

PROGETTO S3L5

Gianluca Barella

SCOPO: Creare una regola firewall che blocchi l'accesso alla DVWA

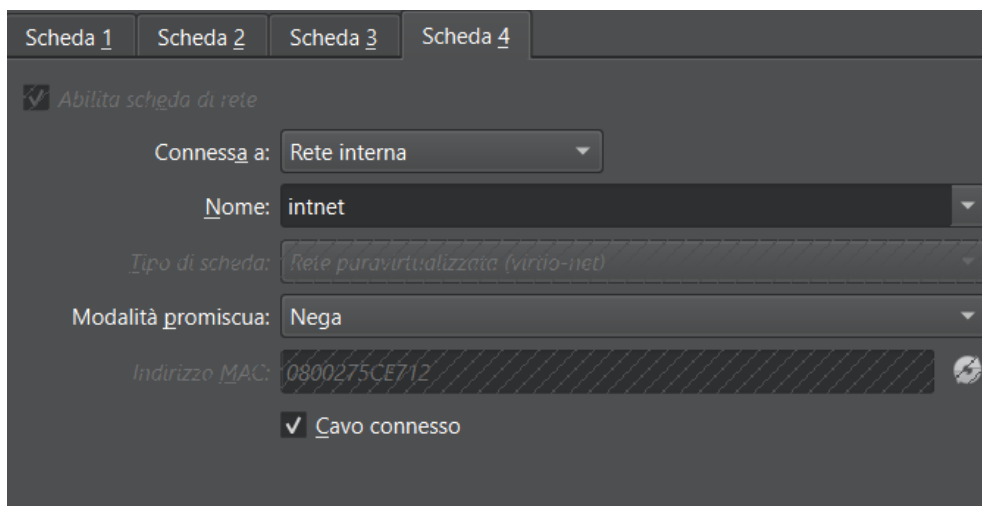
Avremo bisogno di tre macchine virtuali: Kali, Metasploitable e Pfsense.

Possiamo suddividere il progetto in tre punti:

- 1) Creazione interfaccia di rete su Pfsense
- 2) DVWA su Metasploitable
- 3) Creazione regola di firewall su Kali

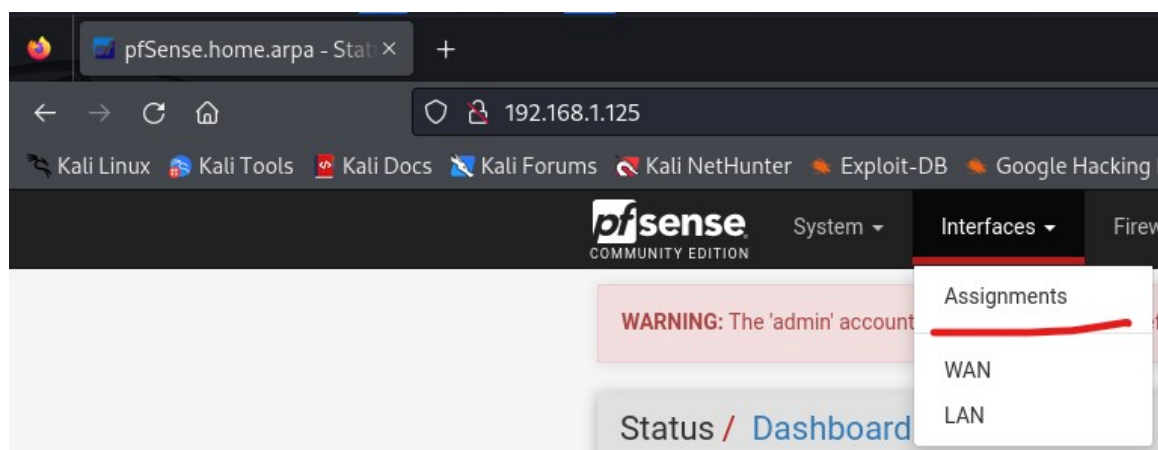
1)

Dal menù "Impostazioni" di Pfsense nella voce "Rete" aggiungiamo una scheda di rete interna per creare un'interfaccia di rete per Metasploitable.





Una volta fatto questo si avvia Kali e si digita sul Browser l'IP di Pfsense, nel nostro caso è 192.168.1.125 e si entra digitando le credenziali di default "admin" e "pfsense" nella pagina che uscirà.

Ora, dal menù "Interfaces" si clicca sulla voce "Assignments" come mostrato in figura:



Qui si vedranno tutte le schede di rete, se si vuole aggiungerne altre basterà premere il pulsante “Add”

Interface	Network port	
WAN	em0 (08:00:27:fc:40:98)	
LAN	vtnet0 (08:00:27:09:a3:9a)	 Delete
Available network ports:	vtnet1 (08:00:27:81:6e:ec)	 Add

Una volta aggiunta la rete si configura la LAN per Metasploitable cliccando sopra il nome dell'interfaccia, si imposta IP statico in questo caso viene usato “192.168.2.125/24” per avere una rete diversa rispetto a quella di Kali.

General Configuration

Enable

☒ Enable interface

Description

LAN_meta

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xxxxxxxxxxxx

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxx: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 minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex

Default (no preference, typically autoselect)

Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address

192.168.2.125

/ 24

Fatto ciò si può accendere Metasploitable per la DVWA

2)

Avviata la macchina di Metasploitable si accede digitando l'utente e la password di default "msfadmin" così facendo si può iniziare a scrivere da terminale.

Ora si configura l'IP di Metasploitable, per farlo si esegue il comando "sudo nano /etc/network/interfaces" facendo così si apre un file, qui andremo a cambiare eth0 e gli forniremo un indirizzo IP statico e un gateway, alla fine nel file sarà scritto così:

```
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

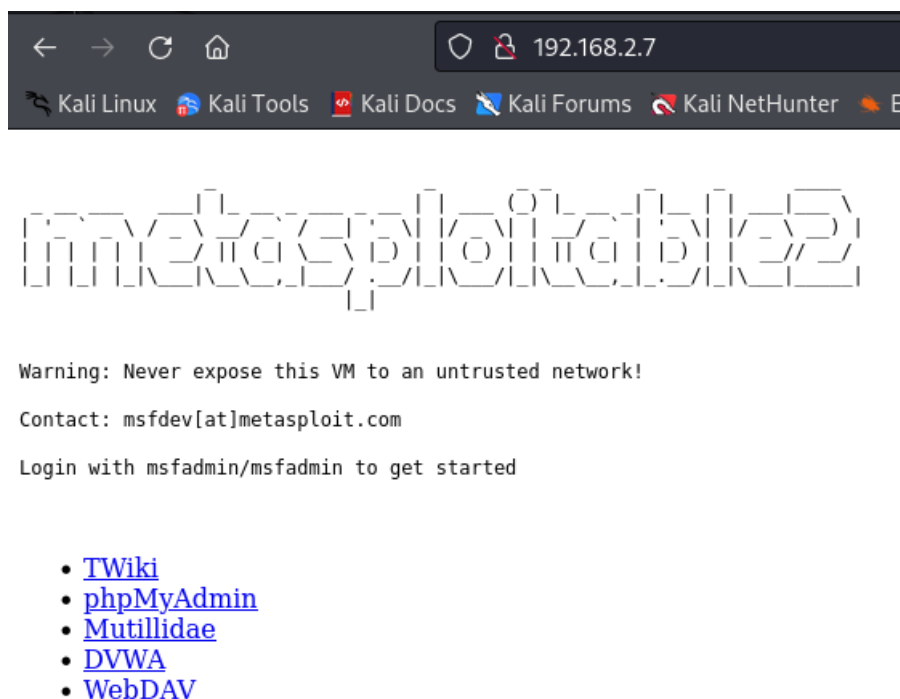
# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.2.7
    netmask 255.255.255.0
    gateway 192.168.2.125
```

in "address" mettiamo un IP che sia nella stessa rete interna di PfSense, come gateway l'indirizzo IP di PfSense 192,168,2,125, fatto questo si salva il file, si riavvia la macchina e si usa il comando "ifconfig" per vedere se l'indirizzo IP è stato configurato correttamente:

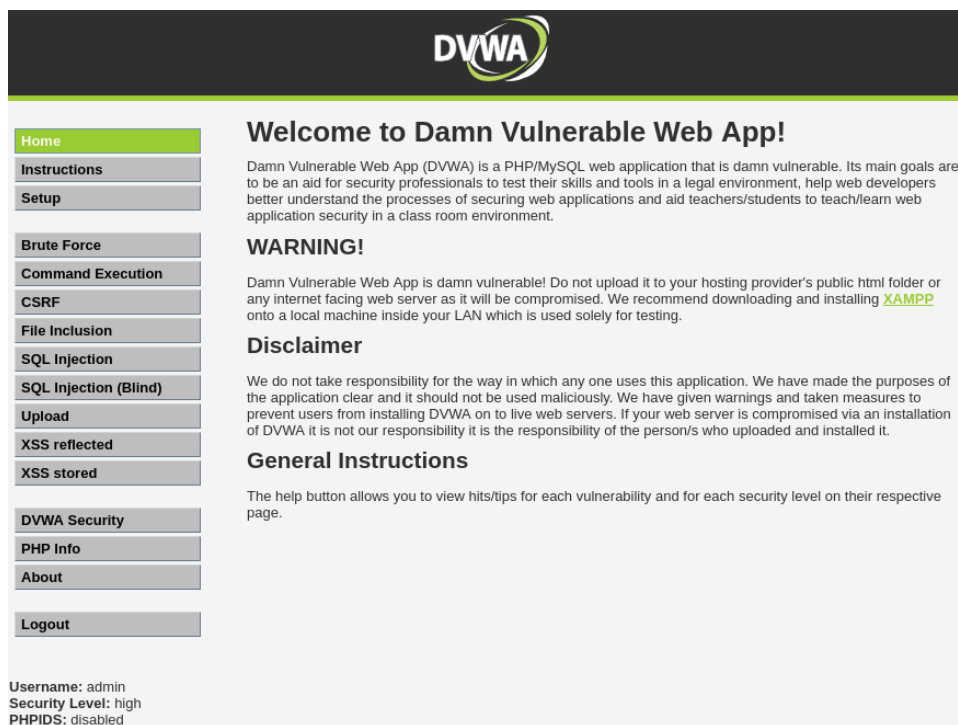
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:fe:b0:fa
          inet addr:192.168.2.7  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe:b0fa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:2954 (2.8 KB)
          Base address:0xd020  Memory:f0200000-f0220000
```

3)

Per prima cosa testiamo se da Kali riesco a raggiungere Metasploitable digitando sul browser l'indirizzo IP 192,168,2,7



Cliccando su DVWA e inserendo le credenziali “admin” “password” si entra nella web app.



Ora bisogna creare la regola di firewall e bloccare a Kali l'accesso alla DVWA, per farlo bisogna premere sul menù "Firewall" voce "Rules" e clicchiamo il tasto "Add".

Qui si aprirà una finestra per selezionare le varie impostazioni della regola, alla fine si imposterà la regola come la figura successiva:

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_META
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 192.168.2.7 /

Destination

Destination ☐ Invert match Address or Alias 192.168.1.5 /

Specificatamente:

- Action: Block perché vogliamo bloccare e scartare tutti i pacchetti, senza necessità di ritomarli al mittente (come invece fa Reject)
- Interface: LAN_META perché è la rete da cui arriveranno i pacchetti da bloccare
- Address Family: IPv4 perché l'IP impostato su Metasploitable è di quel tipo
- Protocol: Any perché vogliamo bloccare qualsiasi tipo di pacchetto indipendentemente dal tipo di protocollo utilizzato
- Source: Address or Alias 192.168.2.7 cioè andiamo a bloccare specificatamente i pacchetti che hanno come fonte quell'indirizzo che è appunto l'indirizzo della DVWA
- Destination: Address or Alias 192.168.1.5 per far sì che vengano bloccati i pacchetti della sorgente specificatamente diretti all'IP di Kali

Così facendo si crea la regola che impedirà a Kali di ricevere i pacchetti da Metasploitable

ESERCIZIO BONUS: impostare una regola su Pfsense per bloccare le comunicazioni da Kali verso Metasploitable tramite telnet

Per eseguire l'esercizio bonus si dovrà implementare una regola questa volta nella rete LAN_META, quindi sempre da "Firewall">"Rules" si clicca "Add" nella LAN designata e si completa la regola:

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 /
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 192.168.2.7 /

Destination Port Range Telnet (23) 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.

Specificatamente:

- Action: Block perché vogliamo bloccare e scartare tutti i pacchetti
- Interface: LAN perché è la rete in cui si trova Kali
- Address Family: IPv4 perché l'IP impostato è di quel tipo
- Protocol: TCP perché Telnet si basa su una rete TCP/IP
- Source: Address or Alias 192.168.1.5 che sarebbe l'indirizzo IP di Kali
- Destination: Address or Alias 192.168.2.7 che sarebbe l'indirizzo IP di Metasploitable
- Destination Port Range: Telnet (23) cioè si va a bloccare la porta 23 che è dove passano le comunicazioni Telnet