

U1W3 - Progetto

Creazione di una regola firewall

Richieste:

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

Procedimento:

Ho anzitutto provveduto a configurare le schede di rete delle varie macchine da Virtual Box.

Per la *PFSense* ho configurato da rete, modalità esperti, tre schede di rete: la prima in *bridged*, la seconda e la terza in *rete interna*, nominate rispettivamente ***kalinet*** e ***metanet***.

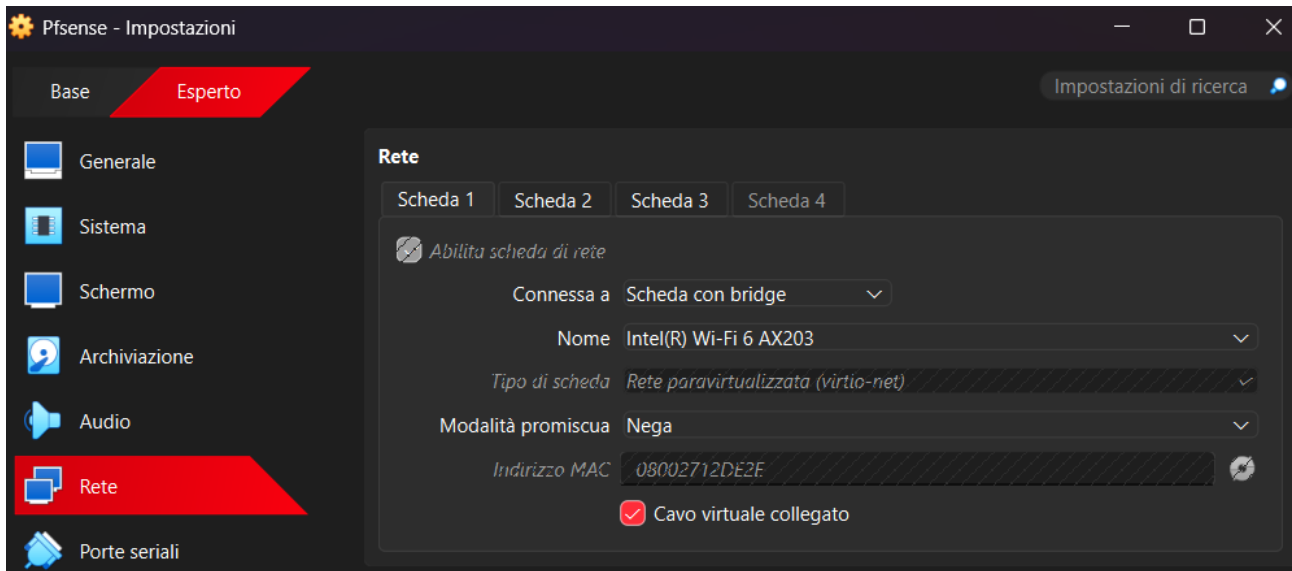


Figura 1 Scheda di rete 1 PFSense, scheda con bridge

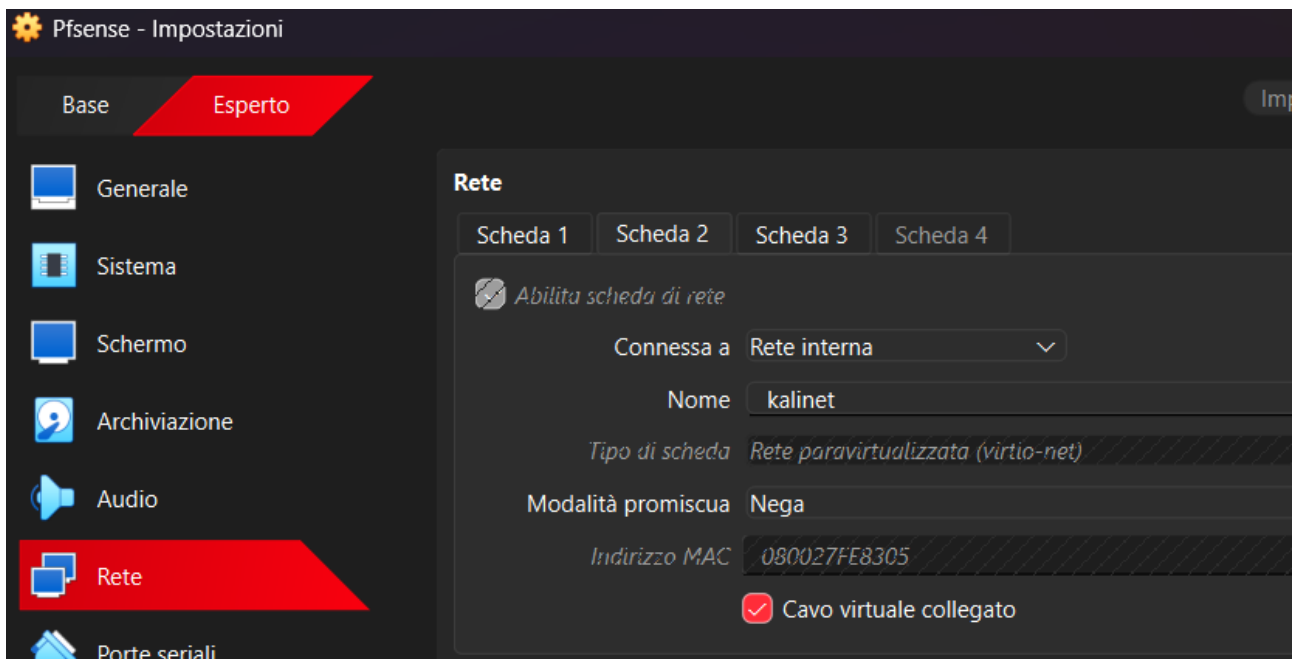


Figura 2 Scheda di rete 2 PFSense, rete interna kalinet

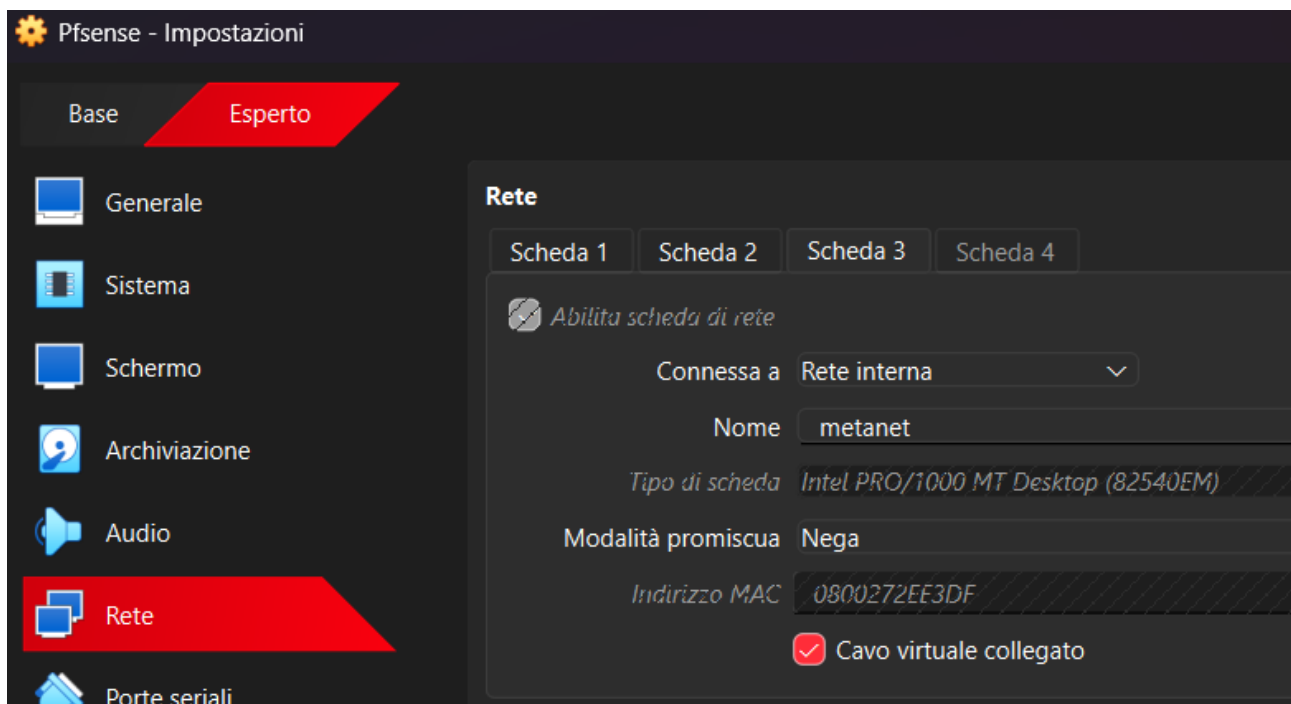


Figura 3 Scheda di rete 3 PFSense, rete interna metanet

Ho configurato poi le *schede di rete* della Kali e della Metasploitable, andando a settarle entrambe come **interne** e usando i **medesimi nomi** dati alle reti interne della PFSense: kalinet per la Kali, metanet per Metasploitable.

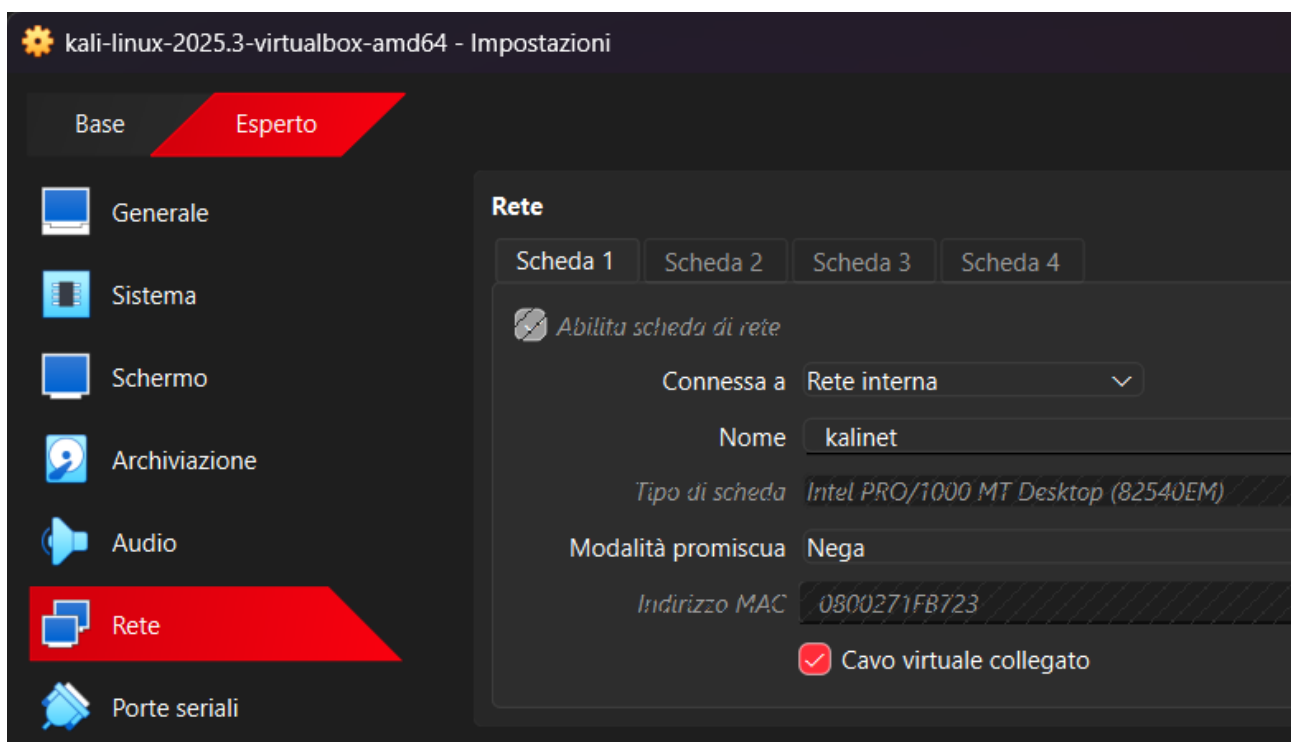


Figura 4 Scheda di rete 1 Kali, rete interna kalinet

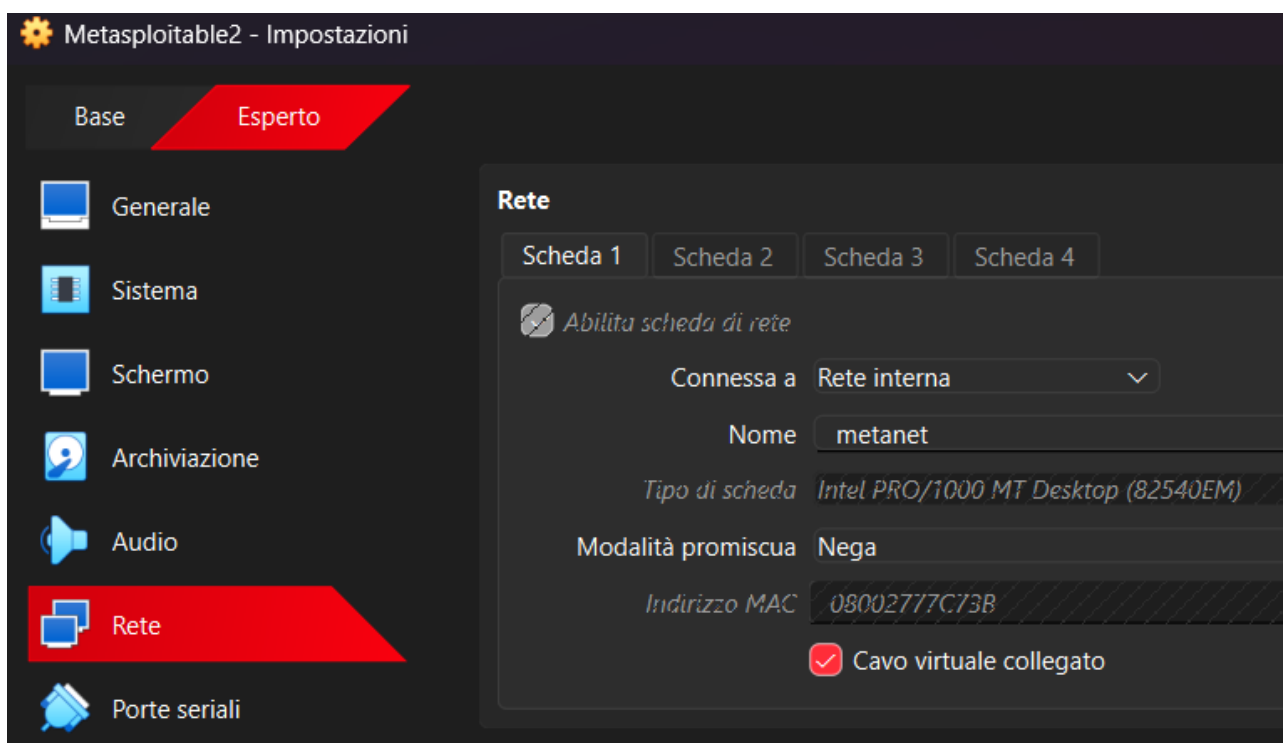


Figura 5 Scheda di rete 1 Metasploitable2, rete interna metanet

Una volta terminata questa configurazione, ho provveduto ad avviare tutte e tre le VMs, per poi concentrarmi sulla configurazione delle *interfacce* tramite *PFSense*.

Da *PFSense* ho configurato le *interfacce* delle prime due schede di rete: WAN e LAN.

Dal menù della *PFSense*, ho selezionato infatti l'**opzione 2: Set Interface(s) IP Address**.

E ho selezionato per prima l'**interfaccia 1**, quella collegata alla WAN.

Ho deciso di configurare l'*IPv4* attraverso il *DHCP*, mentre ho saltato la configurazione dell'*IPv6*.

```

1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfig
3) Reset webConfigurator password 12) PHP shell + pfSense
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell
6) Halt system                15) Restore recent config
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (vtnet0 - dhcp)
2 - LAN (vtnet1 - static)
3 - LAN2 (em0 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) y
Configure IPv6 address WAN interface via DHCP6? (y/n) n
Enter the new WAN IPv6 address. Press <ENTER> for none:
>

```

Figura 6 Configurazione IP WAN, interfaccia 3 visibile in quanto già configurata

Ho proceduto con una configurazione simile per la LAN, ma andando a configurare un *IPv4 statico*, decidendo di assegnarvi l'IP di *gateway* 192.168.10.1 e selezionando il CIDR 24.

```
Enter an option: 2

Available interfaces:

1 - WAN (vtnet0 - dhcp)
2 - LAN (vtnet1)
3 - LAN2 (em0 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.1
```

Figura 7 Configurazione IP LAN (kalinet)

```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.10.50
Enter the end address of the IPv4 client address range: 192.168.10.100
```

Figura 8 Configurazione subnet mask e servizio DHCP offerto con relativo range

Per quello che riguarda invece la scelta di **offrire** un **servizio DHCP**, ho deciso di **abilitarlo**, assegnando il *range* di IP da 192.168.10.50/24 a 192.168.10.100/24.

La terza interfaccia, da me chiamata LAN2, è stata configurata tramite la visualizzazione di *PFSense* da *browser* della *Kali*.

Dalla VM Kali, ho fatto l'accesso a PFSense tramite browser, puntando direttamente all'IP della PFSense dalla scheda di rete connessa in modalità bridged(192.168.1.16/24), e ho poi proceduto ad accedere a *Interfaces*, selezionando *Assignments*, e ho aggiunto un'interfaccia, denominata OPT1 di default.

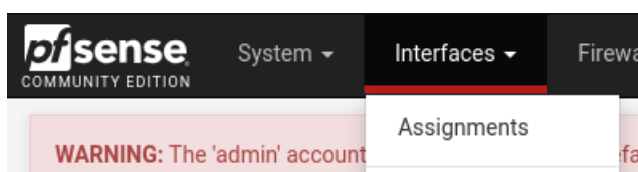


Figura 9 Accesso alla creazione e gestione delle interfacce

Una volta fatto l'accesso a *OPT1*, ho provveduto a rinominarla *LAN2*, ad **attivarla** e a **configurare** il suo *IP* e la sua *maschera di rete*, operazione che una volta abilitata l'interfaccia avrei potuto fare anche da **terminale** della *PFSense* stessa.

The screenshot shows the PFSense web interface at the URL 192.168.1.16/interfaces.php?if=opt1. The browser's address bar and tabs are visible at the top. The main content area is titled "General Configuration" and contains several form fields for configuring the interface. The "Enable" section has a checked "Enable interface" checkbox. The "Description" field is set to "LAN2". The "IPv4 Configuration Type" is set to "Static IPv4". The "IPv6 Configuration Type" is set to "None". The "MAC Address" field contains "xx:xx:xx:xx:xx:xx". The "MTU" and "MSS" fields are empty. The "Speed and Duplex" field is set to "Default (no preference, typically autoselect)". Below the "General Configuration" section is the "Static IPv4 Configuration" section, which has the "IPv4 Address" field set to "192.168.20.1".

General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	LAN2 <small>Enter a description (name) for the interface here.</small>
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xx:xx:xx:xx:xx:xx <small>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.</small>
MTU	<input type="text"/> <small>If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.</small>
MSS	<input type="text"/> <small>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) minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.</small>
Speed and Duplex	Default (no preference, typically autoselect) <small>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</small>

Static IPv4 Configuration	
IPv4 Address	192.168.20.1 / 24

Figura 10 Configurazione LAN2 (metanet) da sito PFSense

Da *Services*, selezionando *DHCP Server*, sono entrata nel menù della LAN2.

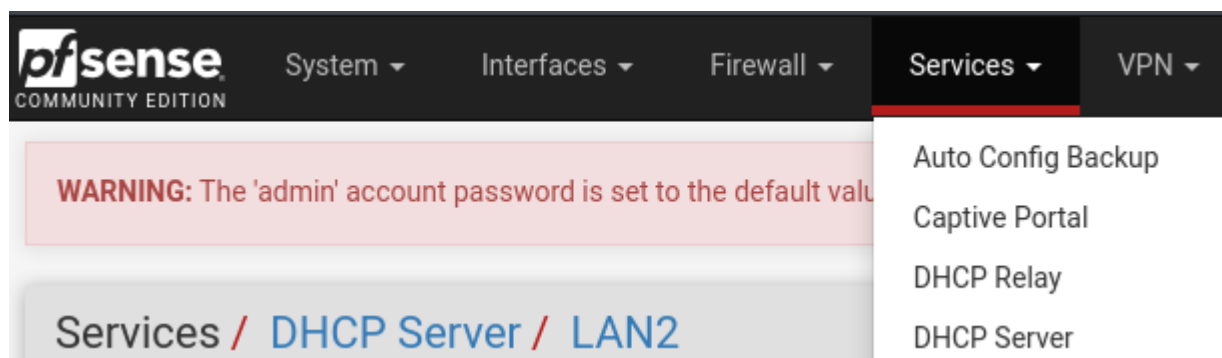


Figura 11 DHCP Service, abilitazione da PFSense su browser

E da qui sono andata ad abilitare il *servizio DHCP* per la rete locale "metanet".

LAN LAN2

General DHCP Options

DHCP Backend ISC DHCP

Enable ☒ Enable DHCP server on LAN2 interface

Figura 12 Attivazione DHCP per LAN2 da PFSense tramite browser

Una volta fatte queste configurazioni, ho controllato dalla *PFSense* le configurazioni delle tre *schede di rete* e degli *IP* ad esse associati.

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

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.1.16/24
LAN (lan)      -> vtnet1      -> v4: 192.168.10.1/24
LAN2 (opt1)    -> em0        -> v4: 192.168.20.1/24
```

Figura 13 Tre schede di rete e IP associati

Una volta configurato il tutto in questo modo, ho proceduto a controllare le regole del *firewall* e se la pagina della *DVWA* sulla *Metasploitable* fosse visualizzabile dal *browser* della *Kali*.

Le regole applicate alla LAN (rete interna kalinet) sono quelle di *default*, il sito risulta raggiungibile tramite il *browser firefox* della *Kali*.

The image consists of two side-by-side browser screenshots. The left screenshot shows the pfSense web interface at 192.168.1.16, specifically the Firewall Rules configuration for the LAN interface. It displays three rules: 'Anti-Lockout Rule' (0/0 B, 80 port), 'Default allow LAN to any rule' (7/1.65 MIB, IPv4), and 'Default allow LAN IPv6 to any rule' (0/0 B, IPv6). The right screenshot shows the DVWA (Damn Vulnerable Web Application) login page at 192.168.20.50, featuring a login form with 'Username' and 'Password' fields and a 'Login' button. Below the form, it mentions that DVWA is a RandomStorm OpenSource project and provides a hint: 'Hint: default username is 'admin' with password 'password''.

Figura 14 Accesso dalla Kali al sito DVWA sulla metasploitable, visione delle regole applicate sulla kalinet

Sempre con le regole settate in quel modo, ho controllato che la Kali fosse in grado di *pingare* sia il *gateway* che l'*indirizzo IP* specifico della *Metasploitable2*.

```

(kali㉿kali)-[~]
$ ping 192.168.20.50
PING 192.168.20.50 (192.168.20.50) 56(84) bytes of data.
64 bytes from 192.168.20.50: icmp_seq=1 ttl=63 time=4.92 ms
64 bytes from 192.168.20.50: icmp_seq=2 ttl=63 time=3.74 ms
^C
— 192.168.20.50 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 3.736/4.327/4.918/0.591 ms

(kali㉿kali)-[~]
$ ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1) 56(84) bytes of data.
64 bytes from 192.168.20.1: icmp_seq=1 ttl=64 time=1.43 ms
64 bytes from 192.168.20.1: icmp_seq=2 ttl=64 time=3.61 ms
^C
— 192.168.20.1 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.429/2.518/3.607/1.089 ms

```

Figura 15 Ping alla metasploitable da Kali

Ho successivamente provveduto ad aggiungere la mia regola personalizzata per poter bloccare **dalla Kali** l'accesso **alla DVWA** sulla Metasploitable.

Da *PFSense* sul browser della Kali, sono andata nella sezione *Firewall*, ho selezionato *Rules* e ho selezionato LAN, la rete legata alla mia Kali.

All'interno, ho aggiunto una regola tramite il bottone *add*, andando a configurarla come segue.

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	Address or Alias	192.168.10.50 /
	<input type="button" value="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	192.168.20.50 /
Destination Port Range	HTTP (80)	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.		

Figura 16 Configurazione regola di Firewall - blocco della Metasploitable DVWA per la Kali

L'action scelta è *Block* in quanto desidero che non ci sia risposta, né negativa, né positiva. Ho settato l'*IP Source* (sorgente) con quello specifico della *Kali* (192.168.10.50/24), *mittente* della mia richiesta verso la pagina DVWA della Metasploitable. Per l'*IP Destination* (destinazione) ho inserito quello della

Metasploitable (192.168.20.50/24), andando però a specificare di voler bloccare solamente il *traffico HTTP* tramite la selezione della *porta 80*.

Mi sono infine assicurata che la regola fosse **in alto**, in modo da venire messa in atto **prima** di quelle di *Pass* generali.

Salvata la regola e confermata l'applicazione dei cambiamenti, ho provato nuovamente a raggiungere la DVWA all'indirizzo IP 192.168.20.50 per assicurarmi che la richiesta andasse in *timeout*.

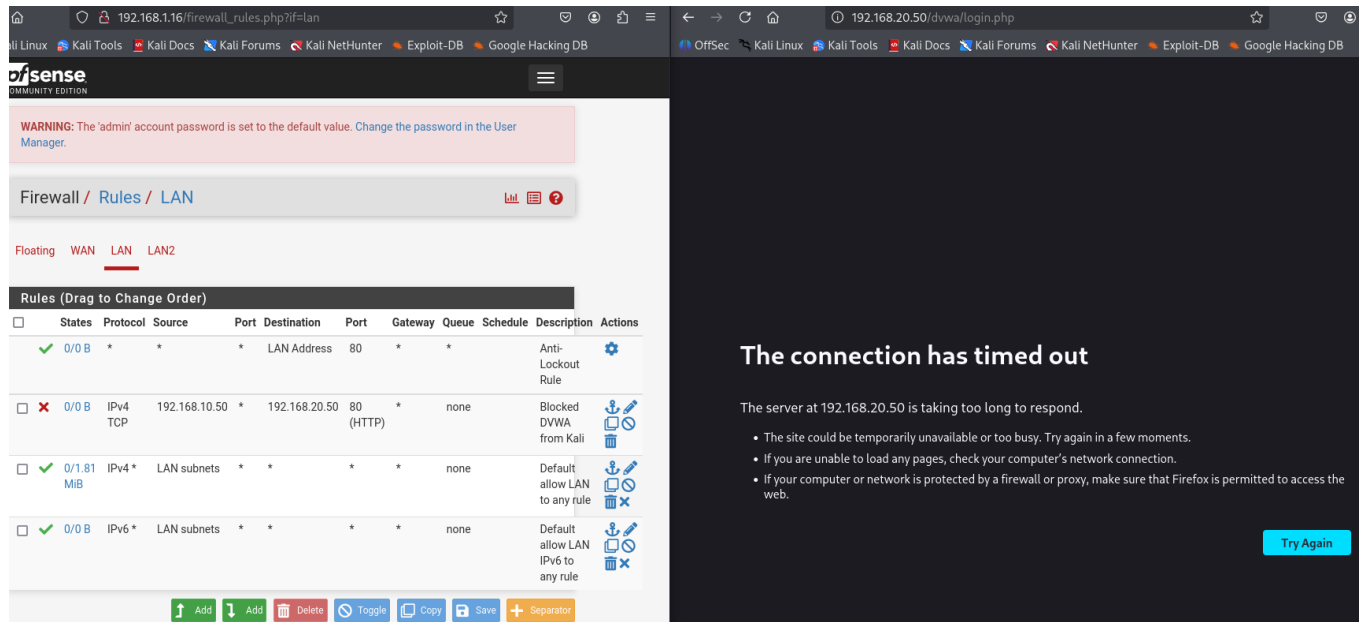


Figura 17 Risultato applicazione regola di block

Ho infine provveduto a controllare che il *ping* dalla *Kali* alla *Metasploitable* ancora funzionasse correttamente nonostante la regola messa in atto.

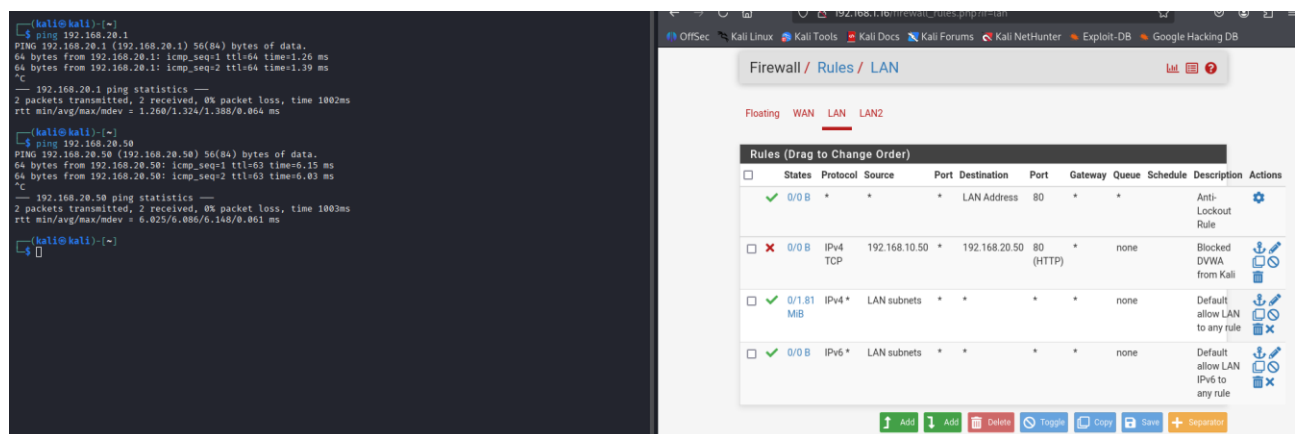


Figura 18 Ping alla Metasploitable dopo l'applicazione della regola

Le configurazioni **finali** delle regole dei *firewall* sono le seguenti:

disense
COMMUNITY EDITION

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

Firewall / Rules / WAN

Floating WAN LAN LAN2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/222 KIB	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	
<input checked="" type="checkbox"/>	0/4 KIB	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Floating WAN LAN LAN2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPV4	*	LAN subnets	*	*	*	*	none	Default allow LAN to any rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPV6	*	LAN subnets	*	*	*	*	none	Default allow LAN IPV6 to any rule	

Add Add Delete Toggle Copy Save Separator

Firewall / Rules / LAN

Floating WAN LAN LAN2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	*	*	*	LAN Address	80	*	*	*	Anti-Lockout Rule
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/1 KIB	IPV4 TCP	192.168.10.50	*	192.168.20.50	80 (HTTP)	*	none	*	Blocked DVWA from Kali
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/1.90 MIB	IPV4 *	LAN subnets	*	*	*	*	none	*	Default allow LAN to any rule
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPV6 *	LAN subnets	*	*	*	*	none	*	Default allow LAN IPV6 to any rule

Add Add Delete Toggle Copy Save Separator

Figura 19 Configurazioni Firewall