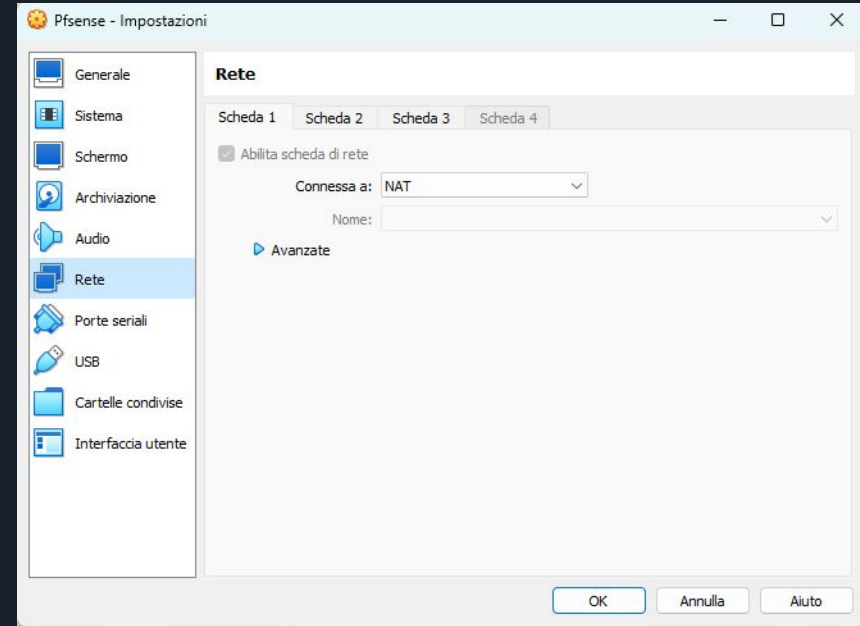




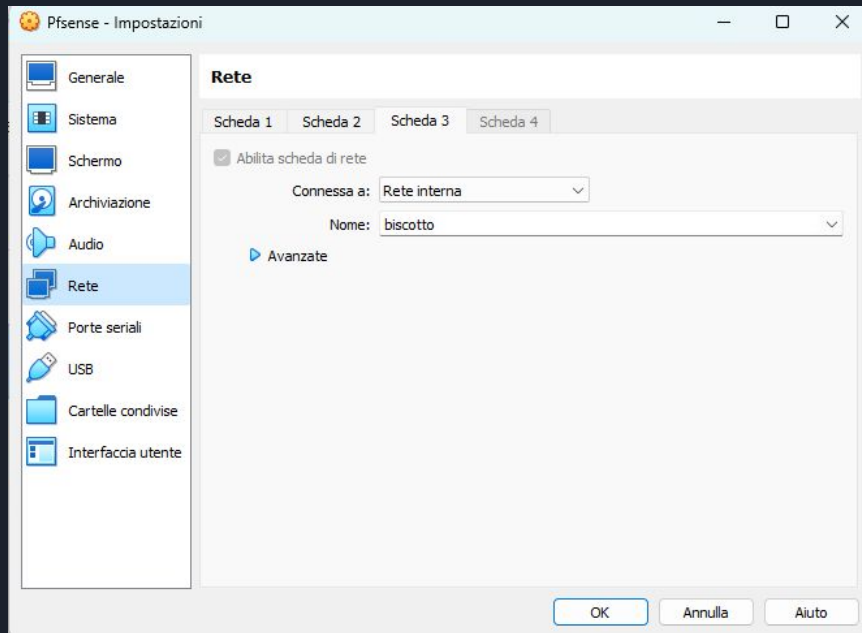
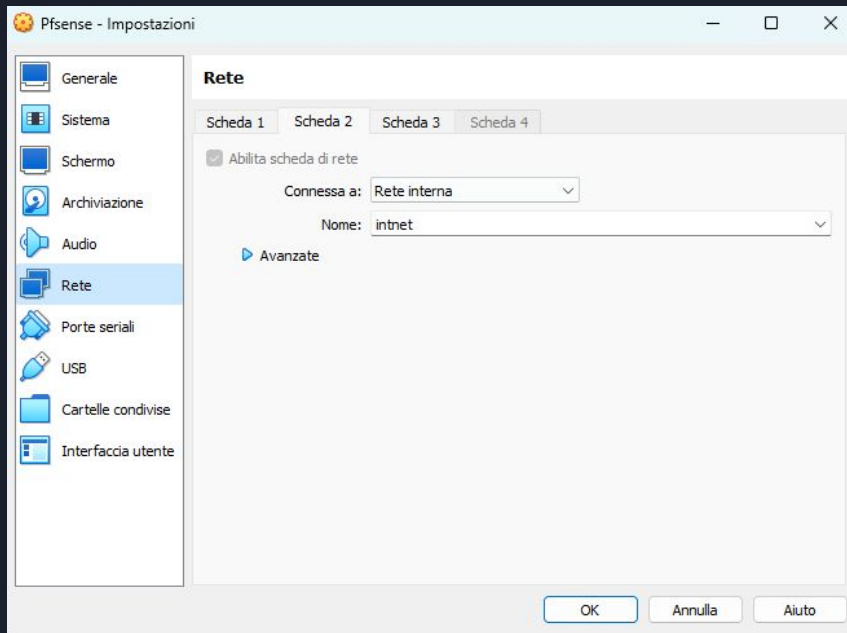
Pfsense basi

Impostazioni delle varie macchine

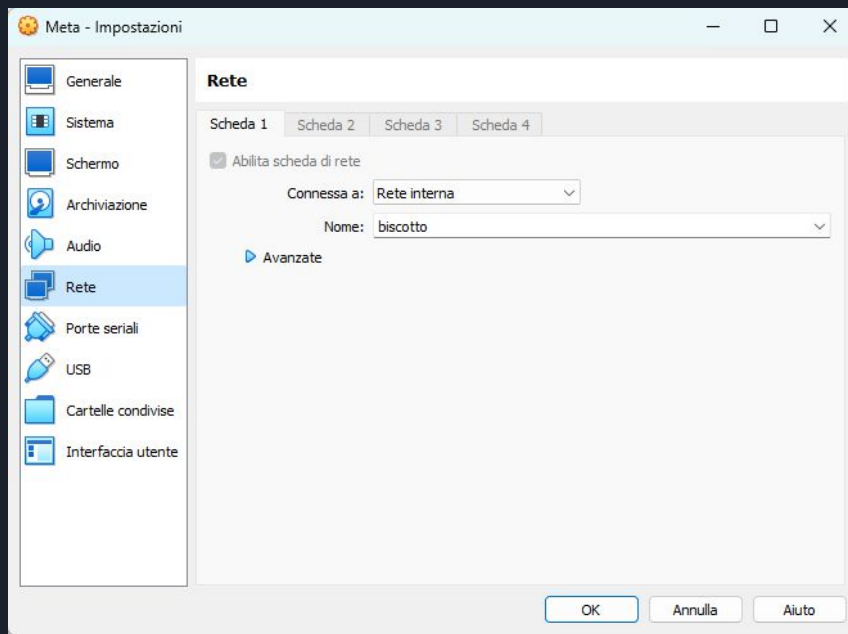
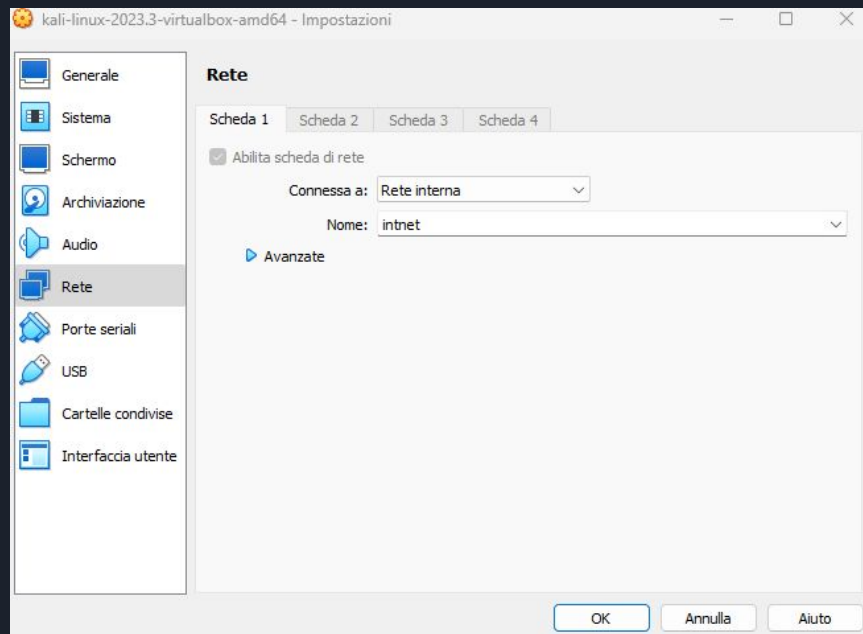
Partiamo dai settaggi, prima andiamo nel firewall Pfsense ed andiamo a settarlo aggiungendo una scheda di rete interna una per kali ed una per meta. Poi inseriamo le altre due macchine in rete interne con nomi differenti



Impostazioni delle macchine

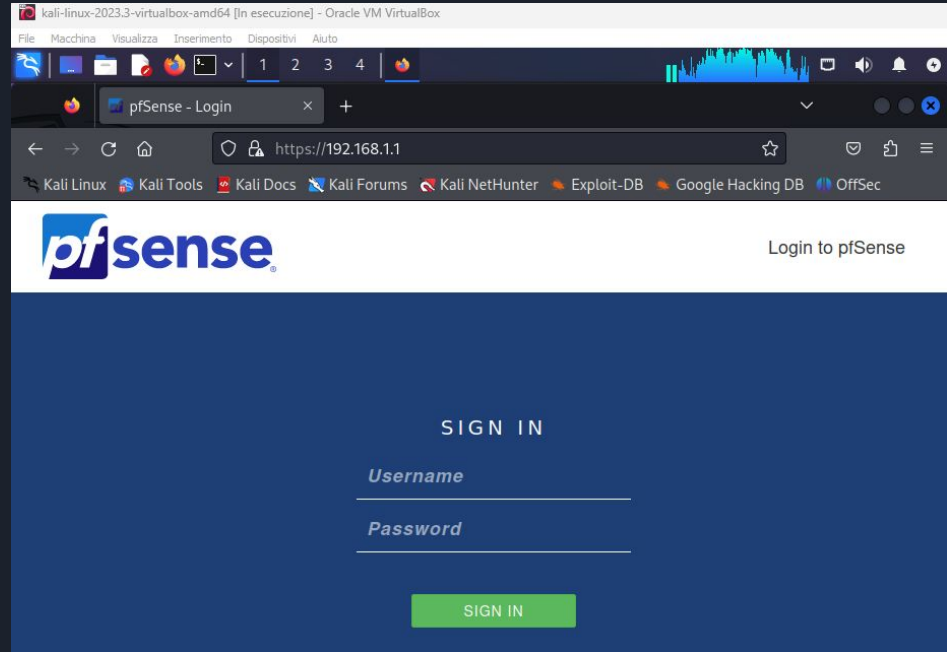


Impostazioni delle varie macchine



Configurazione Interfaccia

Andiamo su kali ed inseriamo l'ip di pfsense, entriamo con admin e pfsense.



Configurazione interfaccia

Andiamo su Interfaces > assignments.

Andiamo ad aggiungere la LAN2 per meta.
(foto destra).

Andiamo a dare la spunta ed inserie un ipv4
statico (foto sotto).

General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway [+ Add a new gateway](#)

kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

1 2 3 4

pfSense.home.arpa - Inter X

https://192.168.1.1/interfaces_assign.php

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

pfSense
COMMUNITY EDITION

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Interfaces / Interface Assignments

[Interface Assignments](#) [Interface Groups](#) [Wireless](#) [VLANs](#) [QinQs](#) [PPPs](#) [GREs](#) [GIFs](#) [Bridges](#)

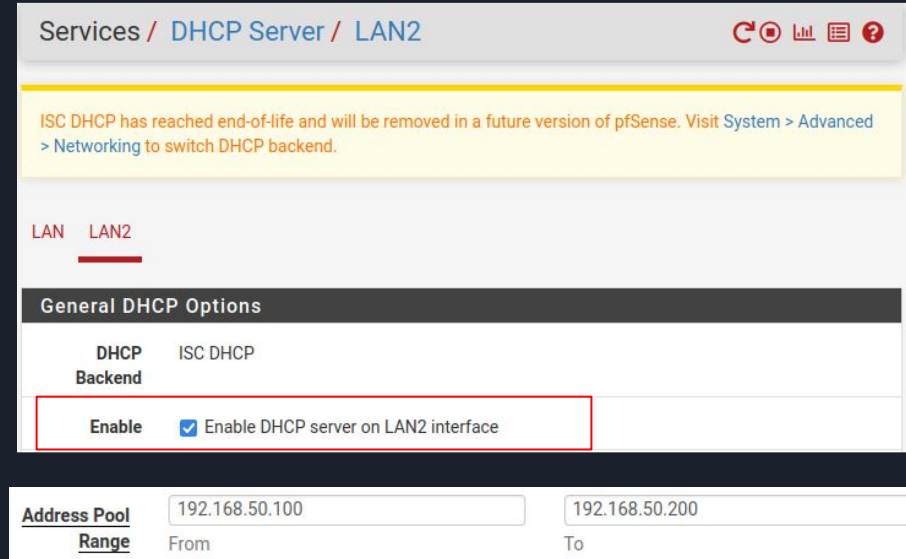
LAGGs

Interface	Network port
WAN	em0 (08:00:27:ba:f2:b9)
LAN	em1 (08:00:27:ab:92:bf) Delete
Available network ports: em2 (08:00:27:37:76:67) + Add	

[Save](#)

Configurazione server DHCP

Andiamo su Servizi > DHCP Server > LAN2.
Facciamo la spunta e modifichiamo il
“Address Pool Range”.



Services / DHCP Server / LAN2

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.

LAN LAN2

General DHCP Options

DHCP Backend

ISC DHCP

Enable ☒ Enable DHCP server on LAN2 interface

Address Pool Range

192.168.50.100 From To 192.168.50.200



Controllo ping

Su metaexploitable2 fate un sudo reboot.

Poi su kali andiamo a controllare se con le reti diverse pingano.

ip Kali (192.168.1.100).

ip Meta (192.168.50.100).

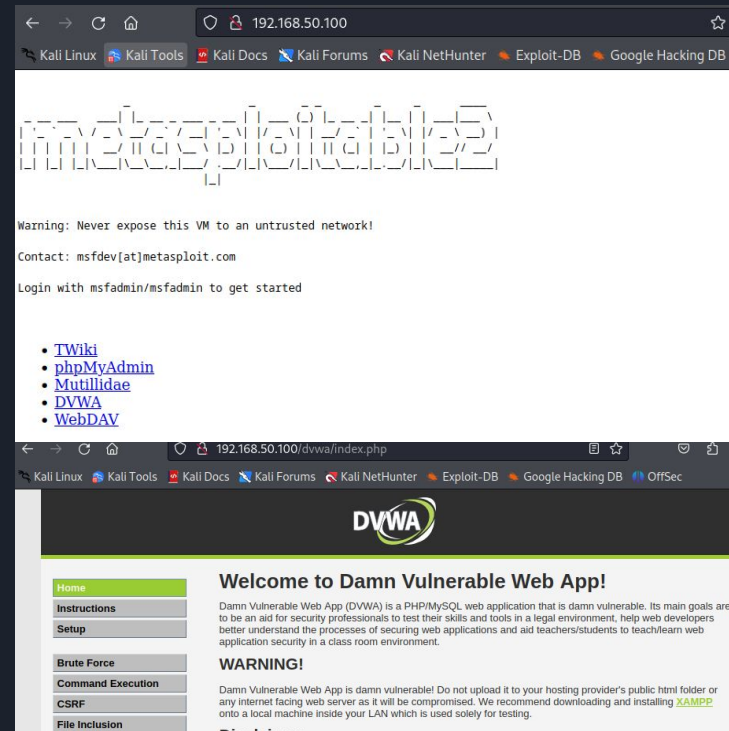
```
(kali@kali)-[~]
$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=63 time=2.70 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=4.70 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=5.85 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=63 time=6.63 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=63 time=5.24 ms
64 bytes from 192.168.50.100: icmp_seq=6 ttl=63 time=3.08 ms

64 bytes from 192.168.50.100: icmp_seq=7 ttl=63 time=4.62 ms
64 bytes from 192.168.50.100: icmp_seq=8 ttl=63 time=5.79 ms
^C
— 192.168.50.100 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 703ms
rtt min/avg/max/mdev = 2.704/4.824/6.626/1.273 ms

(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:feeb:7ef5 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
```


Controllo pagina DVWA

Inserisco L'ip di meta ed entro su metasploitable2 e su DVWA senza problemi.



Configurazione regola

Andiamo su Pfsense > Firewall > Rules > LAN.

Aggiungiamo una nuova regola con add. Le freccette indicano se la regola sarà posizionata in alto o in basso.

Firewall / Rules / LAN

Floating WAN LAN LAN2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/291 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/149 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

Configurazione regola

Inseriamo l'azione di reject, in source mettiamo l'ip di kali, e su destination l'ip di meta con la porta 80.

The screenshot shows the 'Edit Firewall Rule' configuration window. The 'Action' is set to 'Reject'. The 'Source' is configured with 'Address or Alias' set to '192.168.1.100'. The 'Destination' is configured with 'Address or Alias' set to '192.168.50.100' and 'Port Range' set to 'HTTP (80)'. The 'Destination Port Range' is further detailed with 'From' set to 'HTTP (80)' and 'To' set to 'Custom'.

Firewall / Rules / Edit

Edit Firewall Rule

Action Reject

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.

Source

Source ☐ Invert match Address or Alias 192.168.1.100 /

[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 192.168.50.100 /

Destination Port Range HTTP (80) 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.



Conclusione

Il risultato sarà che non saremo in grado di entrare su DVWA.

