

Traccia:

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

Introduzione

Si precisa in via preliminare che per lo svolgimento della traccia in oggetto si renderà necessario l’utilizzo simultaneo di tre macchine virtuali (da qui a seguire v.m.):

- una v.m. con un sistema operativo “Kali Linux”;
- una v.m. con installata la distribuzione “Pfsense”;
- una v.m. con installato il software “Metasploitable”.

Sempre a livello didascalico, si specifica che il software Metasploitable consiste in una piattaforma che consente di eseguire dei *“penetration test”* in totale sicurezza.

Nella consegna odierna si procederà dunque alla realizzazione di una prima – sebbene molto semplice – difesa contro tentativi di accesso alla DVWA dalla v.m. con Kali Linux.

A tale scopo si renderà necessario impostare specifiche regole nel *Firewall*¹ attraverso la Web Gui di Pfsense.

Passo 1 – azioni preliminari

Prima di procedere con lo svolgimento della traccia risulta di fondamentale importanza verificare le impostazioni di rete di tutte e tre le v.m.

Per eseguire la verifica occorre accedere alla propria piattaforma ospitante le v.m., preselezionare la v.m. interessata, quindi cliccare su “impostazioni”.



fig.1

Una volta entrati nelle impostazioni, selezionare “rete” sul menù a tendina e verificare che la scheda di rete sia abilitata e:

- nel caso della v.m. con Kali Linux, impostata su rete interna

¹ “Dispositivo hardware o software di difesa, utilizzato durante la navigazione in rete contro eventuali attacchi di cracker o altri tentativi di intrusione; funziona come un filtro dei dati in entrata e in uscita dal computer collegato a Internet, dei quali controlla l’affidabilità innalzando il livello di sicurezza del sistema sul quale è installato”.
<https://www.treccani.it/vocabolario/firewall/>

PROGETTO S3 - L5

CREAZIONE DI POLICY PFSENSE

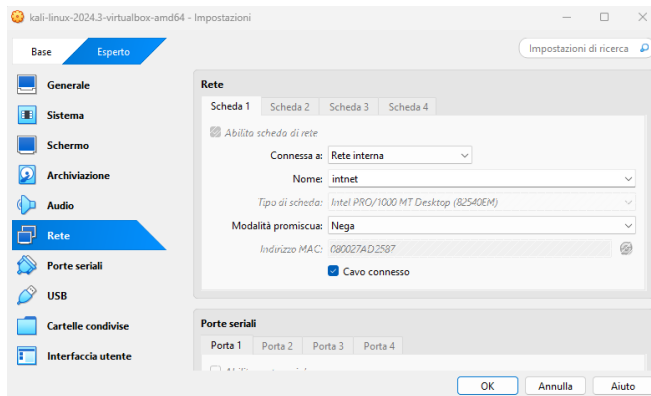


fig.2

- nel caso della v.m. con Pfsense siano abilitate tre schede di rete, rispettivamente la prima con una rete NAT, la seconda con una rete Interna e la terza con una rete bridge

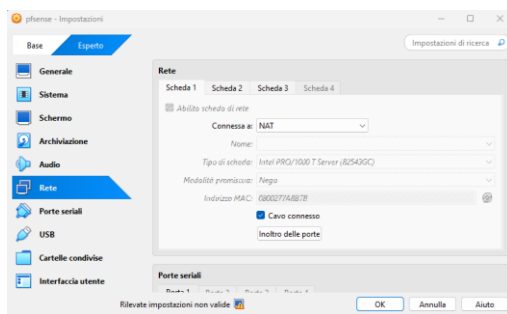


fig.3

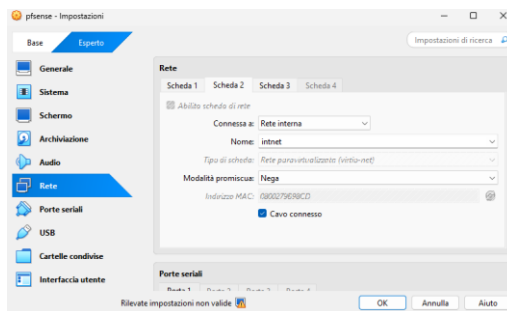


fig.4

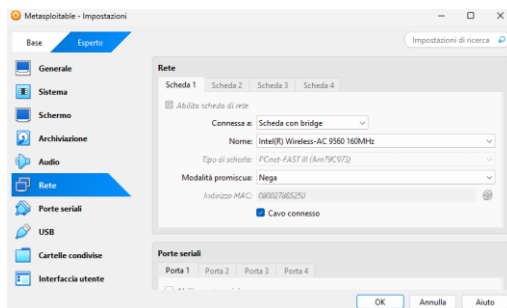


fig.5

- nel caso invece di Metasploitable, vi deve essere una sola scheda di rete attiva, con una rete bridge.

PROGETTO S3 - L5

CREAZIONE DI POLICY PFSENSE

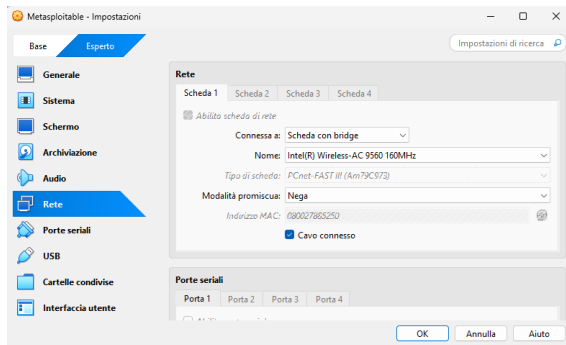


fig.6

Passo 2 – configurazione IP

Una volta verificate che le schede di reti siano correttamente impostate, occorre ora sincerarsi che:

- Kali e Pfsense insistano sulla medesima rete;
- Metasploitable sia collocato in una rete diversa.

Per procedere in tal senso è necessario agire a livello IP: sostanzialmente gli IP di Kali e Pfsense dovranno condividere il terzo ottetto dell'indirizzo.

Nel caso di specie si è imposto manualmente un nuovo indirizzo IP su Kali, seguendo il procedimento di cui alle seguenti figure.

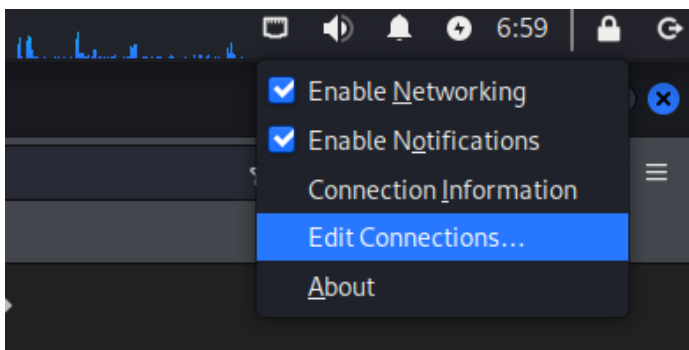


fig.7

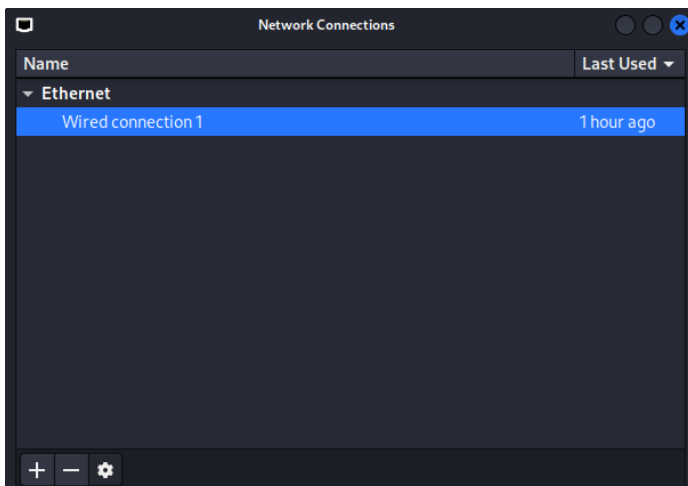


fig.8

PROGETTO S3 - L5
CREAZIONE DI POLICY PFSENSE

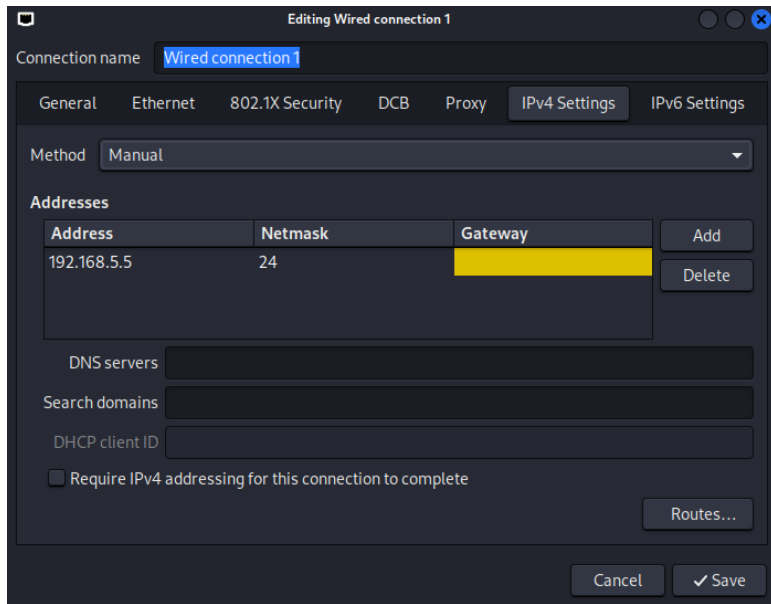


fig.9

Impostare Manual su “Method”, quindi aggiungere l’indirizzo IP di nostro interesse con “add”, congiuntamente con una Netmask (24 nel caso di specie) e infine cliccare su salva. A questo punto per una maggiore sicurezza si può procedere con l’esecuzione di una prova.

Su Terminal Emulator dare il comando “**ip a**”.

L’output dovrebbe dare riscontro col medesimo indirizzo IP impostato manualmente.

```
(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 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.5.5/24 brd 192.168.5.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::9c9:ec2f:e26c:865a/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

fig.10

Ora procedere con il verificare e (se necessario) modificare l’indirizzo IP su Pfsense.

PROGETTO S3 - L5
CREAZIONE DI POLICY PFSense

```
The IPv4 OPT1 address has been set to 192.168.1.2/24
You can now access the webConfigurator by opening the following URL in your web
browser:

    http://192.168.1.2/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 3a08d594a4a8b7c19472

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

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> vtnet0   -> v4: 192.168.5.2/24
OPT1 (opt1)    -> em1      -> v4: 192.168.1.2/24

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

Enter an option: S
```

fig.11

Nel caso che ci interessa l'indirizzo IP di Pfsense si trova già impostato sulla medesima rete di Kali Linux, ma nel caso in cui così non fosse si dovrebbe digitare "2" e seguire la procedura guidata del programma, inserendo solamente l'IP desiderato quando richiesto.

A questo punto, per scrupolo, verificare l'IP di Metasploitable, dandogli il comando "ifconfig".

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:88:52:50
          inet addr:192.168.1.52  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe88:5250/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7360 errors:0 dropped:0 overruns:0 frame:0
          TX packets:541 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:453093 (442.4 KB)  TX bytes:31220 (30.4 KB)
          Interrupt:16 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:331 errors:0 dropped:0 overruns:0 frame:0
          TX packets:331 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:136913 (133.7 KB)  TX bytes:136913 (133.7 KB)
```

fig.12

L'IP di *default* di Metasploitable provvede già a collocarlo su una rete differente.

Passo 3 – il Firewall

A questo punto si apra il *browser* di Kali Linux e digitare nella barra di ricerca l'indirizzo IP di Pfsense.

PROGETTO S3 - L5

CREAZIONE DI POLICY PFSense

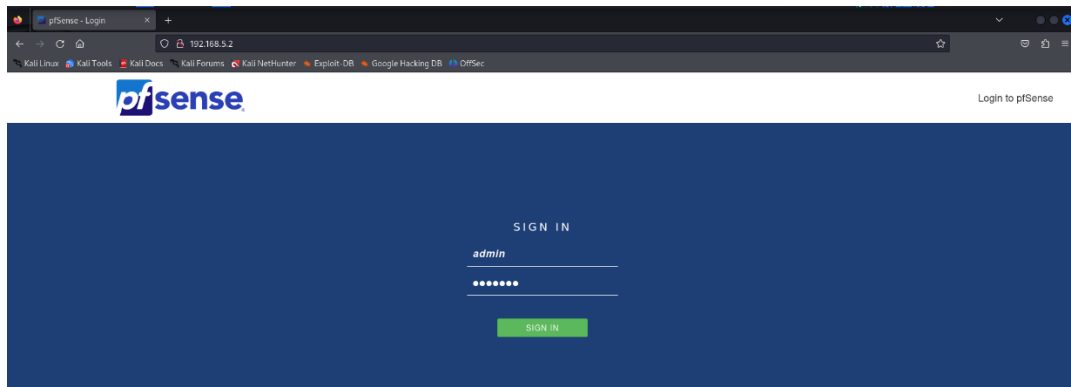


fig. 13

Procedere, qualora richiesto, ad eseguire il “log in” sul Web Gui con le credenziali di *default* (user: “admin”; password: “pfsense”) oppure con quelle personalizzate se precedentemente alterate.

Dalla barra degli strumenti quindi selezionare Firewall e quindi “rules”.

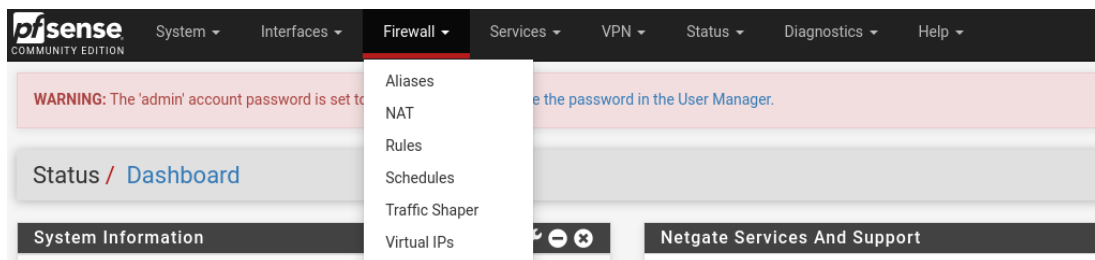


fig.14

A questo punto è possibile procedere con la creazione di una regola su una o più delle reti di PfSense.

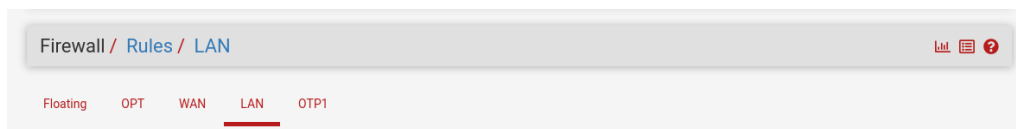


fig.15

Si proceda dunque a imporre una regola di blocco sulla rete LAN, premendo sul tasto “add”.

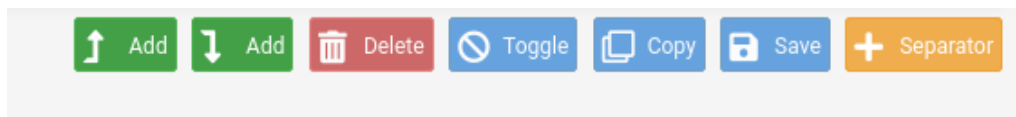


fig.16

Completare i riquadri con le informazioni richieste come nella figura a seguire.

PROGETTO S3 - L5

CREAZIONE DI POLICY PFSENSE

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	<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/UDP Choose which IP protocol this rule should match.

fig. 17

Ora, inserire l'IP sorgente e l'IP destinazione, allo scopo di imporre correttamente il senso di marcia del traffico dati che si intende bloccare con la regola di blocco.

Un elemento particolarmente importante del passaggio in questione è la parte relativa all'indicazione delle porte. Nel caso che interessa si è proceduto ad impostare “any”, allo scopo di impedire che il flusso di dati passi attraverso “qualunque” porta.

Source

Source	<input type="checkbox"/> Invert match	Address or Alias	192.168.5.5	/		
---------------	---------------------------------------	------------------	-------------	---	--	--

[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	<input type="checkbox"/> Invert match	Address or Alias	192.168.1.52	/		
Destination Port Range	any	From	Custom	To	any	Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log	<input type="checkbox"/> 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	Test 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](#)

fig. 18

A questo punto cliccare “salva” e successivamente su “*apply changes*”.

Seguendo il medesimo procedimento è possibile creare anche diverse altre tipologie di regole o ripetere la medesima regola anche su altre reti di PfSense, come nella figura a seguire.

PROGETTO S3 - L5

CREAZIONE DI POLICY PFSENSE

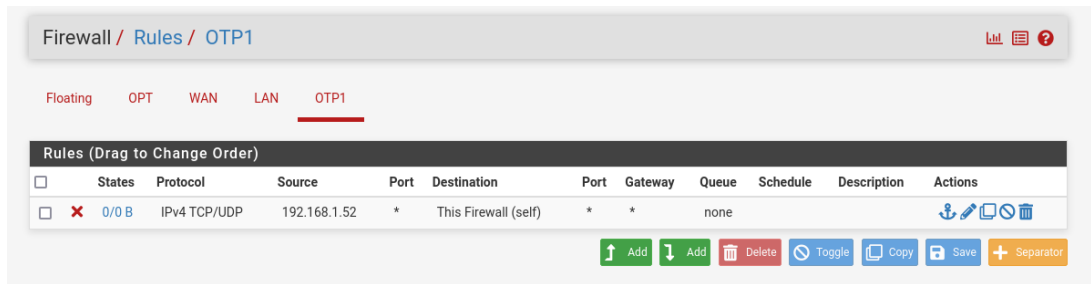


fig.19

Ulteriore passaggio significativo è anche la configurazione dell'interfaccia che si è andata a creare nel momento in cui si sia dovuto procedere con l'abilitazione *ex novo* della terza scheda di rete sulla v.m. di Pfsense.

A tale scopo si torni alla barra strumenti della Web di Pfsense, si selezioni “**Interfaces**” e dunque “**Assignments**”.

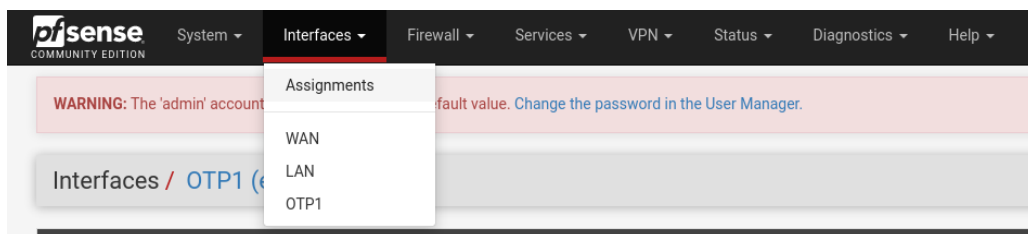


fig.20

Ora si preme sulla rete OTP1

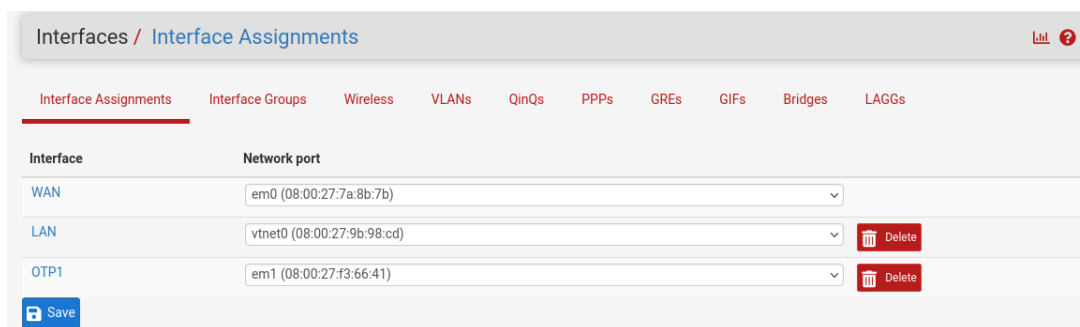


fig. 21

Dunque, si proceda al relativo settaggio come in figura a seguire. Nel caso di interesse si è proceduto ad inserire l'IP di Metasploitable.

PROGETTO S3 - L5

CREAZIONE DI POLICY PFSENSE

Interfaces / OTP1 (em1)

General Configuration

Enable ☒ Enable interface

Description OTP1
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: xxxxxxxxxx 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 192.168.1.52 / 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.

fig.22

Passo 4 – verifica

Con la configurazione del Firewall così come precedentemente descritta nei passaggi precedenti, né Kali Linux né Metasploitable sono in grado di comunicare.

Si è infatti provato sia ad eseguire il comando **ping** da Kali verso Metasploitable e l'output ha dato riscontro negativo;

```
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ ping 192.168.1.52
ping: connect: Network is unreachable
```

fig. 23

Si è provato altresì a dare il comando di scansione a Metasploitable, ricevendo esito sempre negativo.

```
msfadmin@metasploitable:~$ nmap -p0-65535 192.168.5.5
Starting Nmap 4.53 ( http://insecure.org ) at 2024-12-13 08:11 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -PN
Nmap done: 1 IP address (0 hosts up) scanned in 3.119 seconds
```

fig. 24