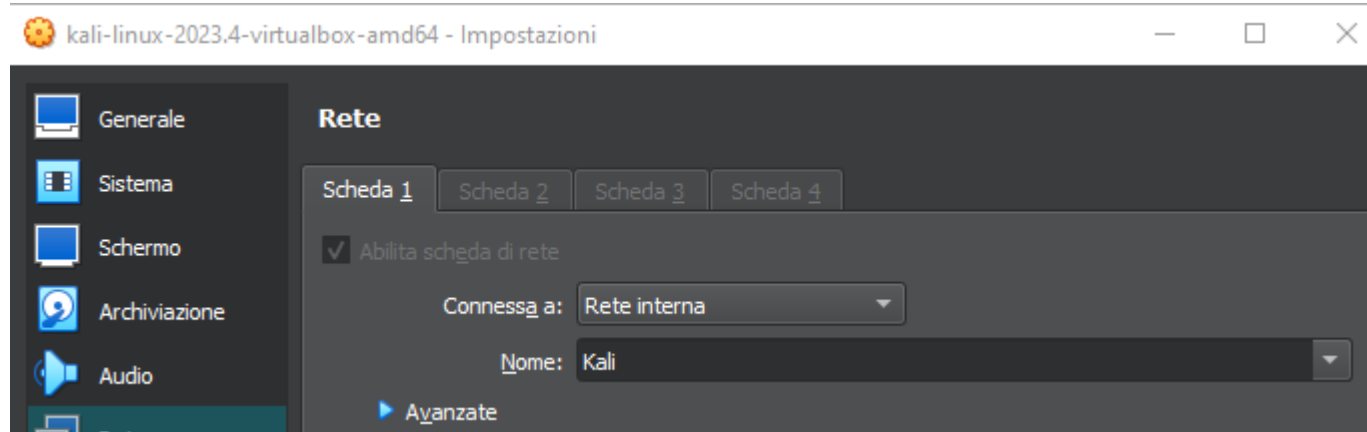
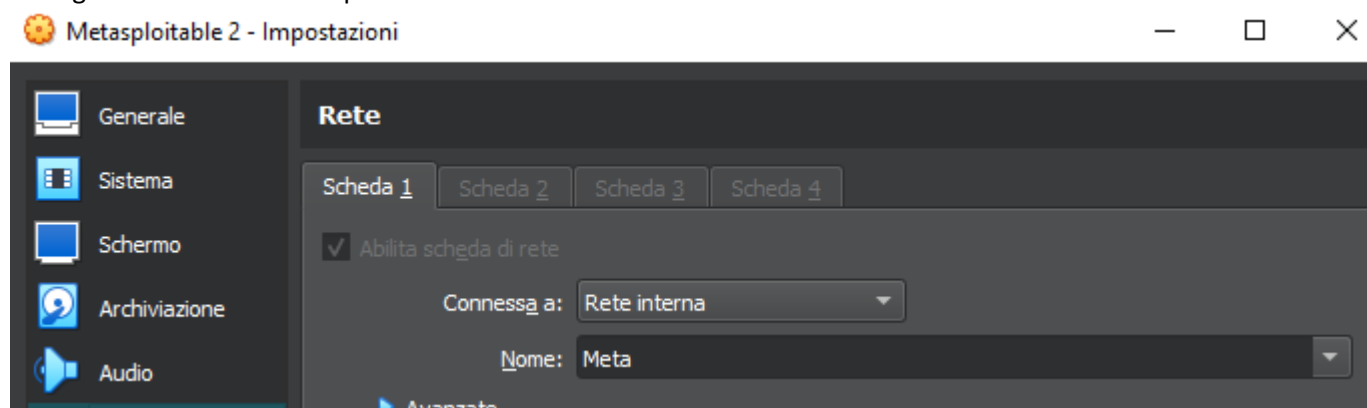


Configurata la rete di Kali Linux su Rete Interna "kali"

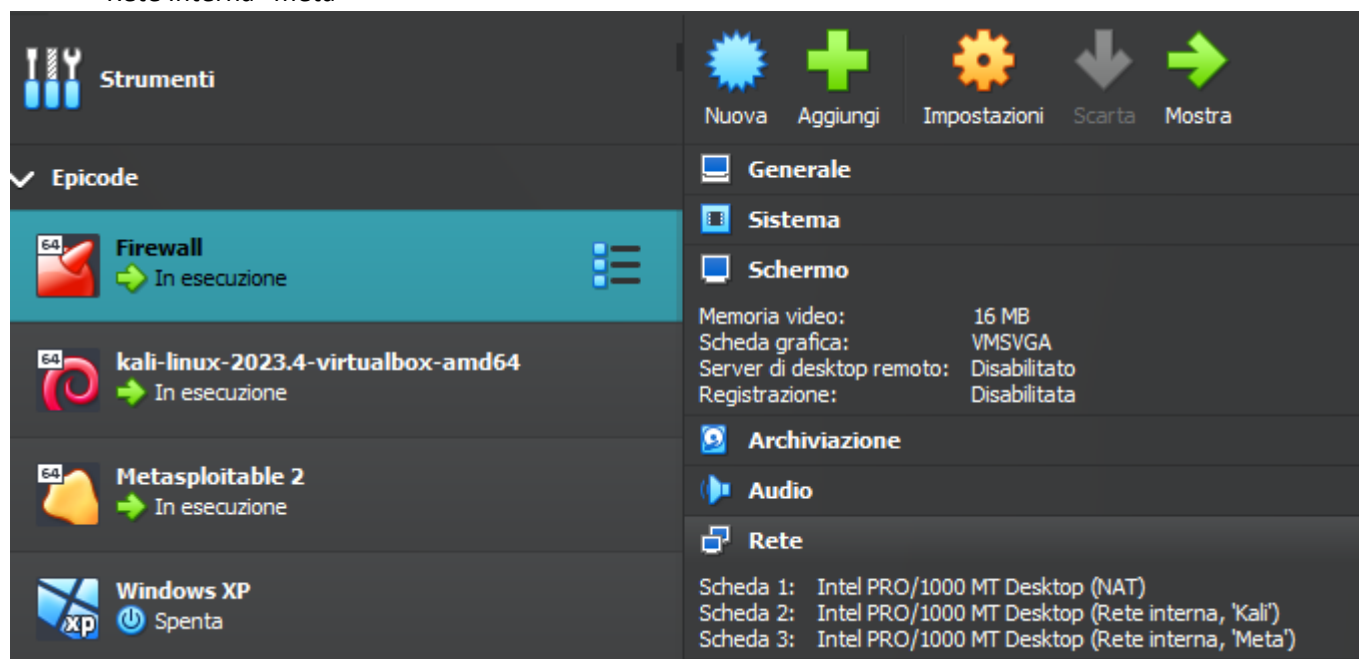


Configurata la rete di Metasploitable2 su Rete Interna "meta"



Configurata la rete di PfSense con 3 schede di rete

- Nat
- Rete Interna "kali"
- Rete Interna "meta"



Dopo aver avviato le macchine Kali Linux e PfSense è stato aperto il browser di Kali, in modo da poter accedere alla pagina di PfSense.

Sulla pagina di PfSense è stata creata una nuova interfaccia di rete andando su “Interfaces Assignments” chiamata LAN2 e abilitata, assegnando un indirizzo IPv4 192.168.50.1 / 24.

Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="LAN2"/> <small>Enter a description (name) for the interface here.</small>
IPv4 Configuration Type	<input type="text" value="Static IPv4"/>
IPv6 Configuration Type	<input type="text" value="None"/>
MAC Address	<input type="text" value="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) a minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.</small>
Speed and Duplex	<input type="text" value="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 forced.</small>
Static IPv4 Configuration	
IPv4 Address	<input type="text" value="192.168.50.1"/> / 24

Modificata l'impostazione di rete della macchina Metasploitable2 da static a DHCP

```
Metasploitable 2 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7  File: /etc/

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see the man page of
# the /etc/network/interfaces file.

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp
```

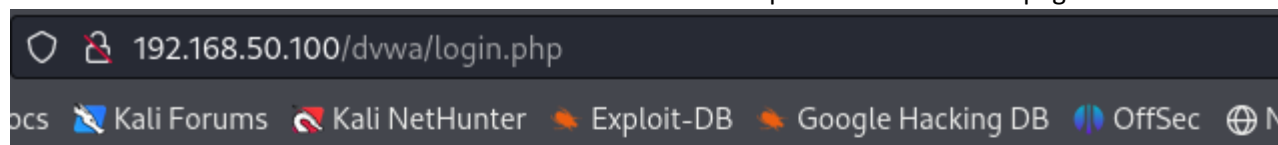
Su PfSense è stata abilitata l'interfaccia LAN2 in DHCP assegnando un range di indirizzi da 192.168.50.100 a 192.168.50.200

DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<div>Allow all clients</div> <p>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.</p>
Ignore Denied Clients	<input type="checkbox"/> 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	<input type="checkbox"/> 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	192.168.1.0/24
Subnet Range	192.168.1.1 - 192.168.1.254
Address Pool Range	<div>192.168.1.10</div> <div>From</div> <div>192.168.1.245</div> <div>To</div>

Da Kali Linux è stato verificato che c'era connessione con Metasploitable visitando la pagina della DVWA



Username

Password


Login

Da PfSense è stata creata una regola per bloccare l'accesso sulla DVWA

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	192.168.1.100	/	
---------------	---------------------------------------	------------------	---------------	---	--

 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	<input type="checkbox"/> Invert match	Address or Alias	192.168.50.100	/	
--------------------	---------------------------------------	------------------	----------------	---	--

Destination Port Range	HTTP (80)		HTTP (80)	
	From	Custom	To	Custom

Dove:

- **Action:** viene gestito il traffico, “**Block**”
- **Interface:** la rete da dove arrivano i pacchetti, “**LAN**”
- **Address Family:** La versione dei protocolli IP a cui applicare le policy, “**IPv4**”
- **Protocol:** il tipo di protocollo, “**TCP**”
- **Source:** L'indirizzo IP sorgente, “**192.168.1.100**”
- **Destination:** L'indirizzo IP da bloccare, “**192.168.50.100**”
- **Destination Port Range:** Le porte di destinazione da bloccare, “**HTTP (80)**”

Dopo aver impostato la regola ho riprovato a collegarmi all'indirizzo IP, ma senza riuscirci

