

Indice

1. Traccia.....	2
2. Soluzione	2
2.1 Configurazione schede di rete Pfsense su VirtualBox.....	2
2.2 Configurazione schede di rete Kali Linux su VirtualBox.....	3
2.3 Configurazione schede di rete Metasploitable su VirtualBox	3
2.4 Configurazioni WAN, LAN (Kali), LAN (Metasploitable2) su Pfsense	3
2.5 Configurazione di rete Kali Linux	4
2.6 Configurazione di rete Metasploitable2	4
2.7 Accesso ad Internet tramite Kali Linux	5
2.8 Impostazioni Firewall Pfsense.....	6
2.9 Dettaglio Regola	7
2.10 Verifica	8
3. Conclusione.....	8

1. Traccia

Creare una regola firewall che blocchi l'accesso alla DVWA su metasploitable dalla macchina Kali Linux e ne impedisca lo scan delle porte. Le macchine Kali e Metasploitable devono essere su reti diverse.

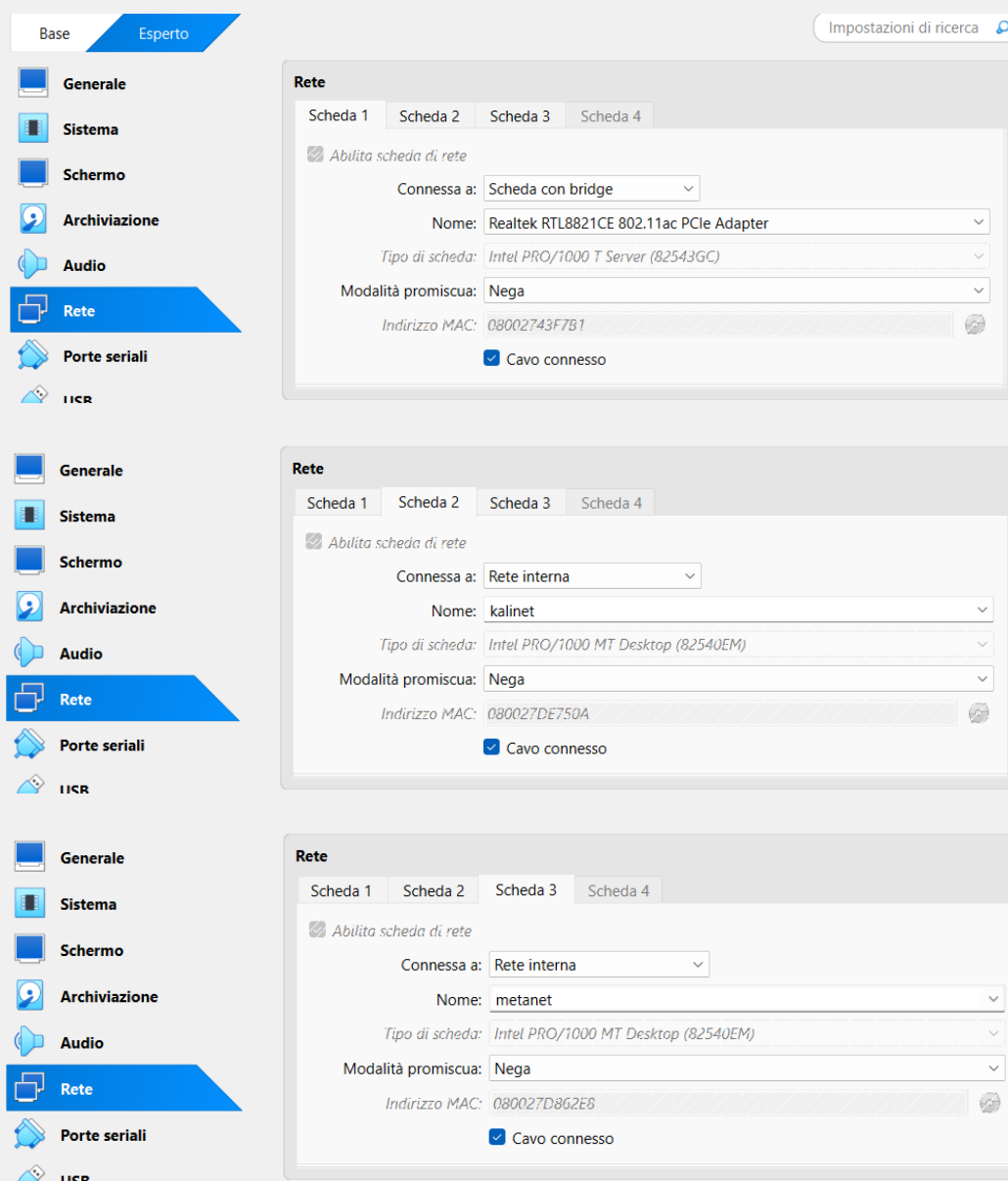
2. Soluzione

2.1 Configurazione schede di rete PfSense su VirtualBox

Per la macchina virtuale PfSense configuriamo tre schede di rete:

- **Scheda 1 (WAN):** in modalità *bridge*, per collegarsi alla rete domestica.
- **Scheda 2 (LAN - Kali):** in modalità *rete interna*, denominata kalinet.
- **Scheda 3 (OPT1 - Metasploitable):** anch'essa in modalità *rete interna*, denominata metanet.

In questo modo PfSense fungerà da gateway e gestore del traffico tra le varie reti.



The image displays three screenshots of the PfSense web interface, specifically the 'Rete' (Network) section, showing the configuration for three different network cards (Scheda 1, Scheda 2, and Scheda 3).

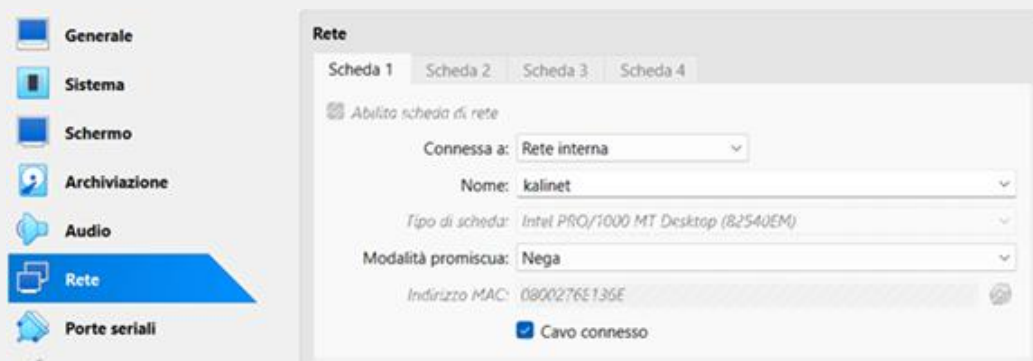
Scheda 1 (WAN): The configuration shows 'Abilita scheda di rete' checked, 'Connessa a' set to 'Scheda con bridge', 'Nome' set to 'Realtek RTL821CE 802.11ac PCIe Adapter', 'Tipo di scheda' set to 'Intel PRO/1000 T Server (82543GC)', 'Modalità promiscua' set to 'Nega', and 'Indirizzo MAC' set to '08002743F7B1'. The 'Cavo connesso' checkbox is checked.

Scheda 2 (Kali): The configuration shows 'Abilita scheda di rete' checked, 'Connessa a' set to 'Rete interna', 'Nome' set to 'kalinet', 'Tipo di scheda' set to 'Intel PRO/1000 MT Desktop (82540EM)', 'Modalità promiscua' set to 'Nega', and 'Indirizzo MAC' set to '080027DE750A'. The 'Cavo connesso' checkbox is checked.

Scheda 3 (Metasploitable): The configuration shows 'Abilita scheda di rete' checked, 'Connessa a' set to 'Rete interna', 'Nome' set to 'metanet', 'Tipo di scheda' set to 'Intel PRO/1000 MT Desktop (82540EM)', 'Modalità promiscua' set to 'Nega', and 'Indirizzo MAC' set to '080027D862E8'. The 'Cavo connesso' checkbox is checked.

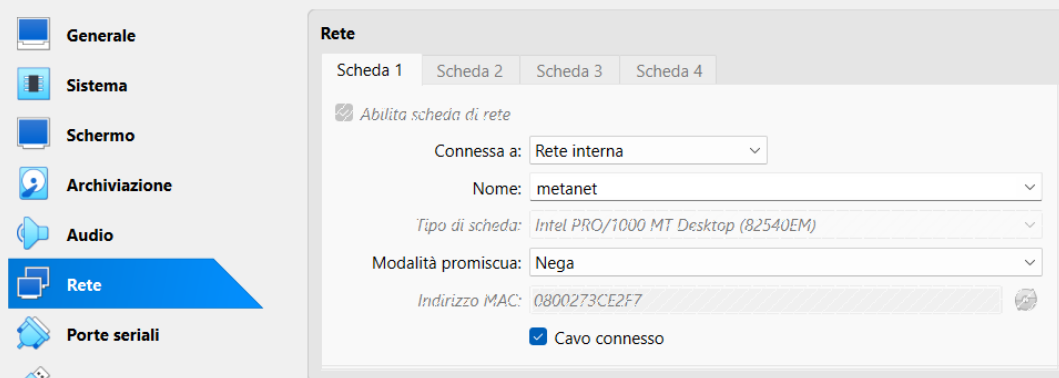
2.2 Configurazione schede di rete Kali Linux su VirtualBox

Alla VM Kali Linux assegniamo la rete interna kalinet, precedentemente definita per la comunicazione con Pfsense.



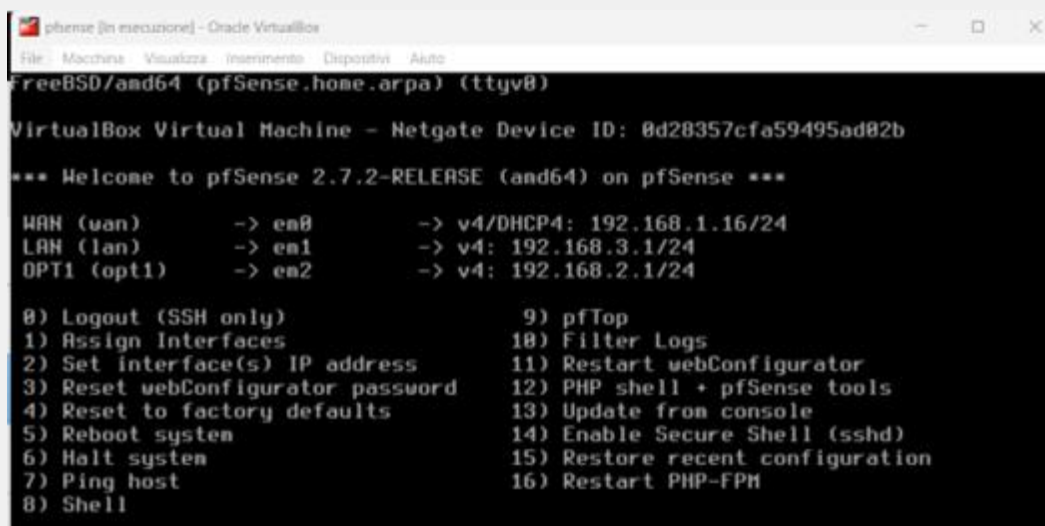
2.3 Configurazione schede di rete Metasploitable su VirtualBox

Alla VM Metasploitable2 assegniamo la rete interna metanet, per connettersi al relativo segmento gestito da Pfsense.



2.4 Configurazioni WAN, LAN (Kali), LAN (Metasploitable2) su Pfsense

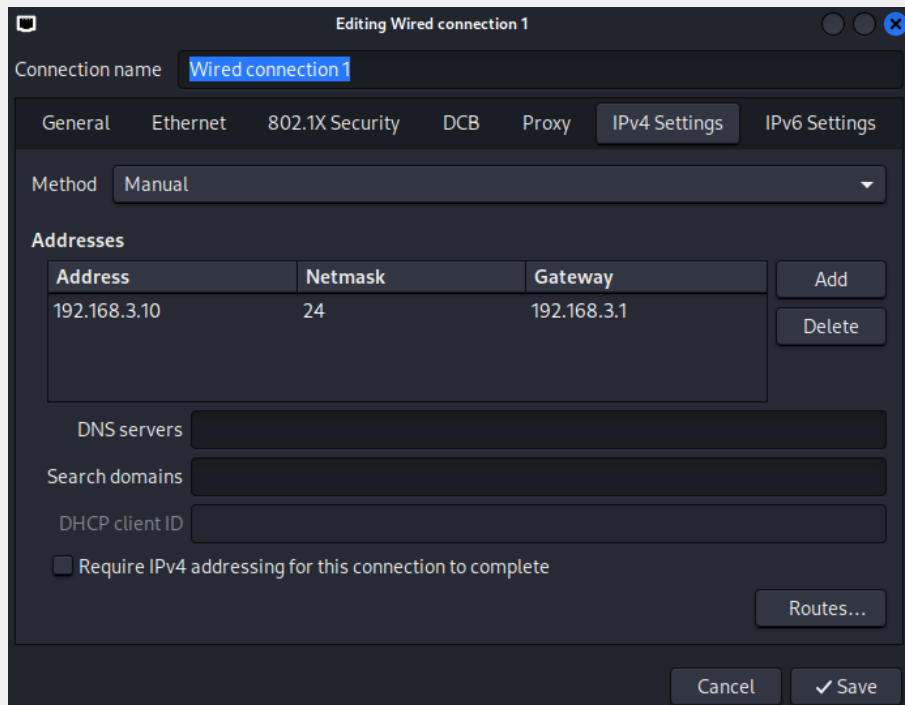
- WAN: configurata in DHCP per ottenere automaticamente l'IP dalla rete domestica.
- LAN (Kali) e OPT1 (Metasploitable2): configurazione statica manuale.



2.5 Configurazione di rete Kali Linux

Impostiamo manualmente:

- IP: 192.168.3.10
- Netmask: 255.255.255.0
- Gateway: 192.168.3.1 (IP della LAN su Pfsense)



2.6 Configurazione di rete Metasploitable2

Modifichiamo il file `/etc/network/interfaces` con i seguenti parametri:

- IP: 192.168.2.10
- Netmask: 255.255.255.0
- Gateway: 192.168.2.1 (IP di OPT1 su Pfsense)

```
GNU nano 2.0.7      File: /etc/network/interfaces

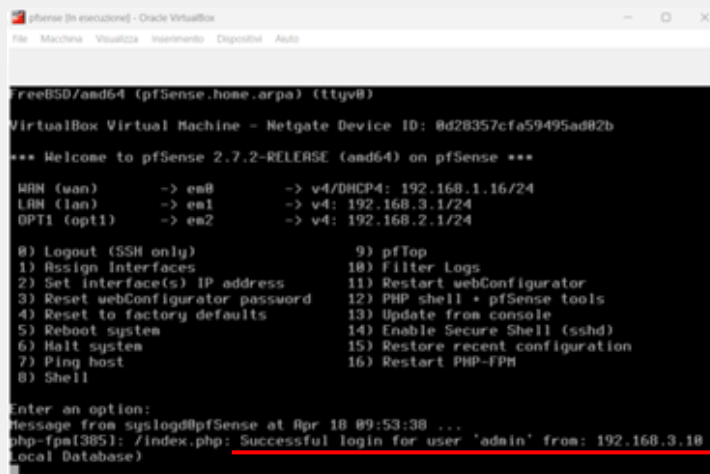
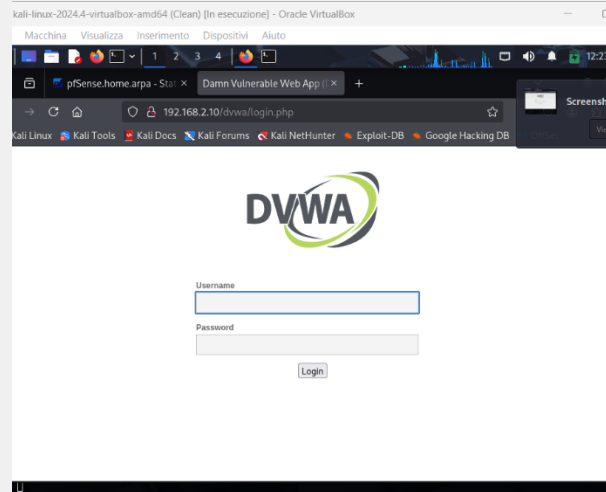
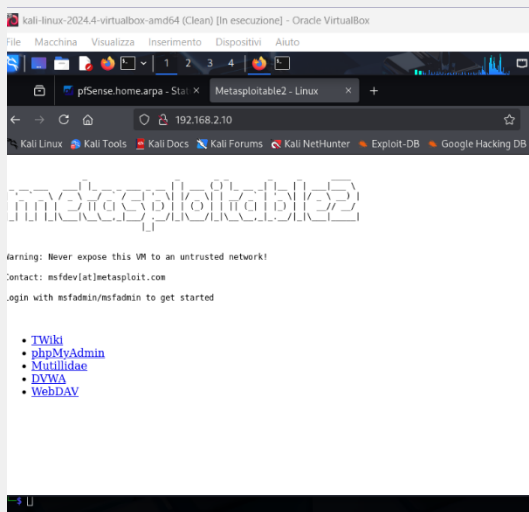
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.2.10
    netmask 255.255.255.0
    gateway 192.168.2.1
```

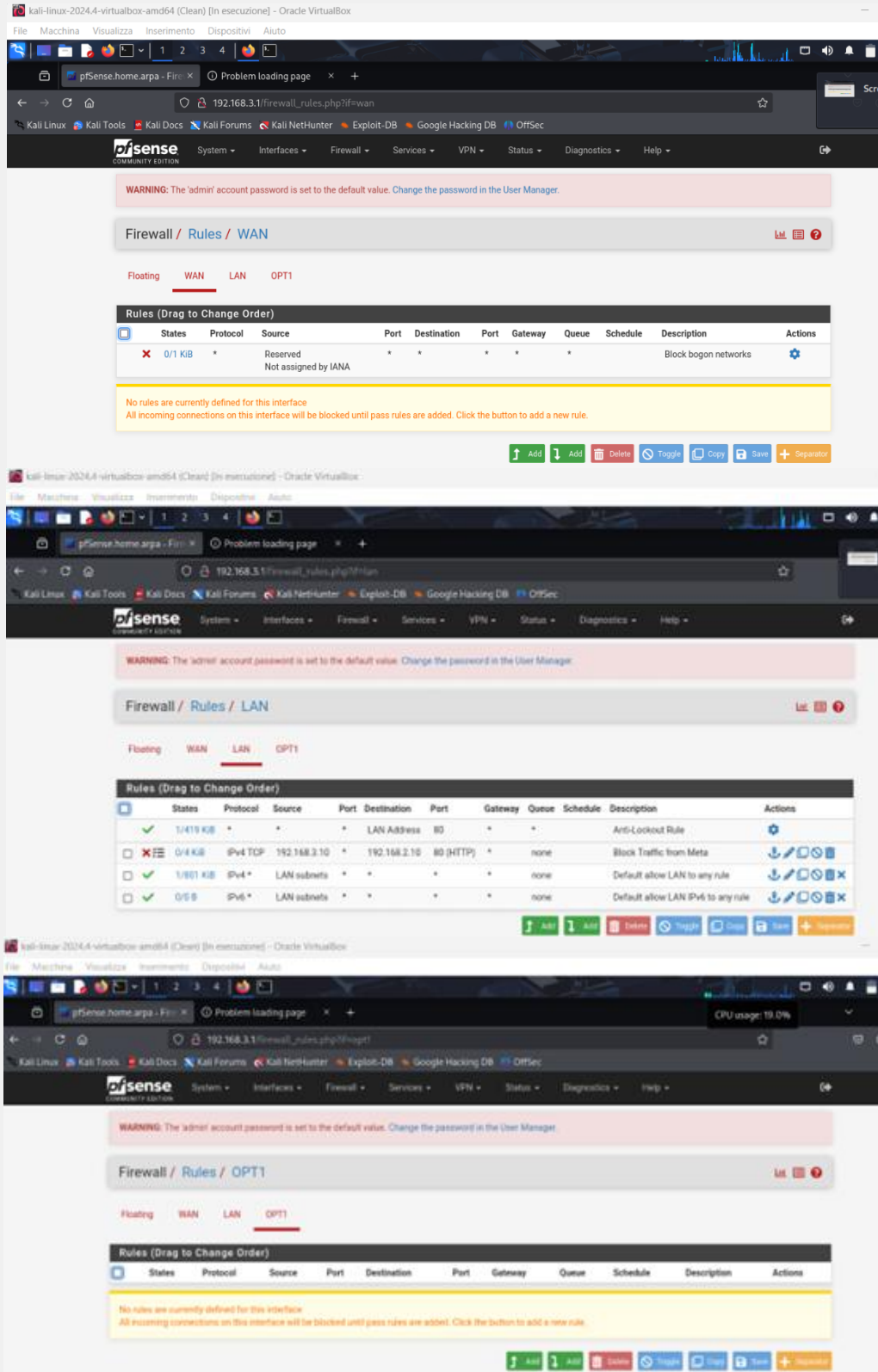
2.7 Accesso ad Internet tramite Kali Linux

Una volta completata la configurazione, la macchina Kali Linux è in grado di accedere a internet tramite il gateway PfSense. Testiamo anche la connessione alla web application DVWA presente su Metasploitable2.



2.8 Impostazioni Firewall Pfsense

Accediamo all'interfaccia web di Pfsense e configuriamo una regola sulla LAN (interfaccia a cui è collegata Kali Linux), per bloccare l'accesso alla macchina Metasploitable2.



The screenshots show the Pfsense web interface for configuring firewall rules. The first screenshot shows the WAN interface with a warning about the default password and a table of rules. The second screenshot shows the LAN interface with a similar warning and a table of rules. The third screenshot shows the OPT1 interface with a warning and a table of rules.

Firewall / Rules / WAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/1 KIB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogus 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.

Firewall / Rules / LAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
1/419 KIB	*	*	*	LAN Address	80	*	*		Anti-Lookout Rule	
0/4 KIB	IPv4 TCP	192.168.3.10	*	192.168.3.10	80 (HTTP)	*	none		Block Traffic from Meta	
1/801 KIB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Firewall / Rules / OPT1

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
--------	----------	--------	------	-------------	------	---------	-------	----------	-------------	---------

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.

2.9 Dettaglio Regola

La regola firewall viene creata come segue:

- **Action:** Block
- **Interface:** LAN
- **Source:** 192.168.3.10 (Kali)
- **Destination:** 192.168.2.10 (Metasploitable2)

La regola va posizionata **sopra** eventuali regole che permettono il traffico generico, per garantirne la corretta applicazione.

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

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 ☐ 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 Address or Alias 192.168.3.10 /

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 192.168.2.10 /

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.

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).

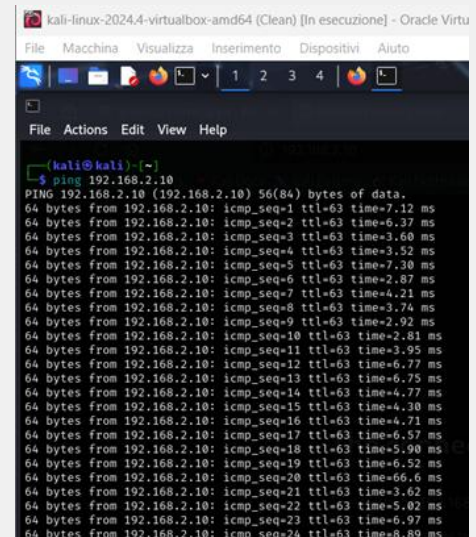
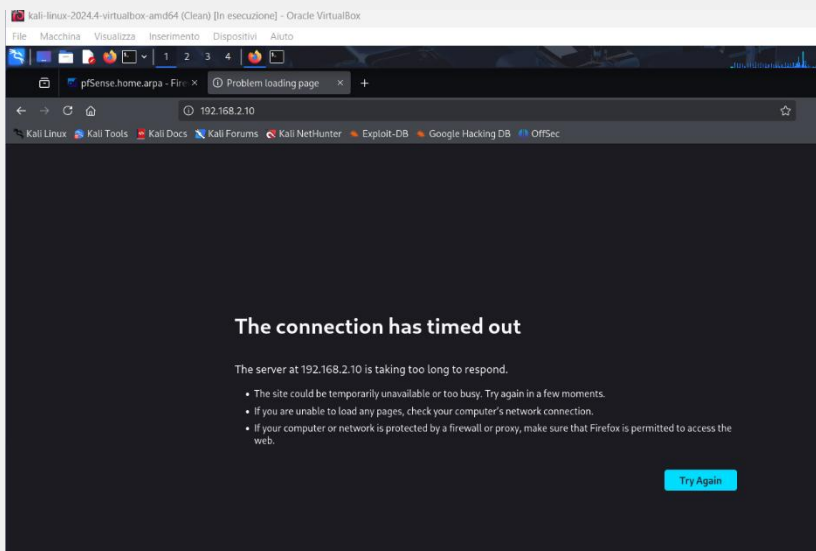
Description Block Traffic from Meta
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

2.10 Verifica

Effettuiamo un test da Kali:

- Il ping verso Metasploitable2 funziona ancora.
- Tuttavia, il tentativo di accedere via browser alla DVWA risulta bloccato, confermando l'efficacia della regola firewall.



3. Conclusione

Attraverso la corretta configurazione delle reti su VirtualBox e la gestione del traffico tramite Pfsense, è stato possibile segmentare correttamente le due macchine (Kali Linux e Metasploitable2) e applicare una regola firewall che blocca l'accesso alla DVWA e impedisce lo scanning. Questo tipo di configurazione è fondamentale per simulare ambienti reali di rete, in cui è necessario limitare l'accesso tra host per motivi di sicurezza e contenimento delle minacce.