

Traccia

Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete

Soluzione

Facciamo un primo test sulle due macchine, rispettivamente **kali** e **metasploitable**, controllando che esse si trovino sulla stessa rete mediante comando **ipconfig** e possano comunicare tra loro mediante comando **ping**.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:05:0a:68
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
```

Figura1: Ip di metasploitable

La macchina metasploitable avrà **ipaddress**: 192.168.56.101 con **subnetmask**: 255.255.255.0.

```
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.104  netmask 255.255.255.0  broadcast 192.168.56
```

Figura2: Ip di kali

La macchina Kali avrà **ipaddress**: 192.168.50.10 con **subnetmask**: 255.255.255.0.

E verifichiamo mediante **ping** che le 2 macchine siano in grado di comunicare tra loro.

```
(kali㉿kali)-[~]
$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=0.259 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.235 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.259 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.258 ms
^C
 192.168.56.101 ping statistics ---
 4 packets transmitted, 4 received, 0% packet loss, time 3086ms
 rtt min/avg/max/mdev = 0.235/0.252/0.259/0.010 ms
```

Figura3: Ping di verifica tra le 2 macchine

Controlleremo anche che sia possibile effettuare l'accesso da kali sulla DVWA su METASPLOITABLE. Andando ad inserire come url l'indirizzo ip della nostra macchina metasploitable.

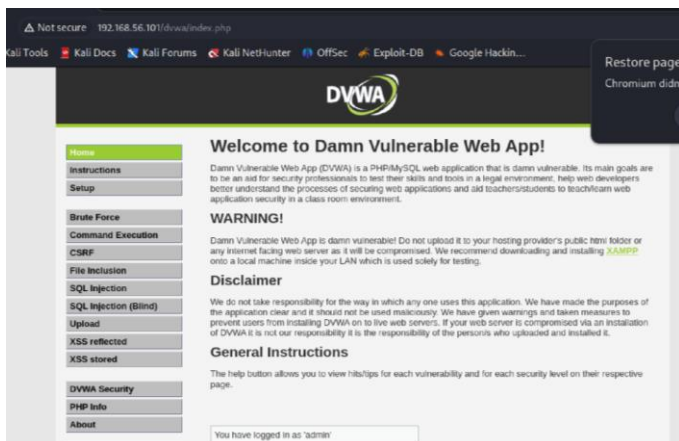


Figura 4: Verifichiamo l'accesso alla DVWA da kali su meta, nella medesima rete

Ai fini dell'esercizio è necessario che i due host siano su reti diverse, per farlo vado manualmente a modificare l'ip statico della macchina kali assegnando un nuovo ip: 192.168.1.10, lasciando invariato quello della macchina metasploitable, ora le macchine non comunicheranno più tra loro e saranno appartenenti a due network differenti.

Figura 4

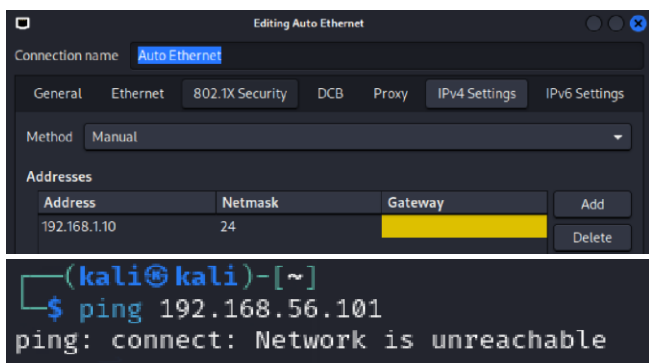


Figura 5: Modifica manuale dell'IP di kali, e test di ping con metasploitable.

Andiamo adesso ad avviare il firewall pfSense con **ip lan**: 192.168.1.1/24 e da kali accediamo al **web-configurator** inserendo nella barra degli url questo indirizzo. Sarà necessario adesso aggiungere la nuova interfaccia per la gestione delle due reti di appartenenze dei due differenti host.

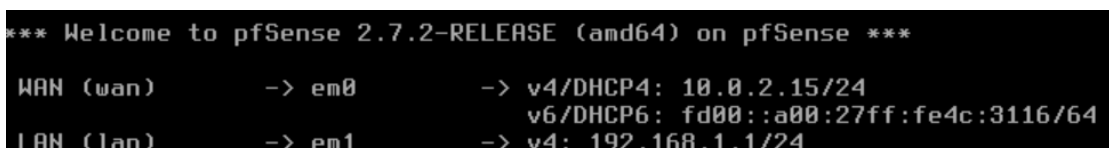
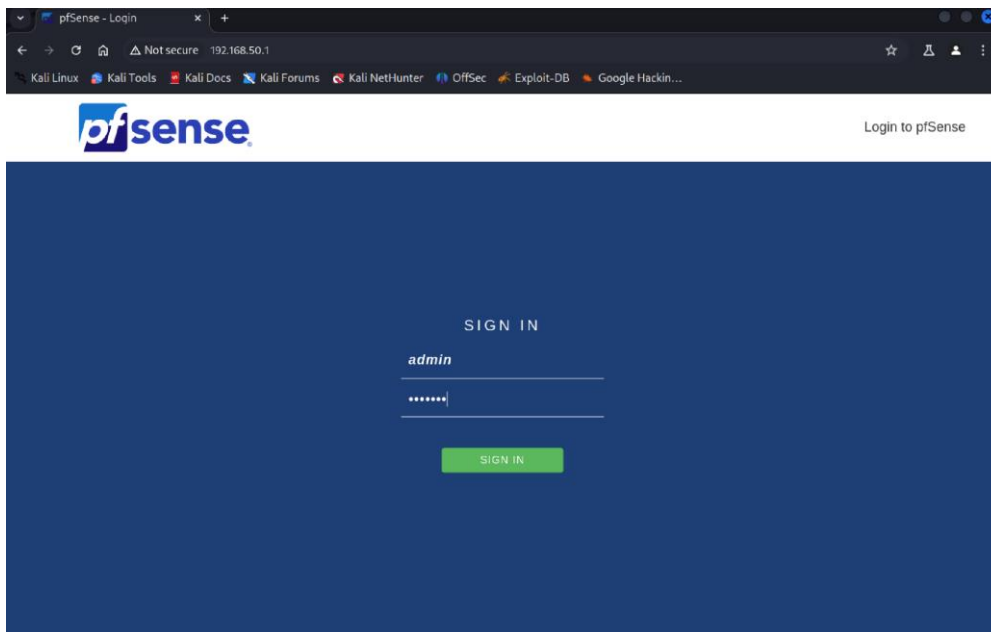


Figura5: Avvio del firewall, 192.168.1.1



Procedo quindi con l'aggiunta della nuova interfaccia alla quale assegnerò ip statico del gateway della macchina **metasploitable**, in questo caso **ip: 192.168.56.1**. **Figura 6**

Interfaces			
WAN	↑	1000baseT <full-duplex>	10.0.2.15 fd00::a00:27ff:fe4c:3116
LAN	↑	1000baseT <full-duplex>	192.168.1.1
LAN_META	↑	10Gbase-T <full-duplex>	192.168.56.1

Figura 6: Aggiungo manualmente la nuova interfaccia dal web configurator di pfsense.

Dobbiamo adesso a gestire le regole per il traffico tra i due host, in particolare dobbiamo consentire il traffico sulla nuova interfaccia creata con delle regole di “pass” su tutte le subnet della nuova interfaccia, come source inseriremo le subnet della rete e come destinazione “any”. **Figura 7**

Per farlo procederemo accedendo alle sezione firewall in alto e successivametne rules.

Edit Firewall Rule

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

Address Family
Select the Internet Protocol version this rule applies to.

Protocol
Choose which IP protocol this rule should match.

Source
☐ Invert match /

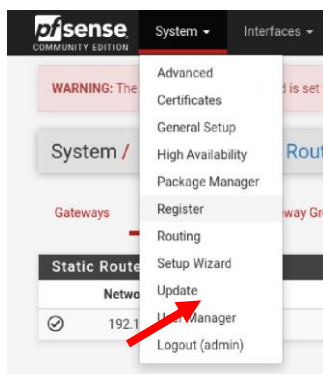
Destination
☐ Invert match /

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 *	LAN_META subnets	*	*	*	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv6 TCP	LAN_META subnets	*	*	*	*	none			

Figura 7: Aggiungo la regola per consentire il traffico.

infine abilitiamo il routing sulla nuova interfaccia da **system→routing→static routes** e aggiungendo la rete riferita alla nuova interfaccia.



Static Routes				
Network	Gateway	Interface	Description	Actions
<input checked="" type="checkbox"/> 192.168.56.0/32	WAN_DHCP - 10.0.2.2	WAN		
Add				

Figura 8: Viene abilitato il routing sulla nuova interfaccia per consentire la comunicazione.

Possiamo ora testare, con il comando **ping**, che le due macchine siano in grado di comunicare pur appartenendo a due reti diverse, proviamo dalla macchina kali pingando la macchina metasploitable.

```
(kali@kali) ~
$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data:
64 bytes from 192.168.56.101: icmp_seq=1 ttl=255 time=0.441 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=255 time=0.400 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=255 time=0.275 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=255 time=0.438 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=255 time=0.431 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=255 time=0.409 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=255 time=0.407 ms
^C
--- 192.168.56.101 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6123ms
rtt min/avg/max/mdev = 0.275/0.400/0.441/0.053 ms
```

Figura 9: Ping di test.

Il ping è riuscito quindi le due macchine comunicano tra loro. Vogliamo ora creare una regola che blocchi il traffico verso la **DVWA** su **metasploitable** da kali. Per farlo aggiungeremo una regola che avrà come sorgente la macchina **kali** come destinazione **meta** e la porta 80 o l'indirizzo specifico da bloccare, **Figura 10**. Andremo successivamente a fare un test per verificare che effettivamente inserendo su un browser di kali l'url della macchina meta/dvwa non si possa fare più effettuare l'accesso a questa poichè il traffico sarà bloccato. **Figura 11**

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	<input type="checkbox"/> 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	<input type="checkbox"/> Invert match	LAN address	Source Address
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	<input type="checkbox"/> Invert match	LAN_META address	Destination Address
Destination Port Range	HTTP (80)	HTTP (80)	

Figura 10: Regola per il blocco all'accesso alla DVWA.

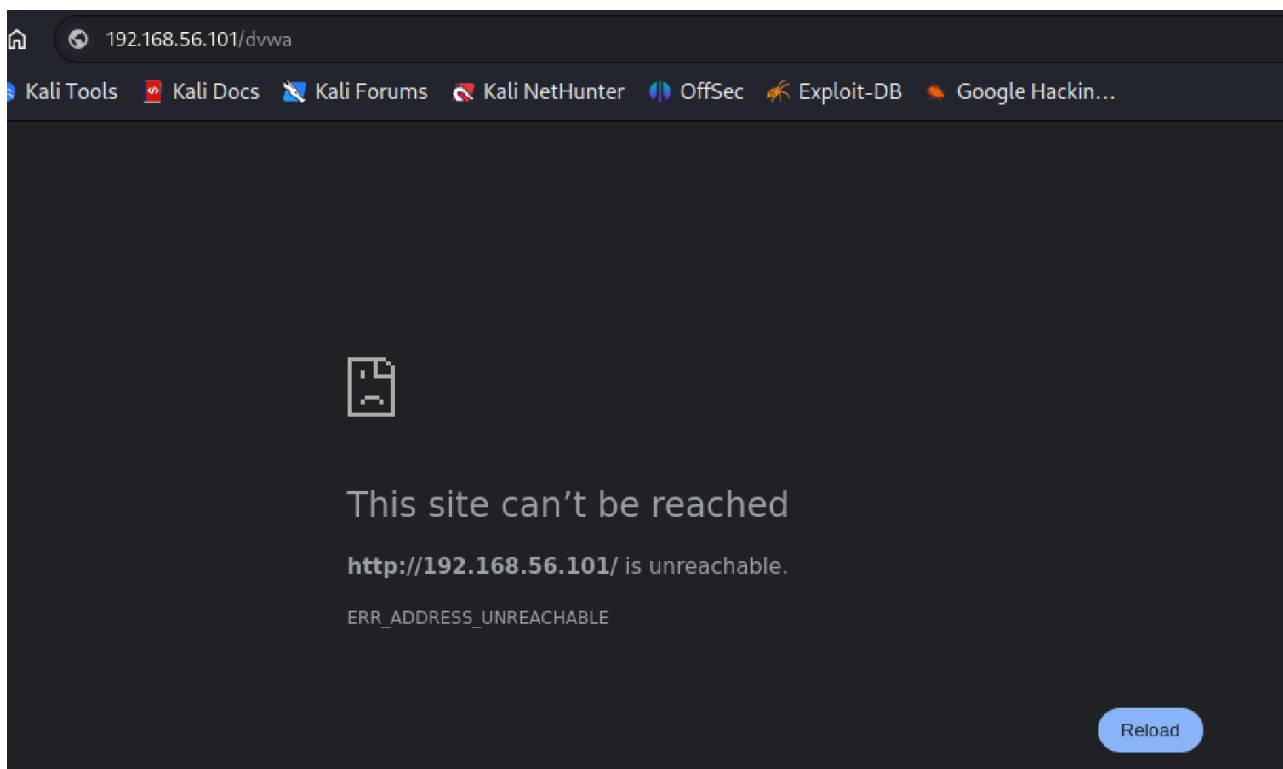


Figura 11: Test di accesso alla DVWA

ESERCIZIO BONUS

Impostare una regola che blocchi il telnet da kali a metasploitable

SOLUZIONE

Ricordiamo che il telnet utilizza la porta 23, analogamente a quanto visto prima andremo ad aggiungere sul pfsense una nuova regola di blocco specifica su questa porta. In interface andremo a impostare la lan di kali, su source la lan di kali e su destination quella di metasploitable specificando la porta **Telnet(23)** e protocollo **Tcp**.

Edit Firewall Rule

Action

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

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

Address Family

Select the Internet Protocol version this rule applies to.

Protocol

Choose which IP protocol this rule should match.

Source

☐ Invert match /

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

☐ Invert match /

Destination Port Range

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	LAN address	*	LAN_META address	80 (HTTP)	*
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	LAN address	*	LAN_META address	23 (Telnet)	*

Figura 12: Regola di blocco telnet.