Destination Port Range

HTTP (80)

From

Custom

HTTP (80)

To

Custom

Dopodiche ho iniziato la configurazione del firewall su LAN1(kali)Ho bloccato le comunicazioni da kali alla DVWA di metasploitable sulla porta 80

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

Any

Choose which IP protocol this rule should match.

Source

Source☐ Invert
match

Address or Alias

192.168.1.5

/

v

Destination

Destination☐ Invert
match

Address or Alias

192.168.2.100

/

v

Un'aggiunta mia, ho scelto il protocollo any e ho bloccato tutte le comunicazioni (per il test, sapendo che non avevo bisogno di nessun tipo di comunicazione con la macchina).

Floating WAN LAN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1/1.55 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	192.168.1.5	*	192.168.2.100	*	*	none			
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	192.168.1.5	*	192.168.2.100	80 (HTTP)	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Le rules del firewall della LAN1.
Aggiunte con la funzione Add on top

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

LAN2

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

Any

Choose which IP protocol this rule should match.

Source

Source☐ Invert
match

Address or Alias

192.168.1.5

/

▼

Destination

Destination☐ Invert
match

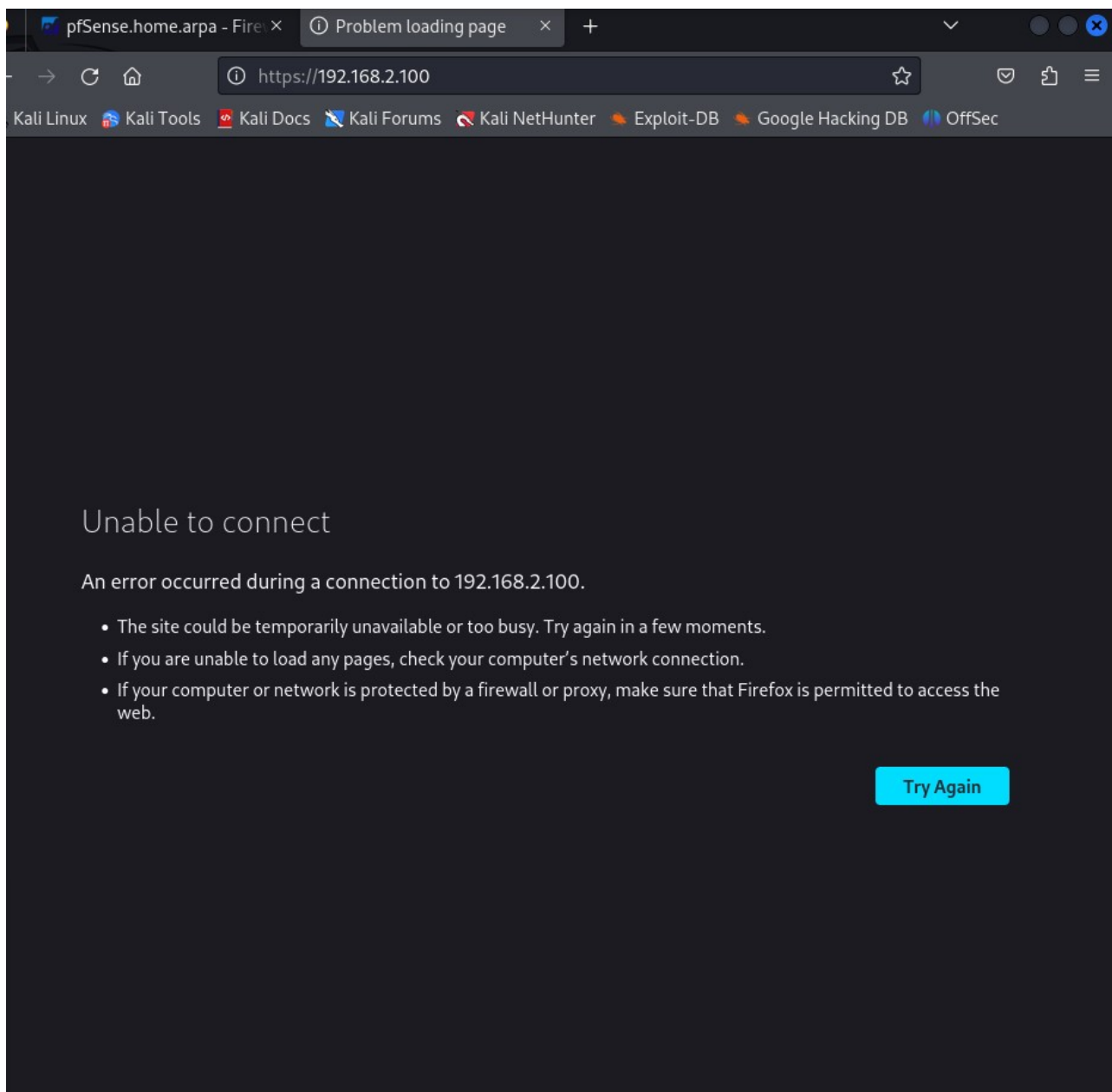
LAN2 subnets

Destination Address

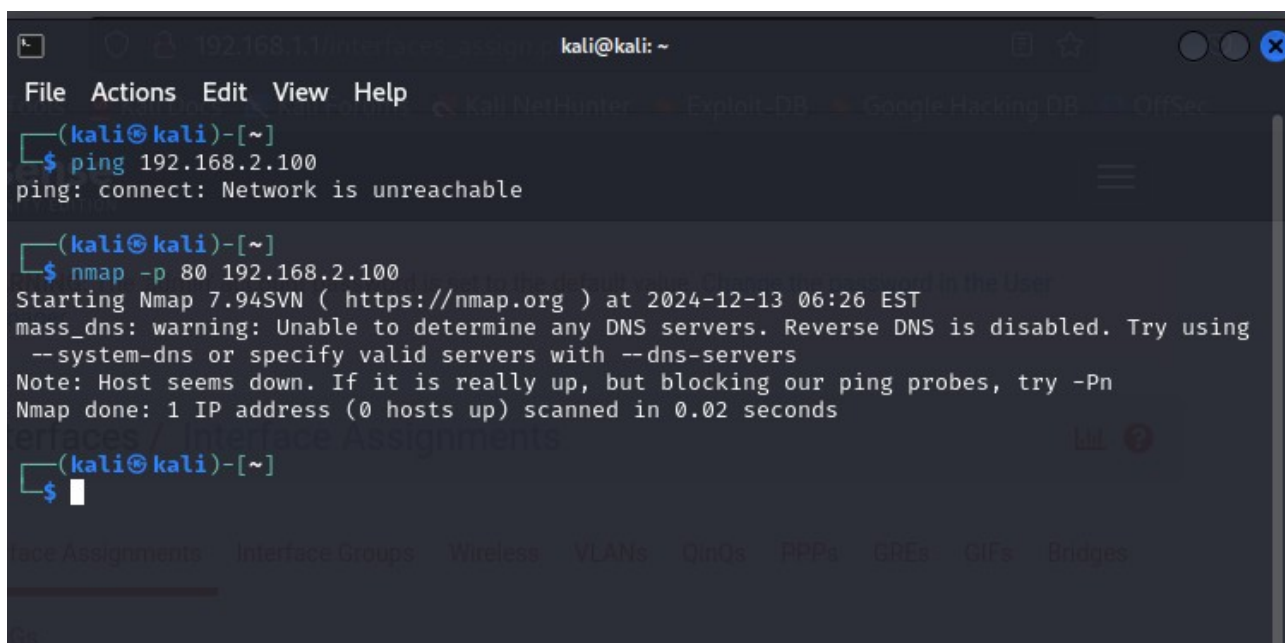
/

▼

Dopo aver abilitato la LAN2(linea 192.168.2.0/24) l'ho configurata in modo da non ricevere comunicazioni dalla linea 192.168.1.0/24(kali).



Prova di collegamento tramite browser bloccata dal firewall.



Prova di ping a metasploitable fallita(correttamente)

prova di raggiungimento della DVWA sulla porta 80 fallita(correttamente)