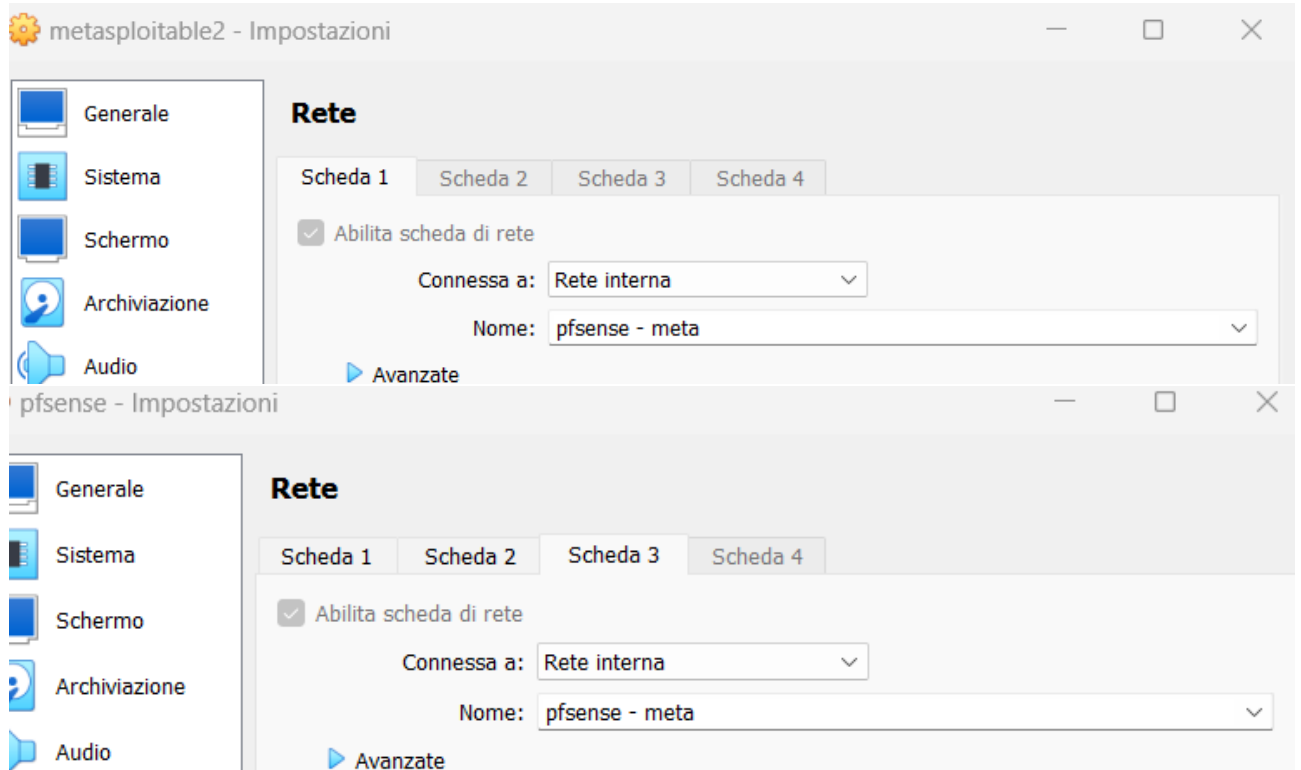
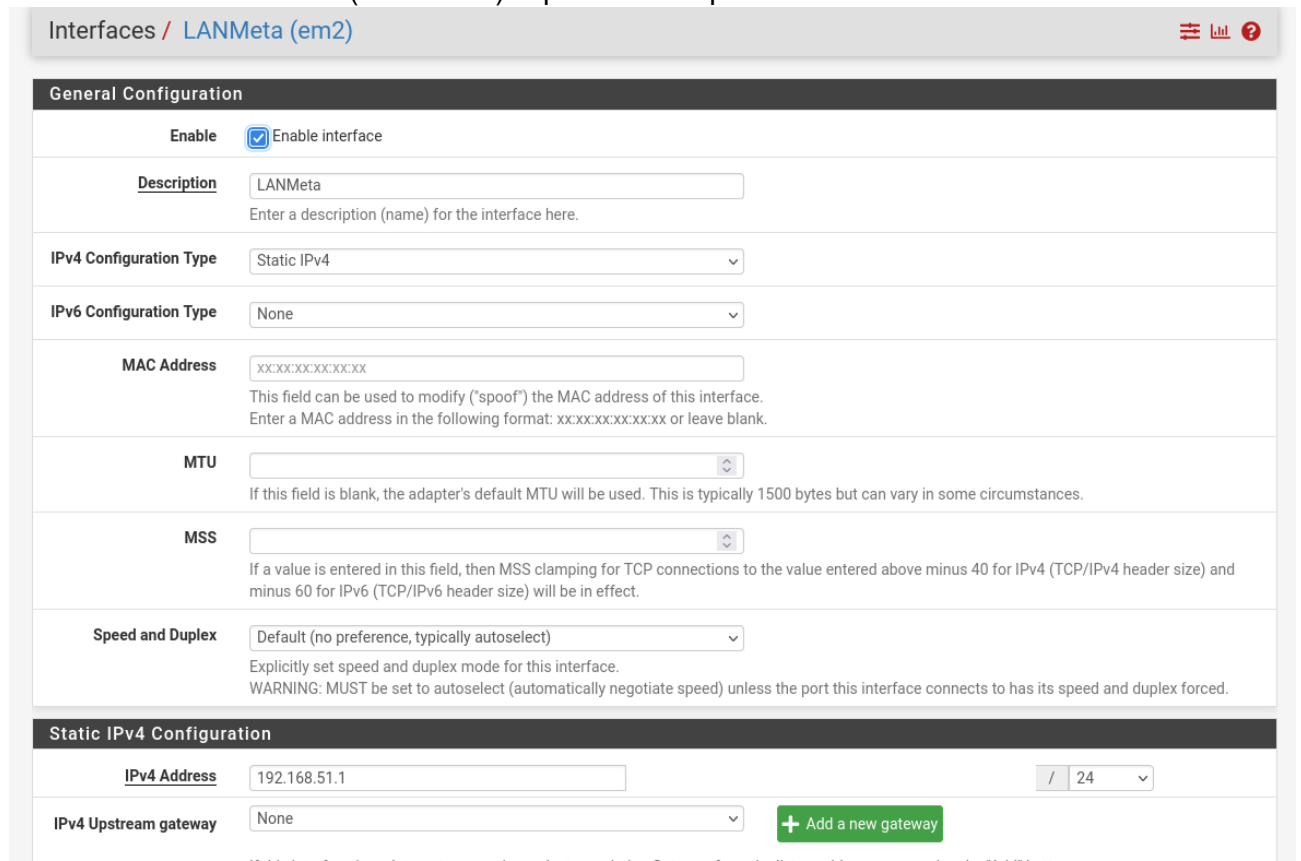


Esercizio L5 – S1

1. Ho creato una nuova rete per pfsense e metasploitable 2:



2. Ho creato una nuova rete (LANMETA) in pfsense e impostato un DHCP:



General DHCP Options

DHCP Backend

ISC DHCP

Enable

☒ Enable DHCP server on LANMETA interface

BOOTP

☐ Ignore BOOTP queries

Deny Unknown Clients

Allow all clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed in a static mapping on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.

Ignore Denied Clients

☐ Ignore denied clients rather than reject

This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore Client Identifiers

☐ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool

Subnet

192.168.51.0/24

Subnet Range

192.168.51.1 - 192.168.51.254

Address Pool Range

192.168.51.100

192.168.51.150

From

To

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools

+ Add Address Pool

If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

3. IP Metasploitable 2

```

eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 08:00:27:8c:1b:a5 brd ff:ff:ff:ff:ff:ff
inet 192.168.51.100/24 brd 192.168.51.255 scope global eth0
inet6 fe80::a00:27ff:fe8c:1ba5/64 scope link

```

IP Kali

```

eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 08:00:27:2b:ca:da brd ff:ff:ff:ff:ff:ff
inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
inet6 fe80::a00:27ff:fe2b:cada/64 scope link proto kernel_ll

```

- Ho creato delle regole per permettere alla metasploitable di comunicare sulla nuova lan creata (LANMETA)

Floating

WAN

LAN

LANMETA

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/840 B	IPv4 ICMP any		LANMETA subnets	*	*	*	*	none	Anchor Edit Copy Delete Toggle
<input type="checkbox"/>	✓	1/2 KiB	IPv4 *		LANMETA subnets	*	*	*	*	none	Default allow LAN to any rule Anchor Edit Copy Delete Toggle
<input type="checkbox"/>	✓	0/0 B	IPv6 *		LANMETA subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule Anchor Edit Copy Delete Toggle

↑ Add

↓ Add

🗑 Delete

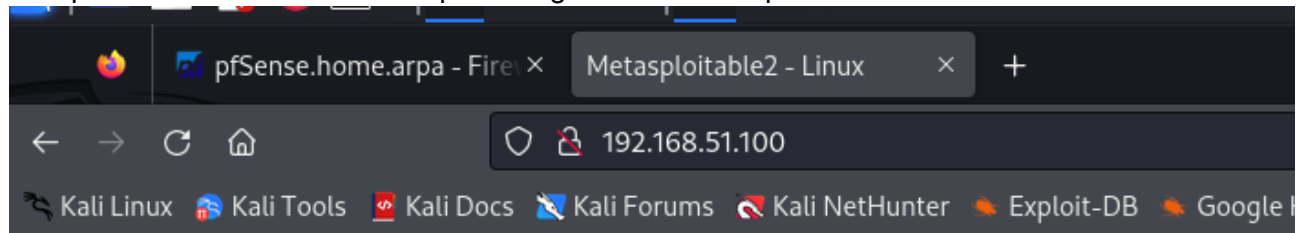
🔄 Toggle

📄 Copy

💾 Save

+ Separator

5. Ho aperto il browser su kali linux per collegarmi alla metasploitable



metasploitable

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

6. Ho creato una regola nel firewall per bloccare l'accesso alla metasploitable da kali

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 TCP
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Address or Alias 192.168.50.100 /

[Display Advanced](#)

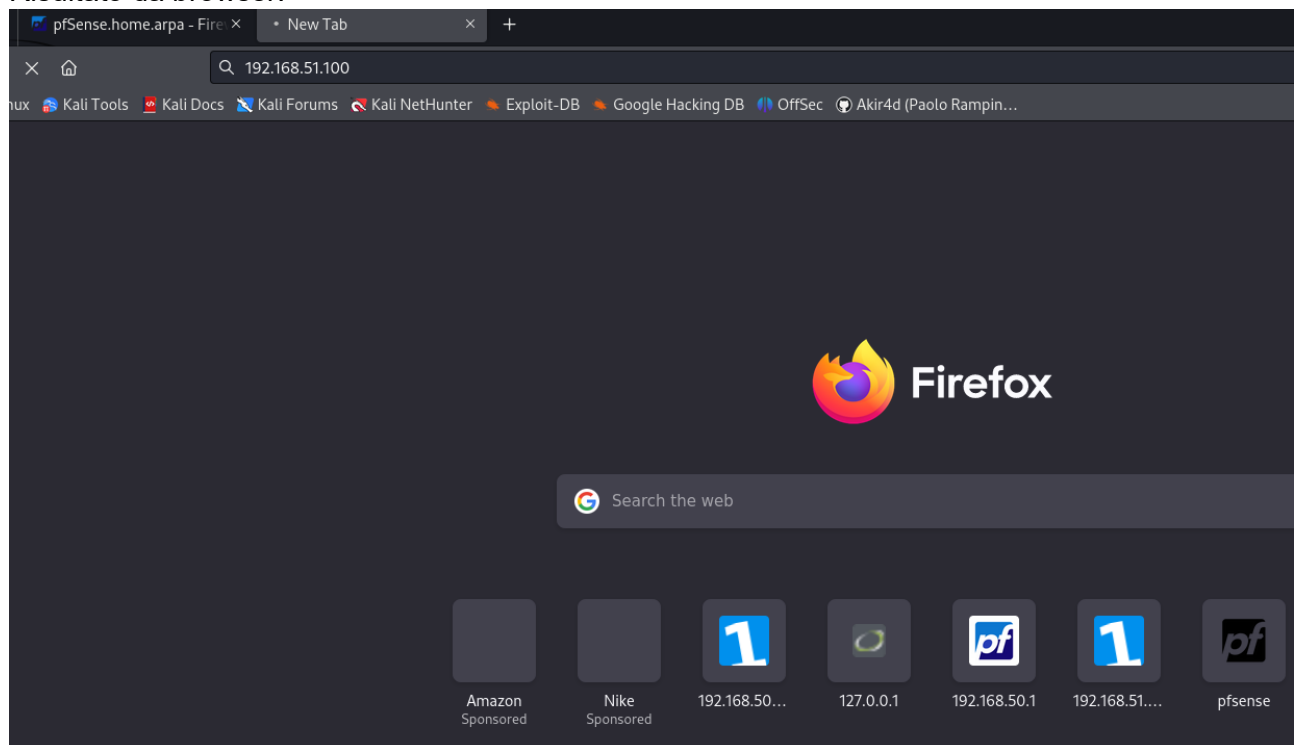
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination ☐ Invert match Address or Alias 192.168.51.100 /

Destination Port Range any Custom HTTP (80) Custom

Risultato da browser:



Risultato con nmap:

```
(kali@kali)-[~]  
$ nmap -A 192.168.51.100  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 11:35 EDT  
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 3.37 seconds
```

7. Ho modificato la regola con un reject e questo è il risultato:

