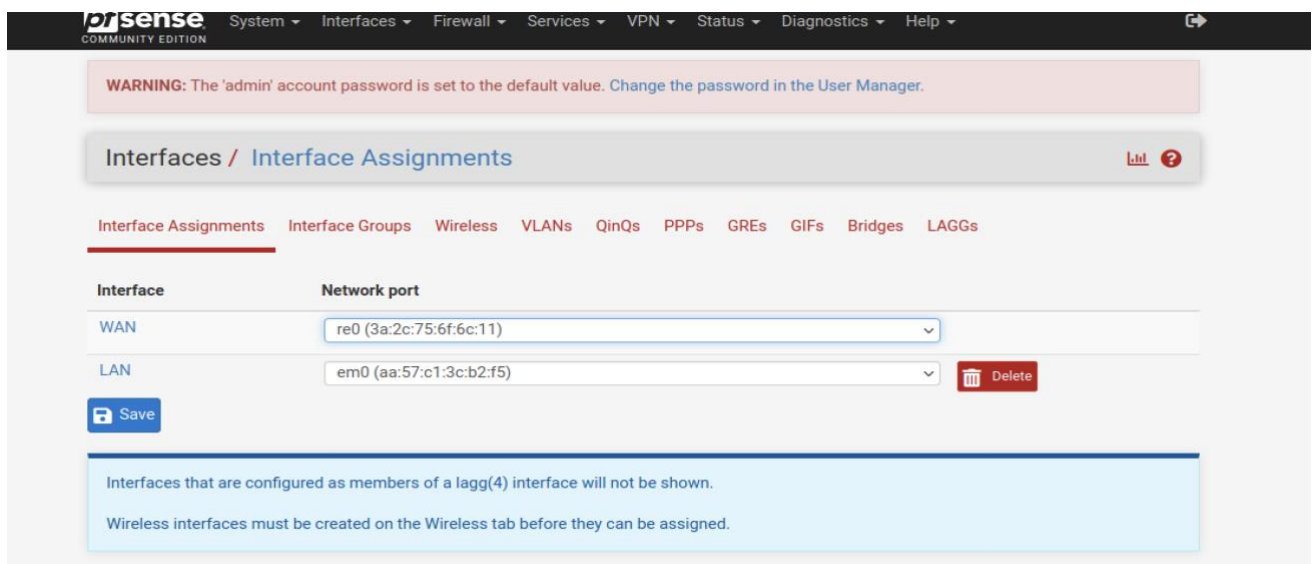


Progetto 13 dicembre

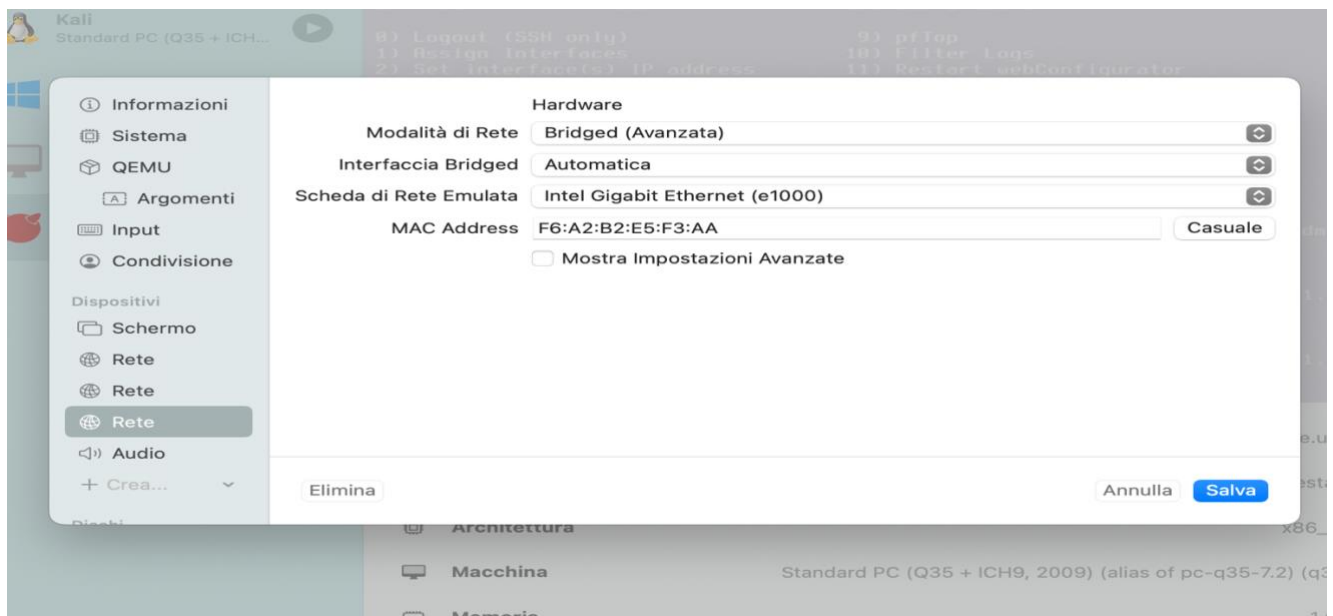
La traccia è la seguente:

Sulla base di quanto visto, creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete. Connettetevi poi in Web Gui per attivare la nuova interfaccia e configurarla .

Passaggio 1: all'inizio mi dava questo problema, cioè non mi faceva aggiungere un'interfaccia su pfsense così andando su UTM nelle impostazioni di rete di pfsense ho aggiunto un'altra rete .(Foto2)



2.



Una volta eseguiti questi passaggi ho configurato la nuova interfaccia chiamandola Kali-Rete, configurandola con ip statico e indirizzo: 192.168.2.2 con gateway 192.168.2.1.

The screenshot shows the Mikrotik WinBox interface for configuring a new interface. The 'Static IPv4 Configuration' section is active, showing the following settings:

- IPv4 Configuration Type:** Static IPv4
- IPv6 Configuration Type:** None
- MAC Address:** xx:xx:xx:xx:xx:xx (with a note: '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:** (empty field, with a note: '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:** (empty field, with a note: '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) (with a note: '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.'))

The 'Static IPv4 Configuration' section shows:

- IPv4 Address:** 192.168.2.2 / 24
- IPv4 Upstream gateway:** Kali_ReteGW - 192.168.2.1 (with a '+ Add a new gateway' button)

Successivamente ho configurato su Firewall-Rules una nuova regola per bloccare il traffico dal nuovo indirizzo ip di Kali a quello di meta (nel mio caso 192.168.1.52)

The screenshot shows the Mikrotik WinBox interface for editing a Firewall Rule. The 'Edit Firewall Rule' section is active, showing the following settings:

- Action:** Block (with a note: '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 (with a note: 'Set this option to disable this rule without removing it from the list.'))
- Interface:** KALI_RETE (with a note: 'Choose the interface from which packets must come to match this rule.'))
- Address Family:** IPv4 (with a note: 'Select the Internet Protocol version this rule applies to.'))
- Protocol:** TCP (with a note: 'Choose which IP protocol this rule should match.'))

Ho impostato l'azione su "block" per bloccare il traffico dal nuovo ip di kali '192.168.2.2' verso l'ip di meta '192.168.1.52' e ho inserito come "destination port" quella di DVWA cioè 80.

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 Network 192.168.2.2 / 24

[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 ☐ Invert match Address or Alias 192.168.1.52 /

Destination Port Range HTTP (80) Custom HTTP (80) 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).

Però una volta configurata questa nuova regola e salvata, non funziona.

192.168.1.120/firewall_rules.php?if=opt1

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

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

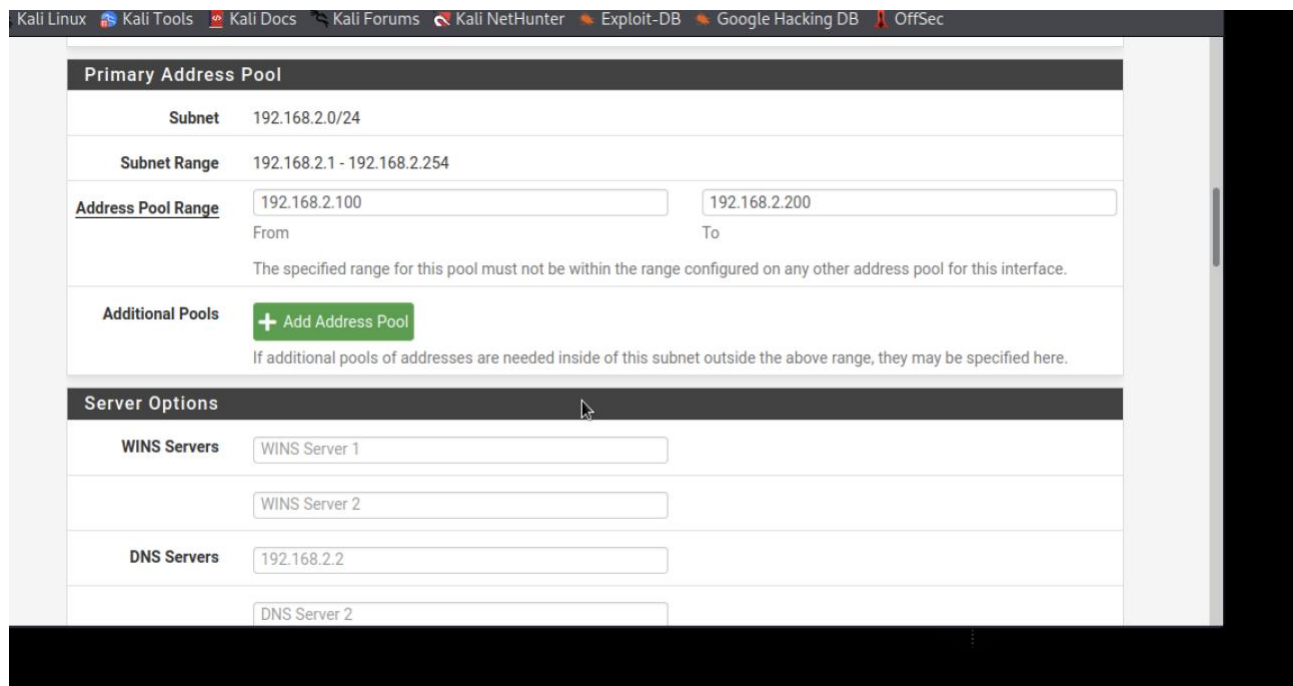
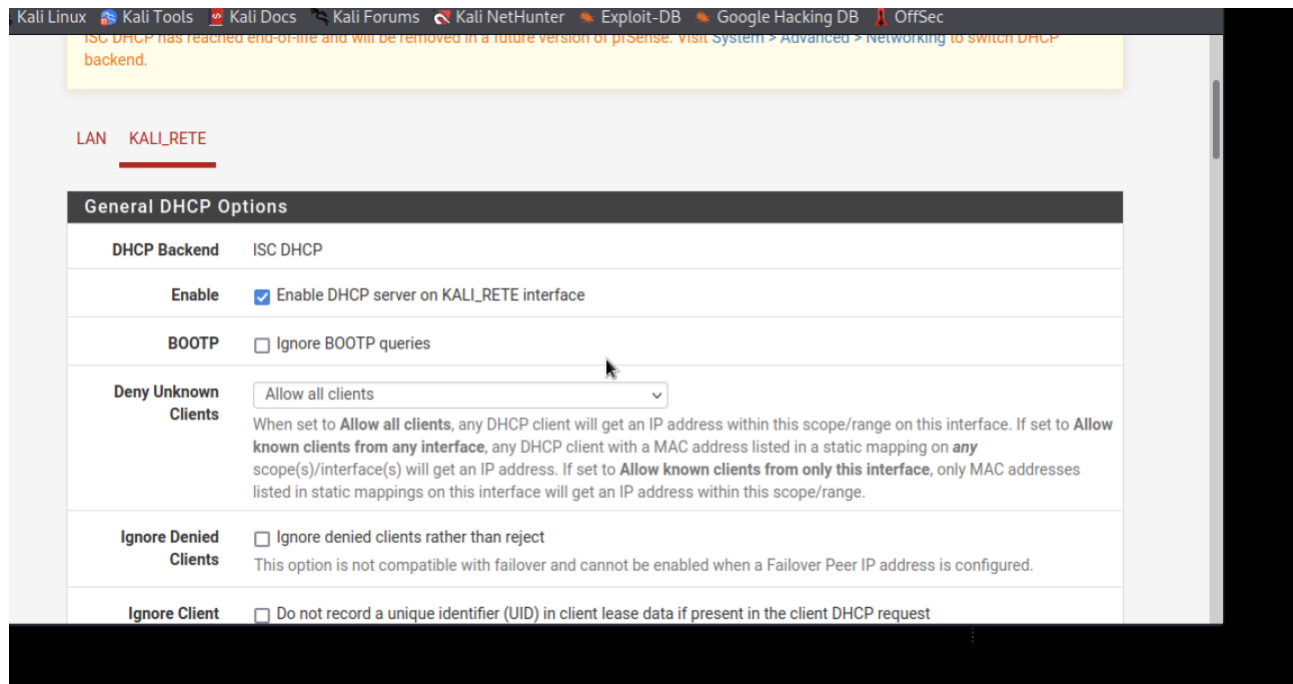
Firewall / Rules / KALI_RETE

Floating WAN LAN KALI_RETE

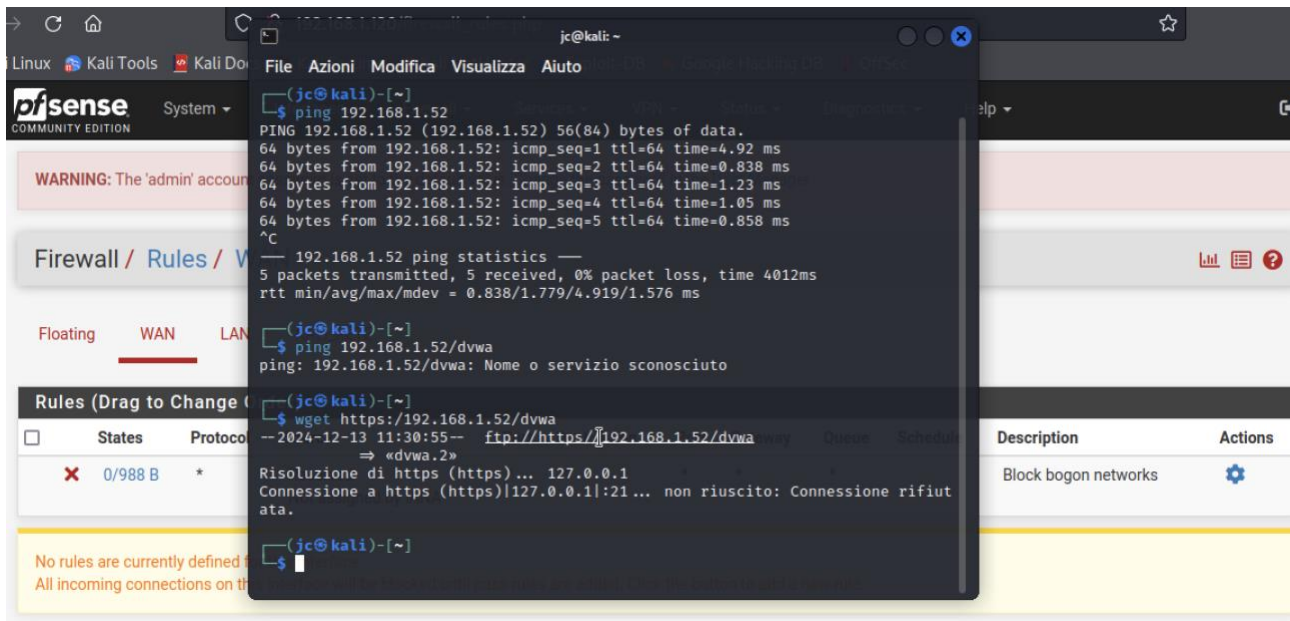
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	X	0/0 B	IPv4 TCP	192.168.2.2/24	*	192.168.1.52	80 (HTTP)	*	none		Add Delete Toggle Copy Save Separator

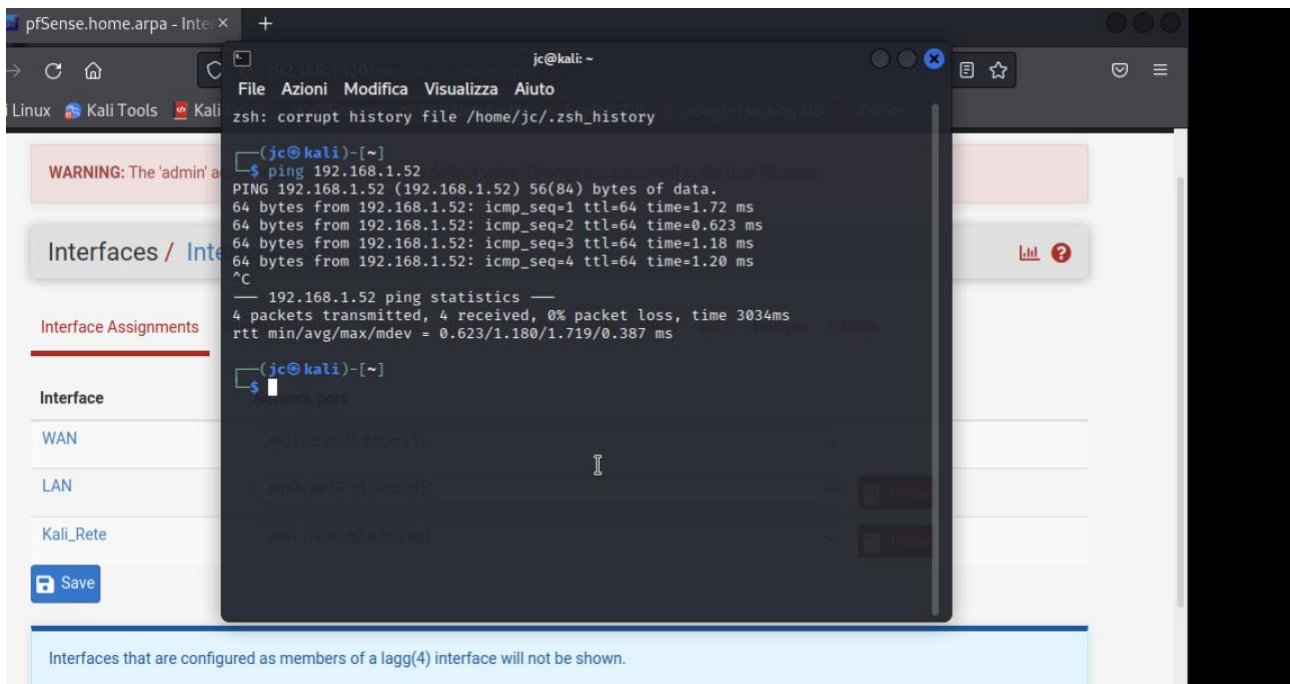
Precedentemente avevo configurato anche il DHCP per fare in modo che Kali prendesse automaticamente il nuovo ip, cosa che non è avvenuta.



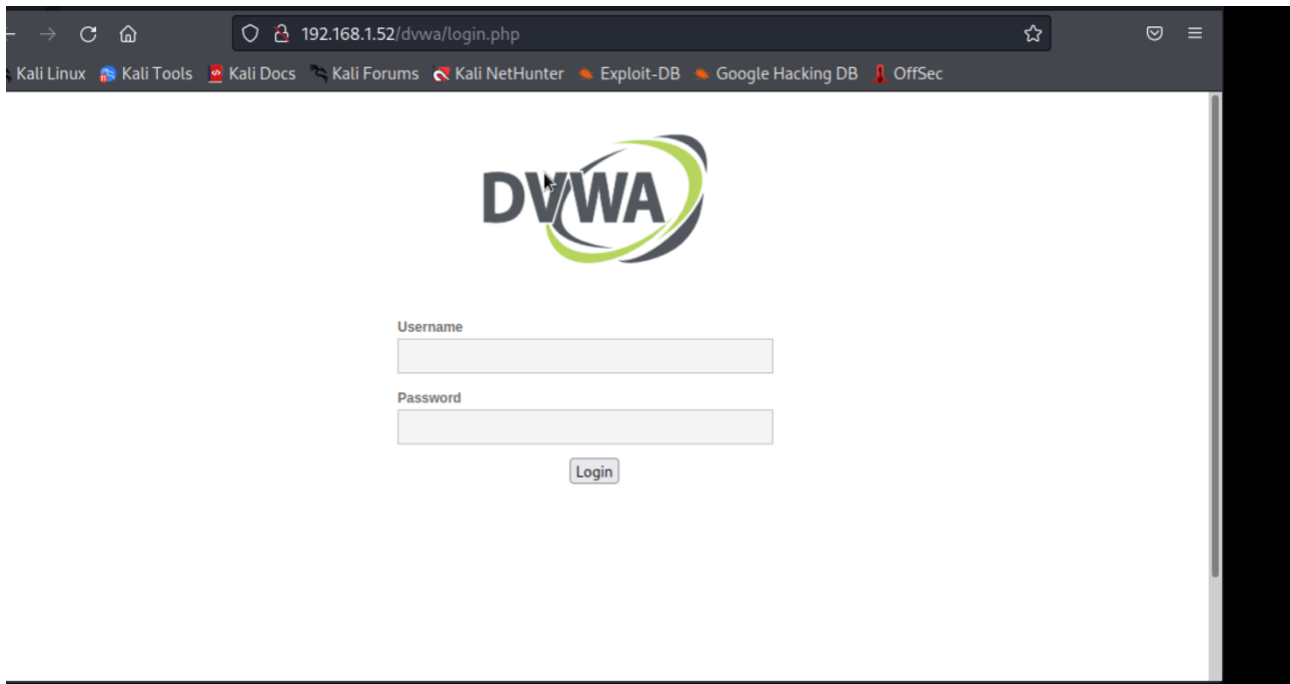
Infatti facendo il comando 'ip a' l'indirizzo ip di kali è sempre lo stesso.



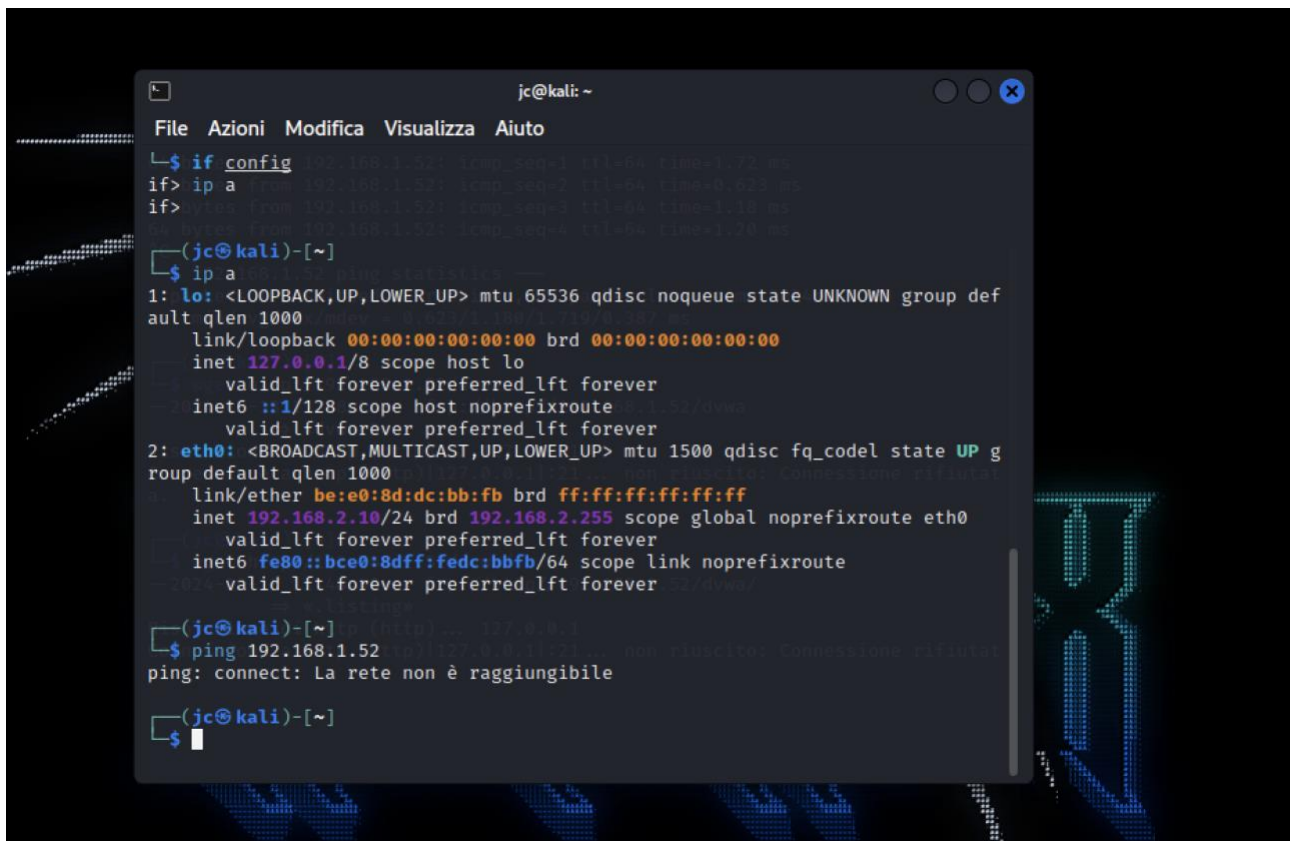
Visto che l'ip non è cambiato facendo ping a meta va tutto a buon fine e non viene bloccato nulla.

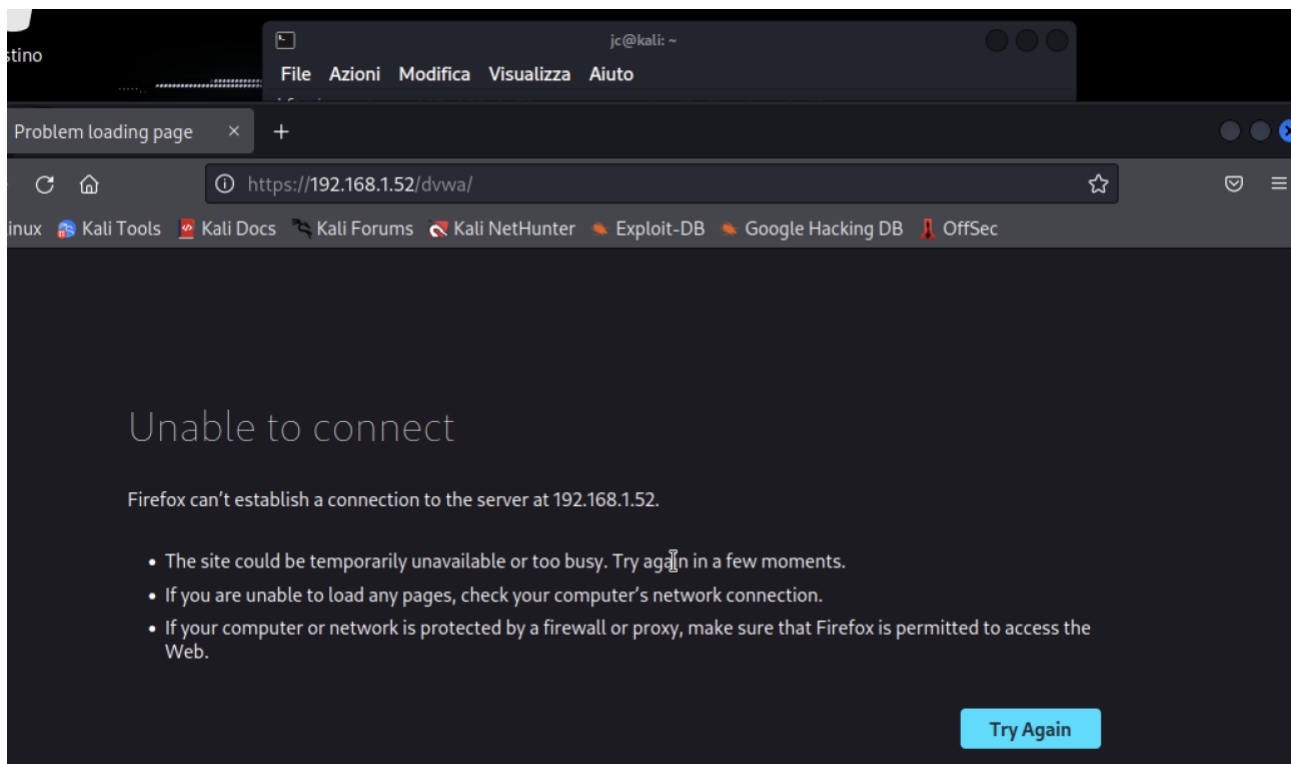


Di conseguenza cercando : 192.168.1.52/dvwa/ la pagina mi si apre e non viene bloccata dal firewall in quanto l'ip di kali non è cambiato correttamente anzi è rimasto invariato.



Ho anche provato. Cambiare ip direttamente dal terminale di kali





Non so che cosa ho sbagliato o dove.

Ci sto provando dalle 9:30 di stamattina e ora sono le 15:30 e non ci sono riuscito quindi basta. La prossima volta vorrei delle spiegazioni migliori in quanto ho capito che è un progetto e che c'è un voto, ma se non lo si risolve e poi nemmeno si spiega (ne prima e ne dopo) allora questo corso è abbastanza inutile...