

S3L5

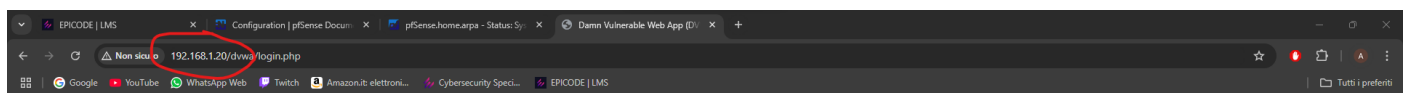
Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan.

Prima di tutto avvio metasploitable2 per ottenere il suo indirizzo IP e mi collego dalla mia macchina fissa per provare a collegarmi a DVWA.

```
metasploitable2 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
http://help.ubuntu.com/
do mail.
nsfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:6e:fa:f8
          inet addr:192.168.1.20  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6e:faf8/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:55 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5848 (5.7 KB)  TX bytes:7179 (7.0 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:16384  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

nsfadmin@metasploitable:~$
nsfadmin@metasploitable:~$
nsfadmin@metasploitable:~$
```



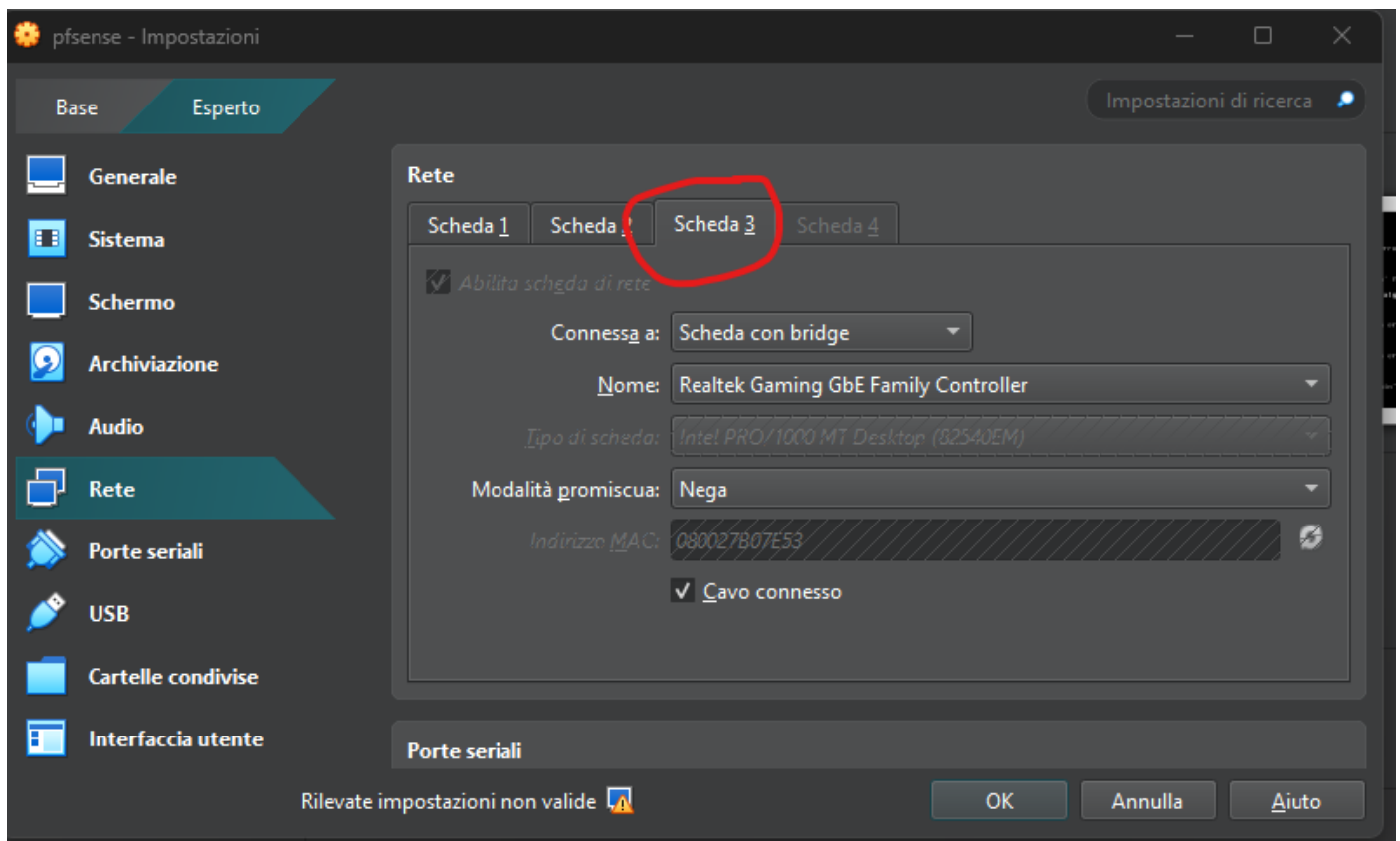
Username

Password

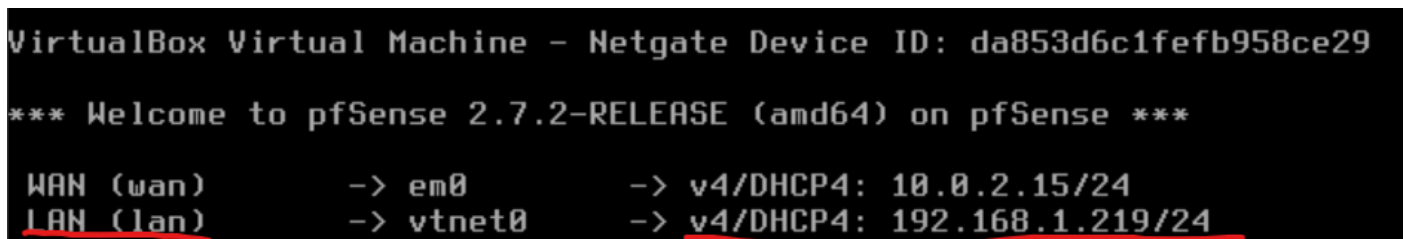
Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'

Come si può notare dalle immagini riesco a collegarmi correttamente.

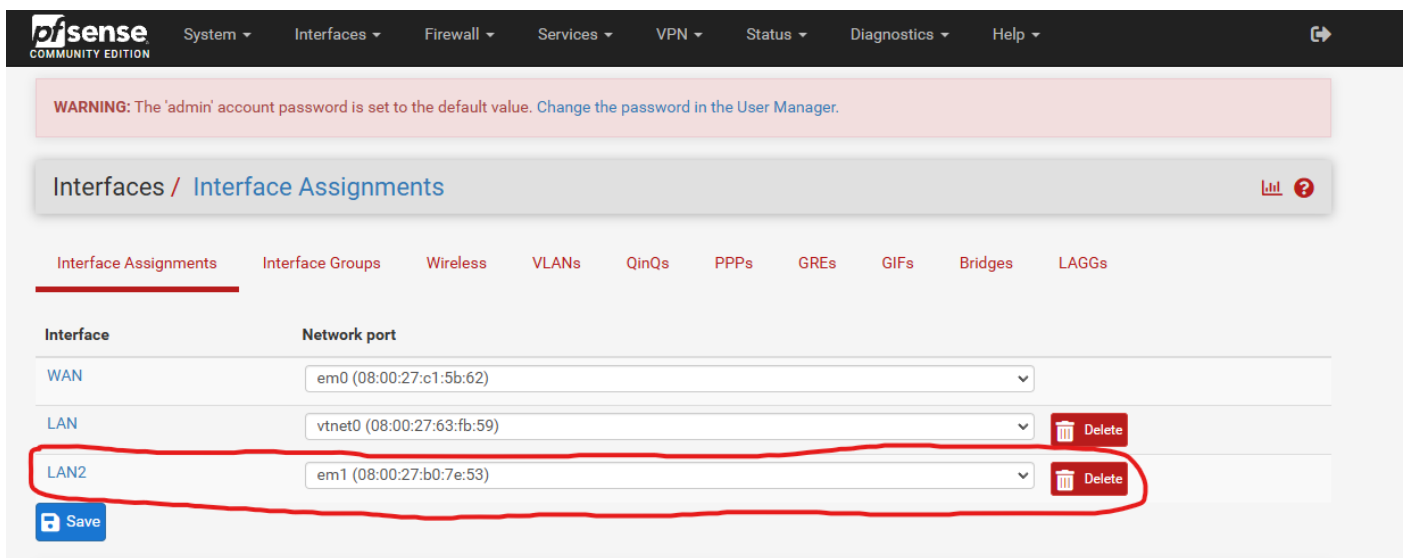
Dopo tramite Oracle Virtual Box aggiungo una nuova scheda di rete per la macchina PFSENSE che sarà il firewall.



Avvio la macchina per trovare l'indirizzo IP a cui collegarmi alla Web GUI dalla mia macchina fisica.



Mi dirigo nella sezione Interfaces nella web GUI e vado ad impostare la nuova lan che ho chiamato LAN2



General Configuration

Enable

☒ Enable interface

Description

LAN2

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: 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 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

192.168.2.2

/24

IPv4 Upstream gateway

None

+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).
Gateways can be managed by [clicking here](#).

Reserved Networks

Adesso mi sposto nella sezione Firewall della GUI e imposto la regola per vietare l'accesso dalla LAN2(Kali) alla LAN principale(metasploitable).

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

LAN2 address

Source Address

/

Destination

Destination

☐ Invert match

LAN address

Destination Address

/

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

Display Advanced

Nel frattempo ho impostato la seconda rete per kali

Addresses

Address	Netmask	Gateway	
192.168.2.2	24	192.168.1.1	<div>Add</div> <div>Delete</div>

DNS servers

Infine provo a connettermi all'ip di metasploitable tramite kali per testare se il firewall è stato impostato correttamente e come dalla seguente immagine non è possibile connettermi.

