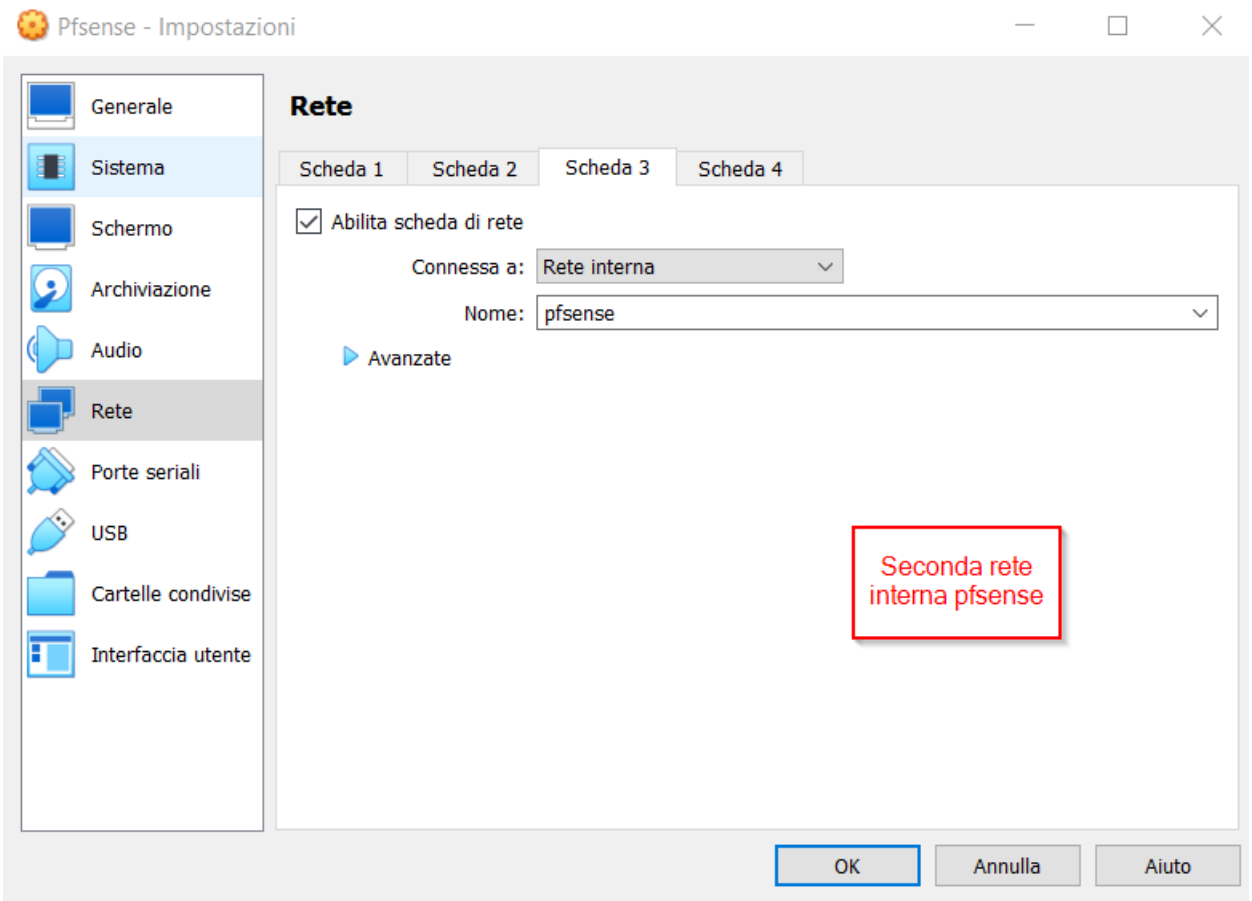
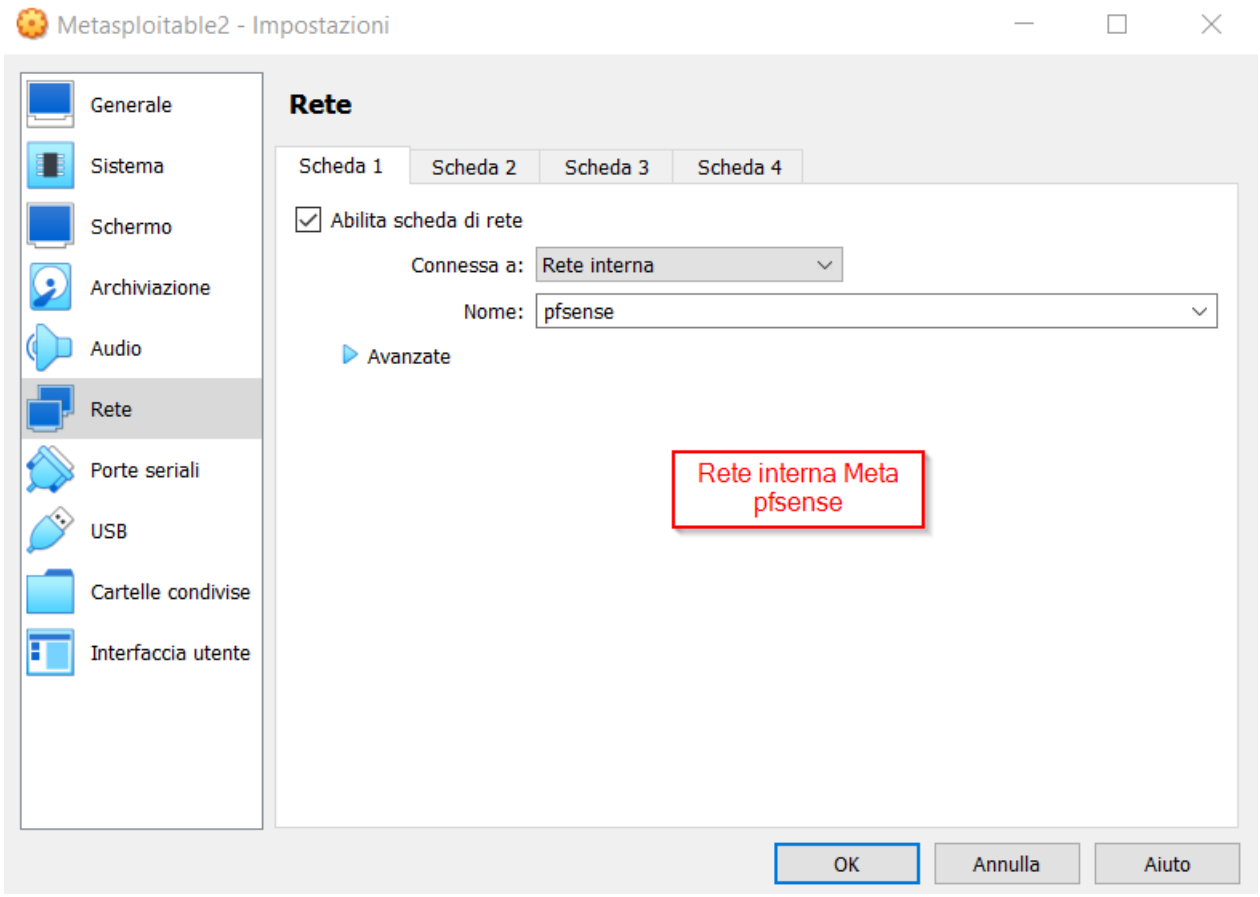
ESERCIZIO W9D4

L'esercizio seguente ci porterà a creare un'eccezione nel policy set di pfsense, il nostro firewall. Negheremo lo scambio di pacchetti in partenza da Kali verso Meta.

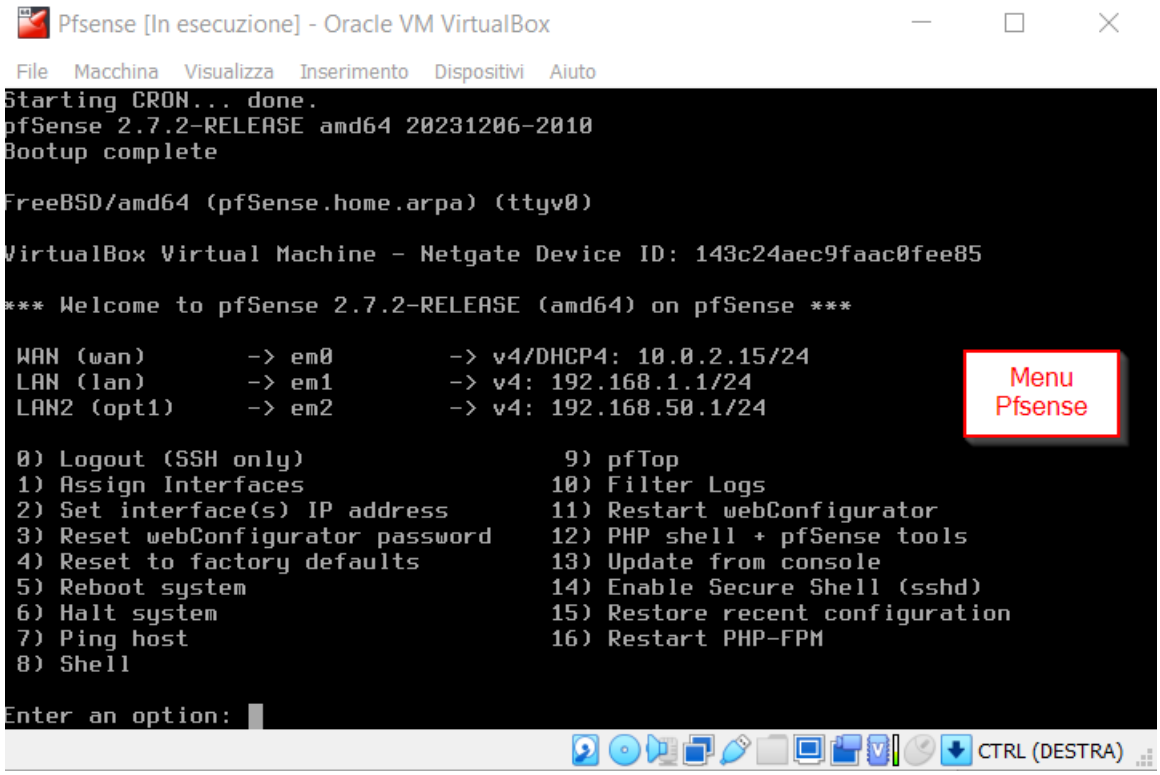
Configurazione macchine

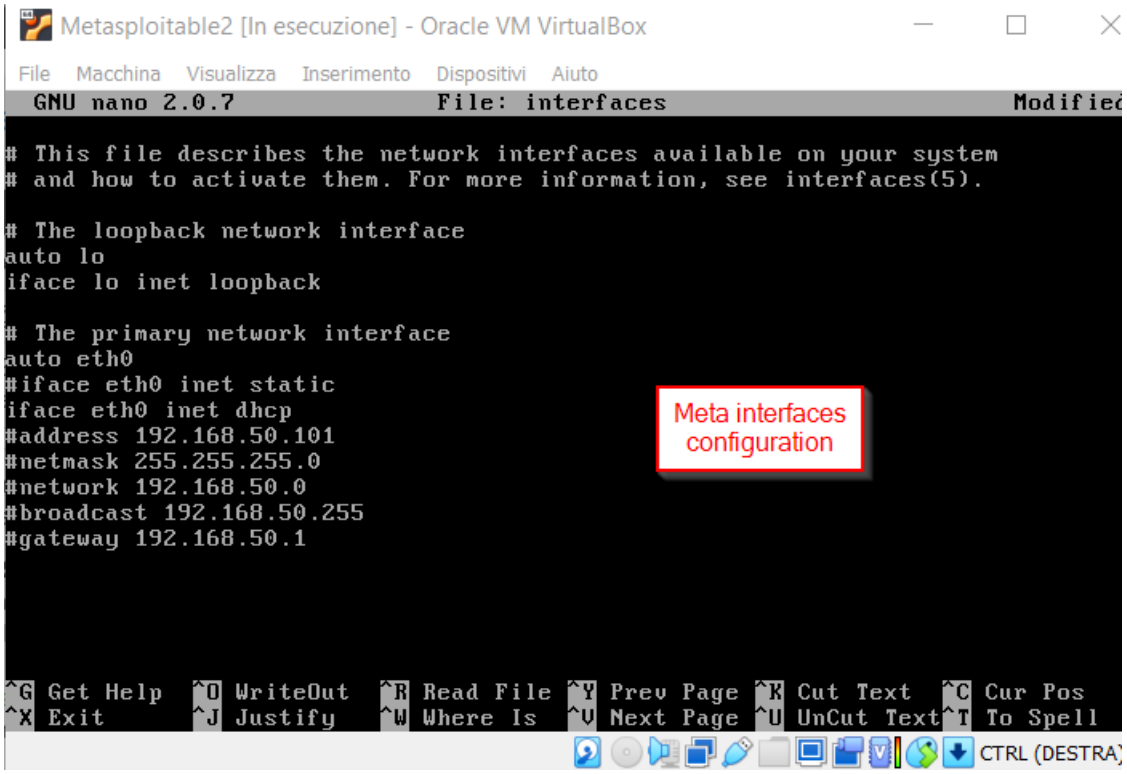
Iniziamo con il preparare pfsense andando ad aggiungere un secondo indirizzo LAN. Se avremo aperto la terza rete su VM, ci basterà seguire le opzioni di settaggio di set interface ed attivare cosi il nuovo servizio avente come IP 192.168.50.100. Ricordiamoci anche di cambiare la spunta nome per Meta in pfsense, altrimenti non sarà possibile per Meta ricevere un indirizzo dal DHCP.



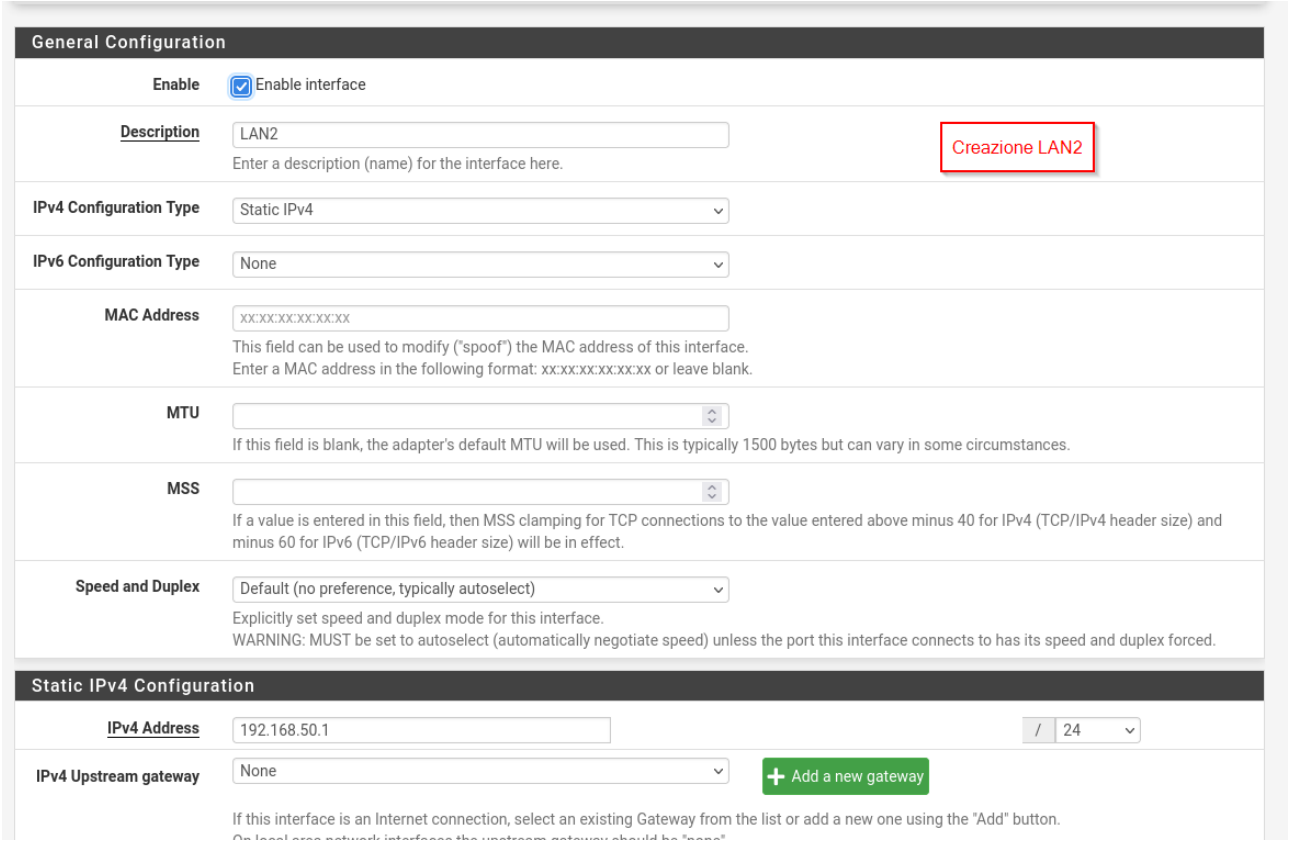


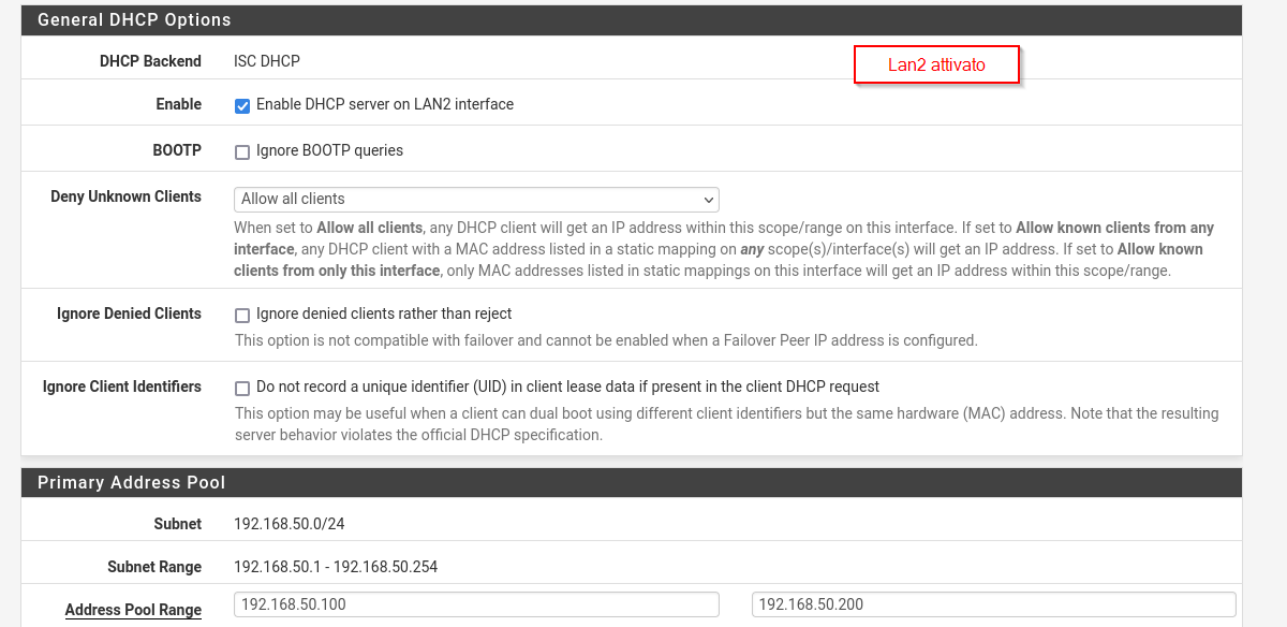
Per fare in modo che pfsense assegni un certo range di indirizzi alla macchina, modifichiamo inoltre l'interfaccia di rete di Meta.





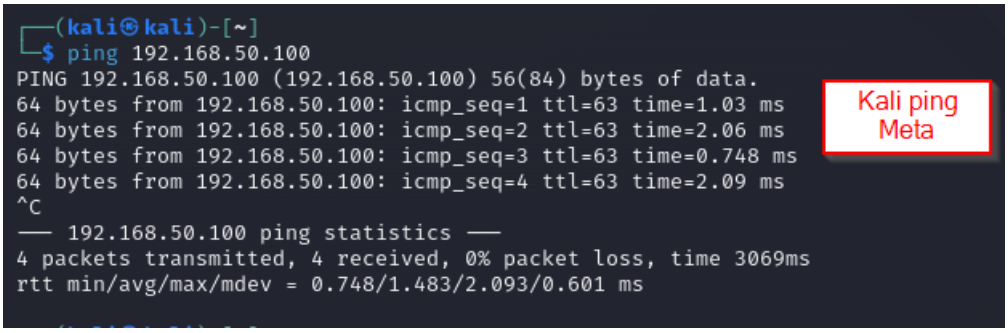
Su pfsense invece ci muoviamo come segue. Assicuriamoci di rendere operativa la nuova rete grazie ai dati essenziali. Attivazione interfacce, servizio DHCP, range utilizzabili, etc.

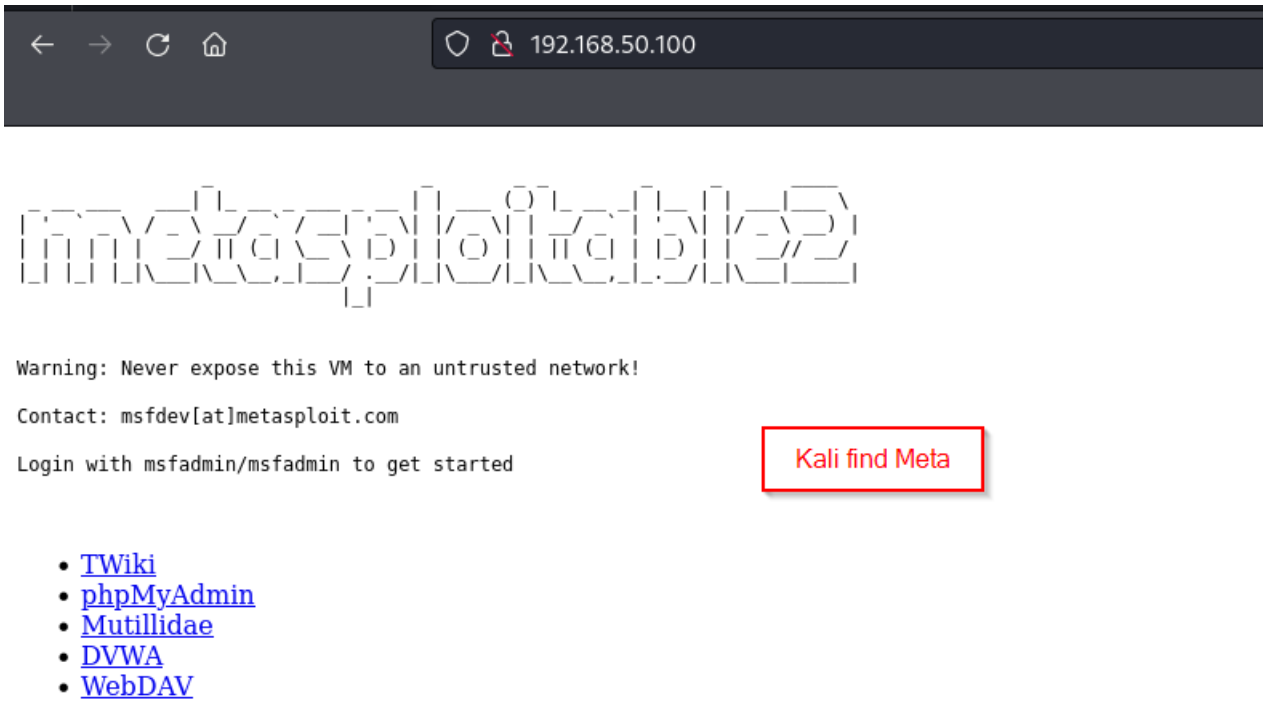




Test connettività tra Kali e Meta

Prima di passare al policy set, controlliamo che le macchine riescano a comunicare tra di loro nonostante si trovino su reti diverse. Pinghiamo Meta con Kali e cerchiamo di accadere con il browser al server Metasploitable2.

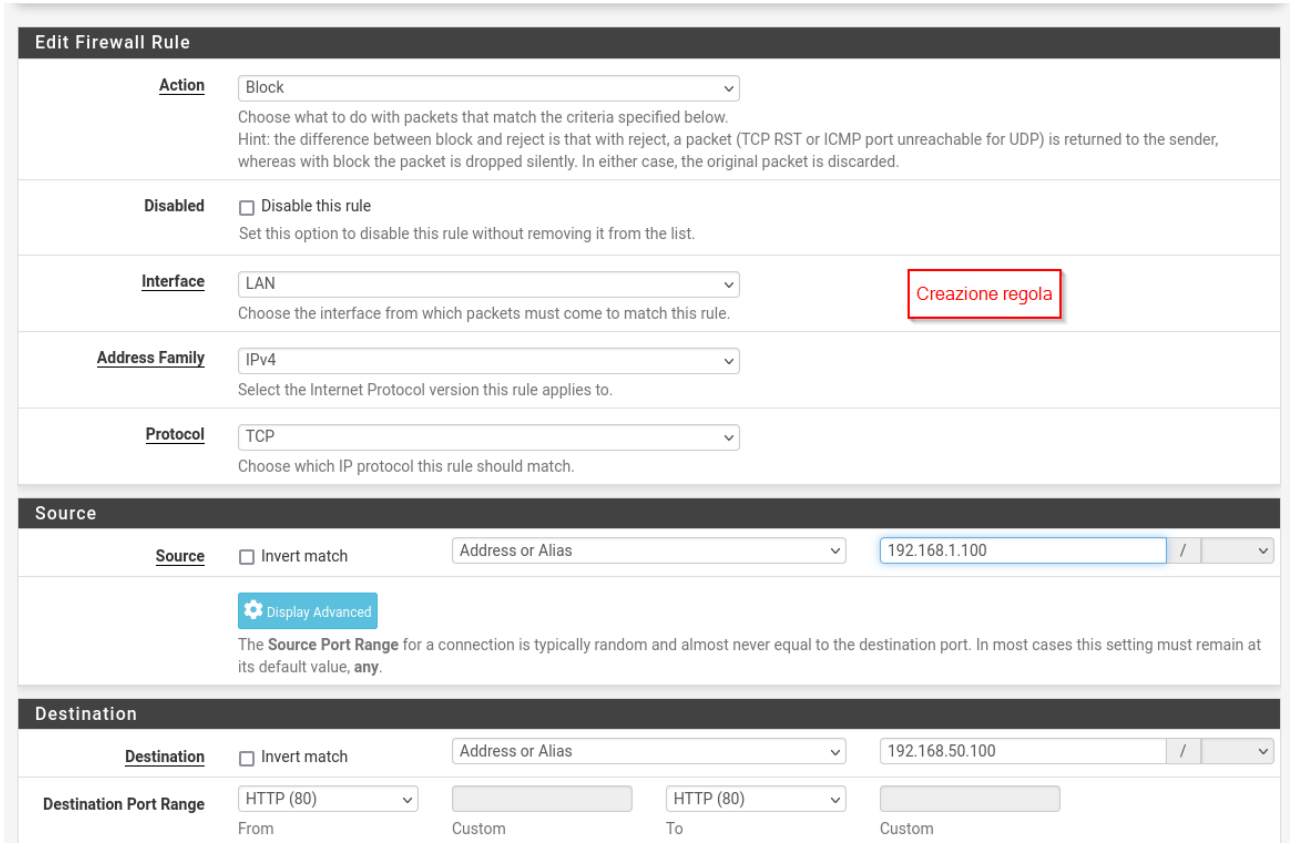


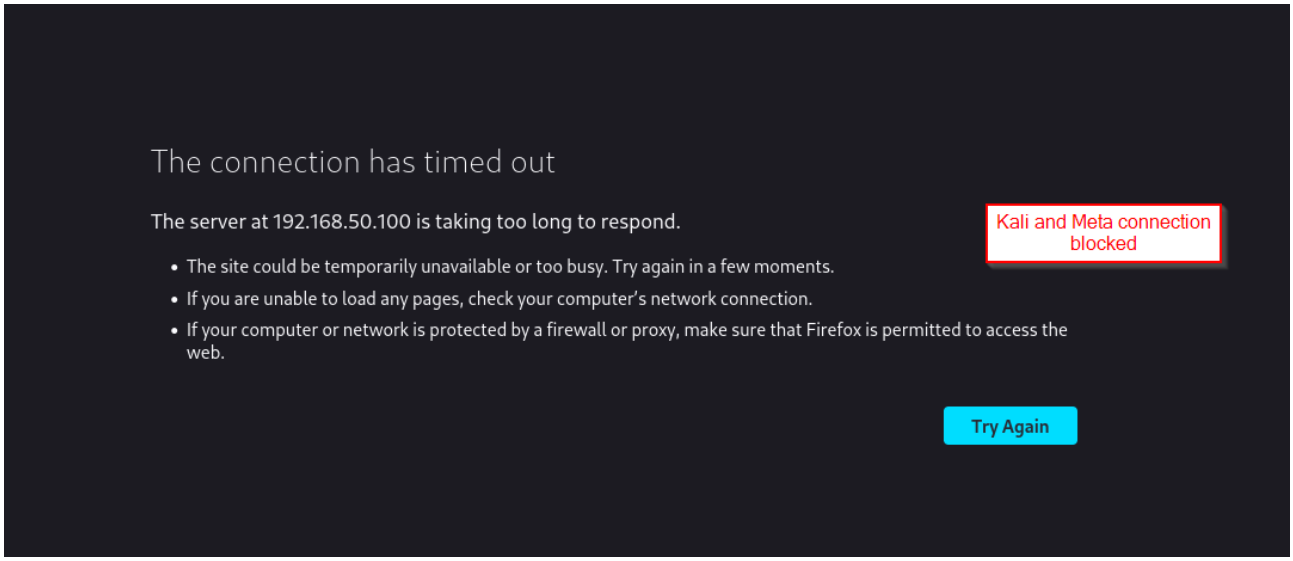


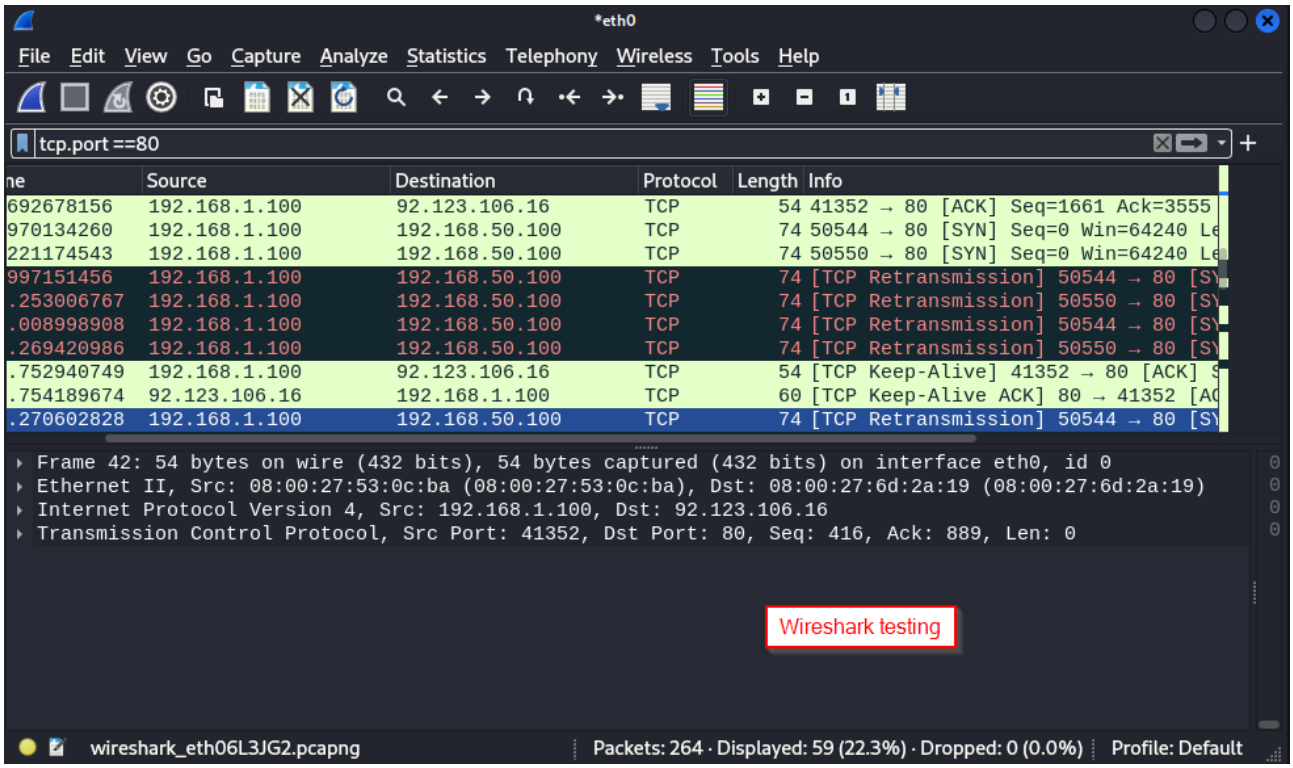
Tutto funziona. Ora, non ci resta che inserire l'eccezione usando pfsense.

Negazione pacchetti

Andiamo a specificare porta e indirizzi interessanti nella regola del policy set riguardante la rete LAN1. In questo modo Kali non sarà in grado di connettersi al server web Metasploitable2. Nel caso vogliamo un ulteriore conferma, Wireshark ci fornisce, nelle sue analisi numerosi tentativi di connessione falliti, come nell'ultima figura sottostante.


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.
Creazione regola
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
192.168.1.100
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)
From
Custom
HTTP (80)
To
Custom


The connection has timed out
The server at 192.168.50.100 is taking too long to respond.
Kali and Meta connection blocked
The site could be temporarily unavailable or too busy. Try again in a few moments.
If you are unable to load any pages, check your computer's network connection.
If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.
Try Again


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port ==80
ne Source Destination Protocol Length Info
692678156 192.168.1.100 92.123.106.16 TCP 54 41352 → 80 [ACK] Seq=1661 Ack=3555
970134260 192.168.1.100 192.168.50.100 TCP 74 50544 → 80 [SYN] Seq=0 Win=64240 Le
221174543 192.168.1.100 192.168.50.100 TCP 74 50550 → 80 [SYN] Seq=0 Win=64240 Le
997151456 192.168.1.100 192.168.50.100 TCP 74 [TCP Retransmission] 50544 → 80 [SY
.253006767 192.168.1.100 192.168.50.100 TCP 74 [TCP Retransmission] 50550 → 80 [SY
.008998908 192.168.1.100 192.168.50.100 TCP 74 [TCP Retransmission] 50544 → 80 [SY
.269420986 192.168.1.100 192.168.50.100 TCP 74 [TCP Retransmission] 50550 → 80 [SY
.752940749 192.168.1.100 92.123.106.16 TCP 54 [TCP Keep-Alive] 41352 → 80 [ACK] S
.754189674 92.123.106.16 192.168.1.100 TCP 60 [TCP Keep-Alive ACK] 80 → 41352 [AC
.270602828 192.168.1.100 192.168.50.100 TCP 74 [TCP Retransmission] 50544 → 80 [SY
Frame 42: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: 08:00:27:53:0c:ba (08:00:27:53:0c:ba), Dst: 08:00:27:6d:2a:19 (08:00:27:6d:2a:19)
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 92.123.106.16
Transmission Control Protocol, Src Port: 41352, Dst Port: 80, Seq: 416, Ack: 889, Len: 0
Wireshark testing
wireshark_eth06L3JG2.pcapng
Packets: 264 · Displayed: 59 (22.3%) · Dropped: 0 (0.0%)
Profile: Default