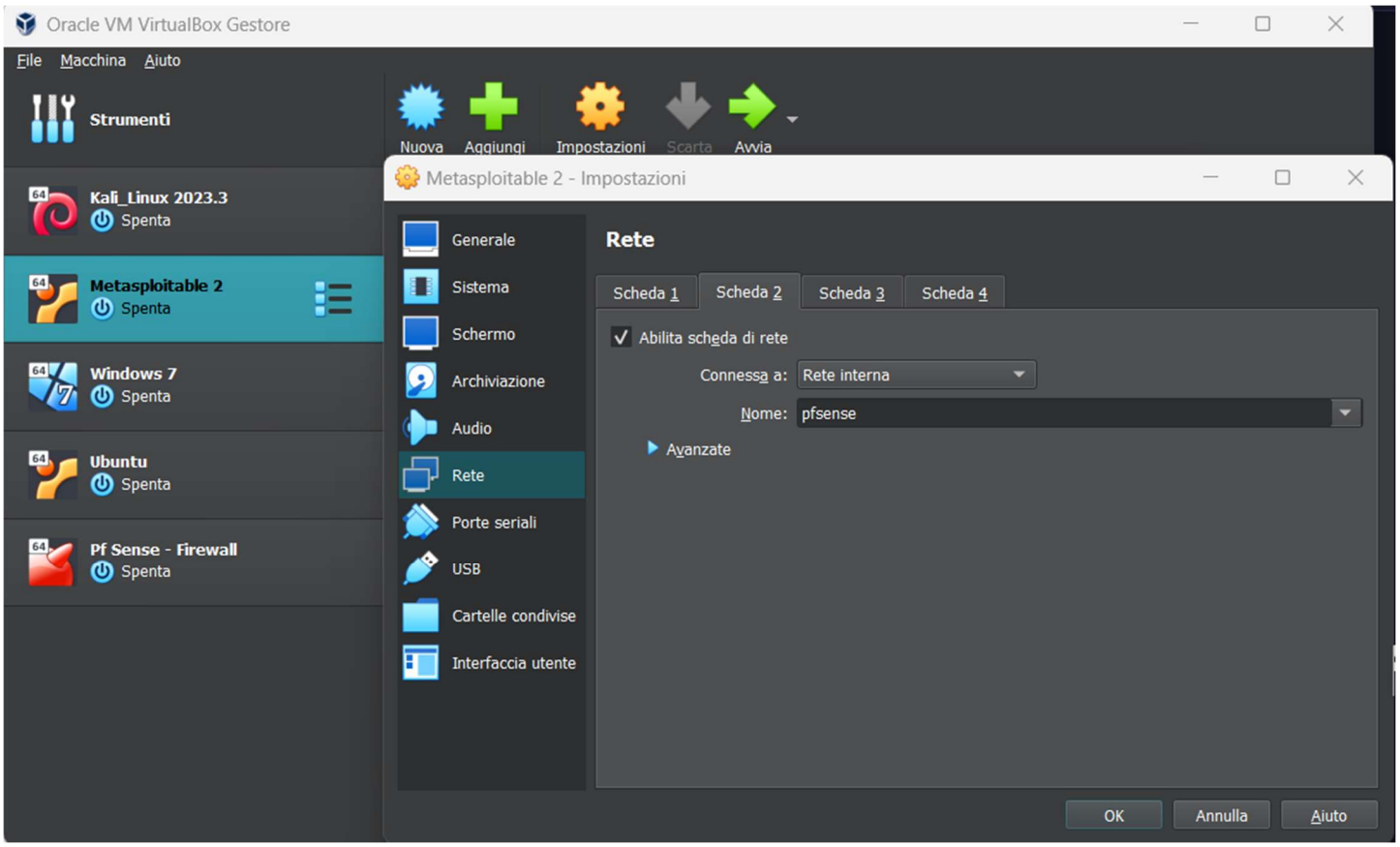
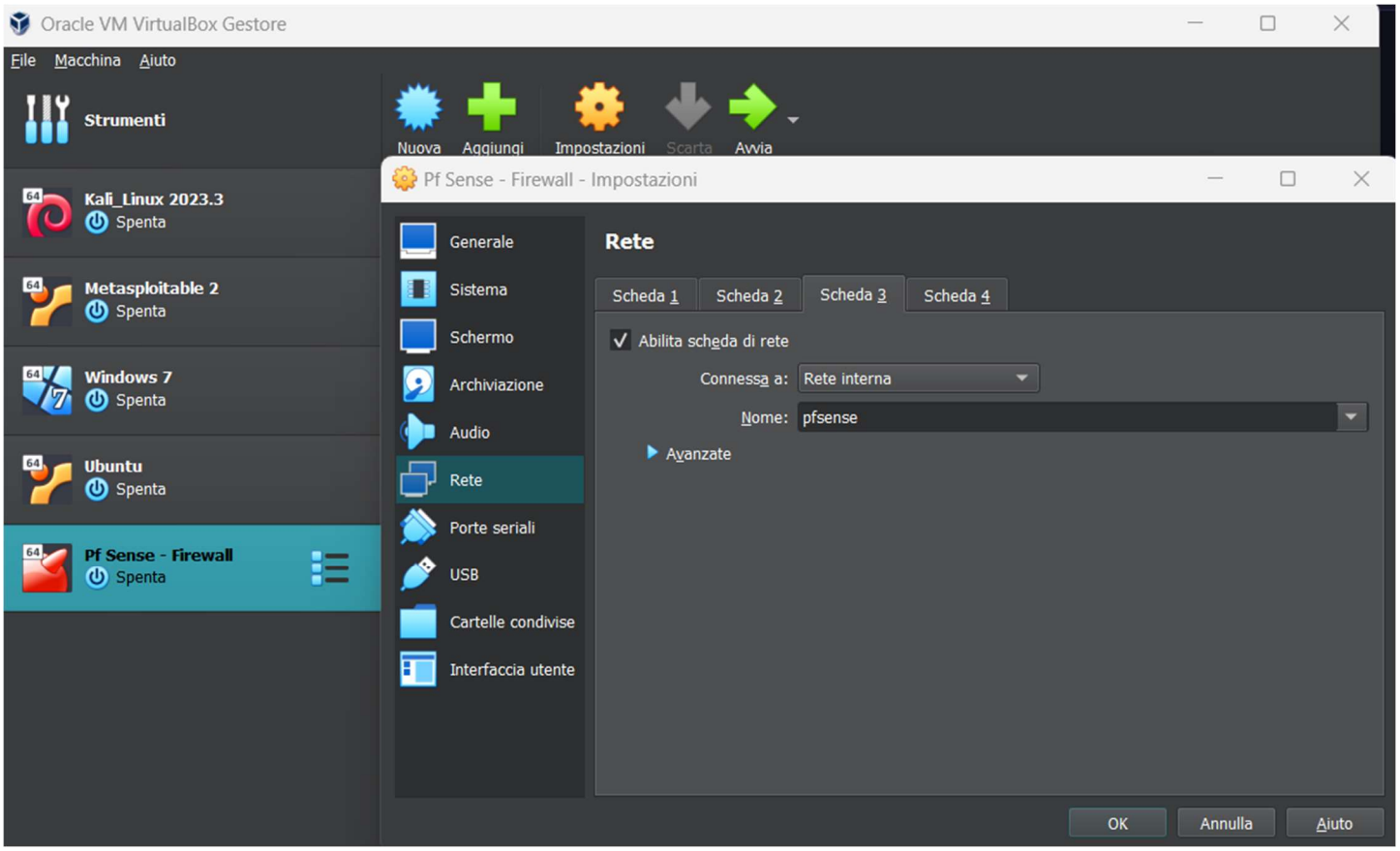
CREAZIONE POLICY PFSENSE

Creo delle nuove schede di rete su macchina Metasploitable e su PfSense





Configuro la nuova scheda di rete in PfSense con servizio DHCP Attivo e che abbia come rete 192.168.51.0/24

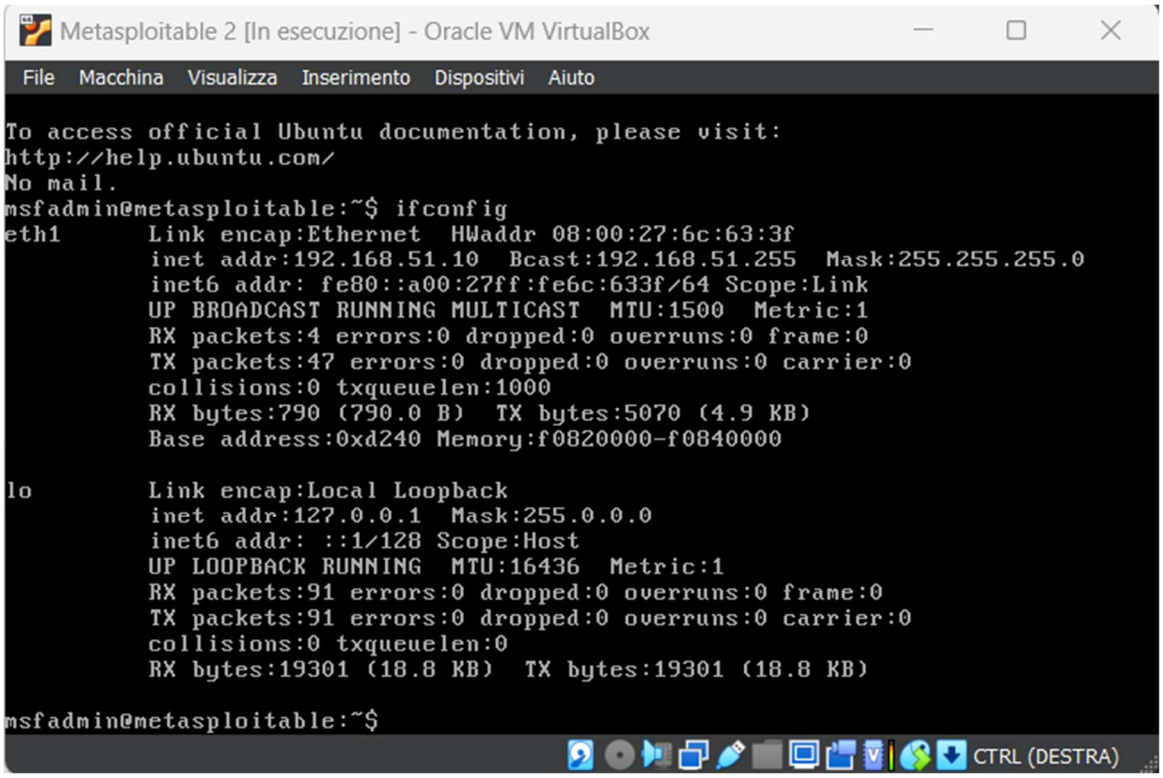
LAN LAN2

General DHCP Options

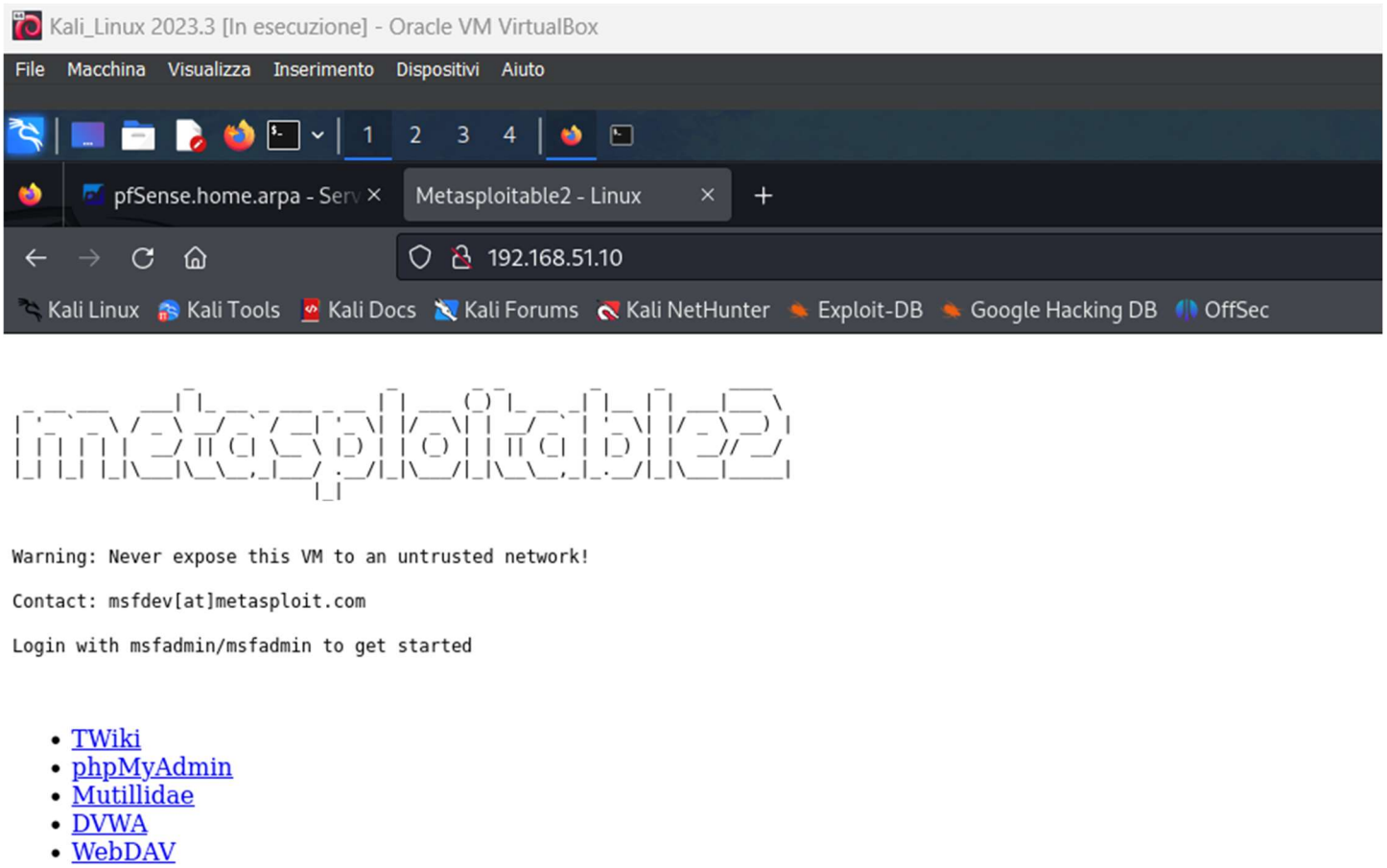
DHCP Backend	Kea DHCP
Enable	☑ Enable DHCP server on LAN2 interface
Deny Unknown Clients	Allow all clients When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a 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 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

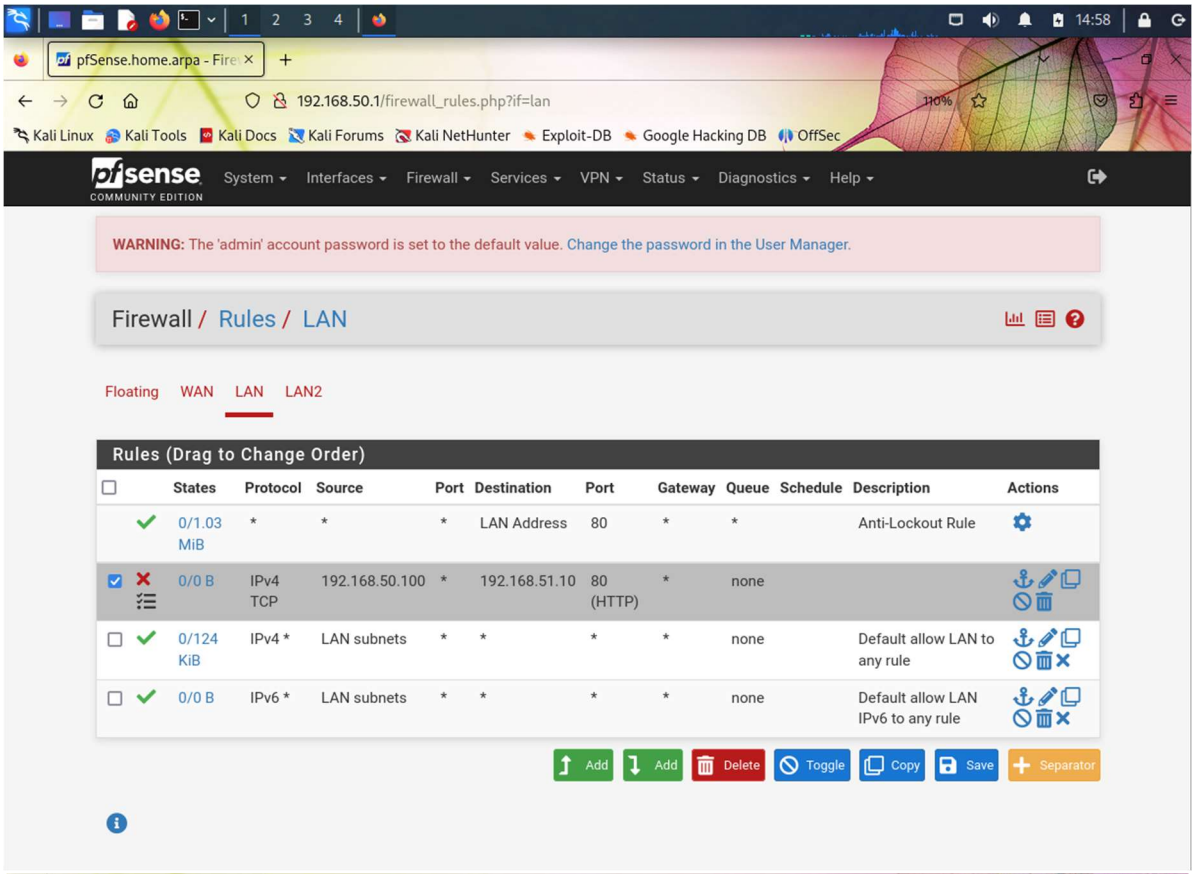
Subnet	192.168.51.0/24
Subnet Range	192.168.51.1 - 192.168.51.254
Address Pool Range	192.168.51.10 (From) — 192.168.51.20 (To) The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools	+ Add Address Pool If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

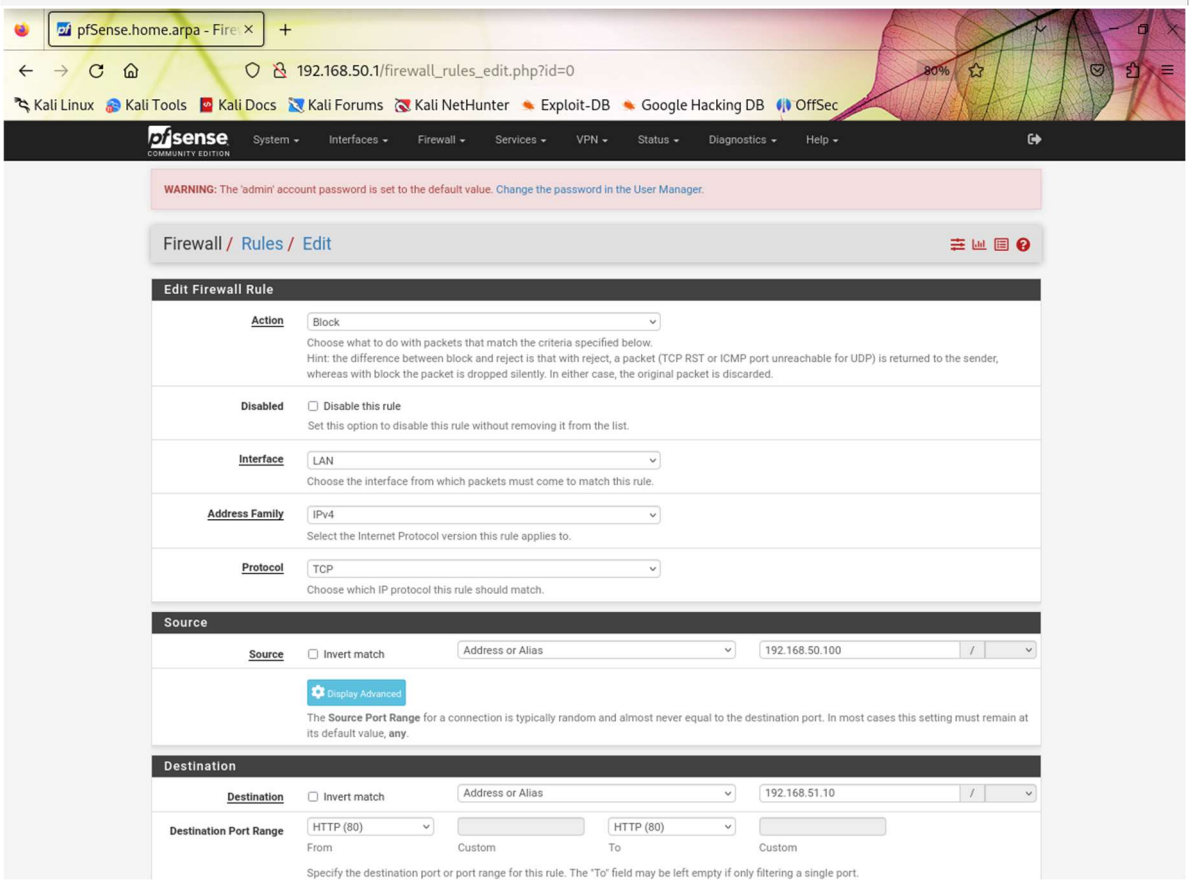


Eseguo una prova di connessione alla pagina Metasploitable.

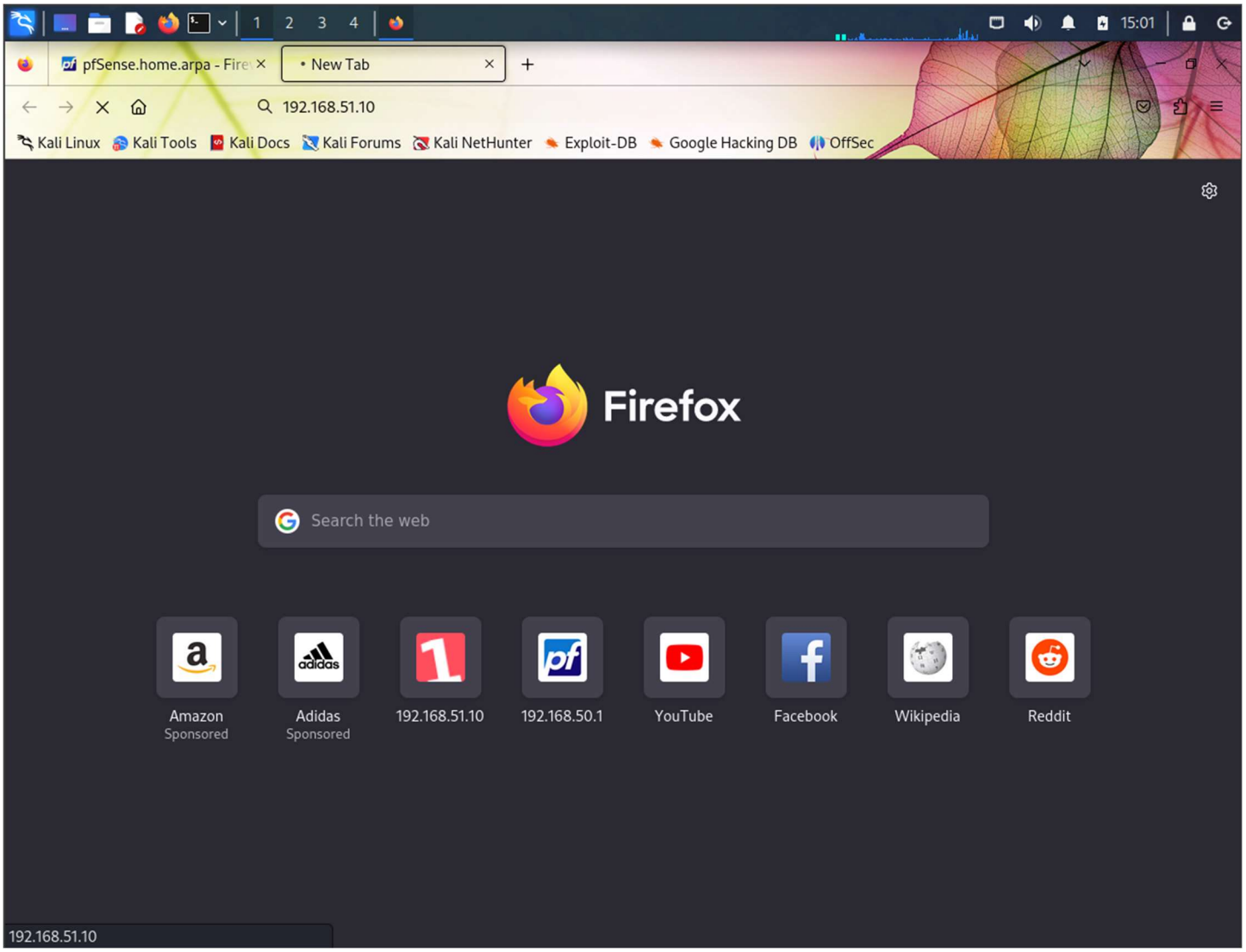


Ora configuro la regola Firewall di PfSense per impedire a Kali di poter accedere alla pagina web di Metasploitable.

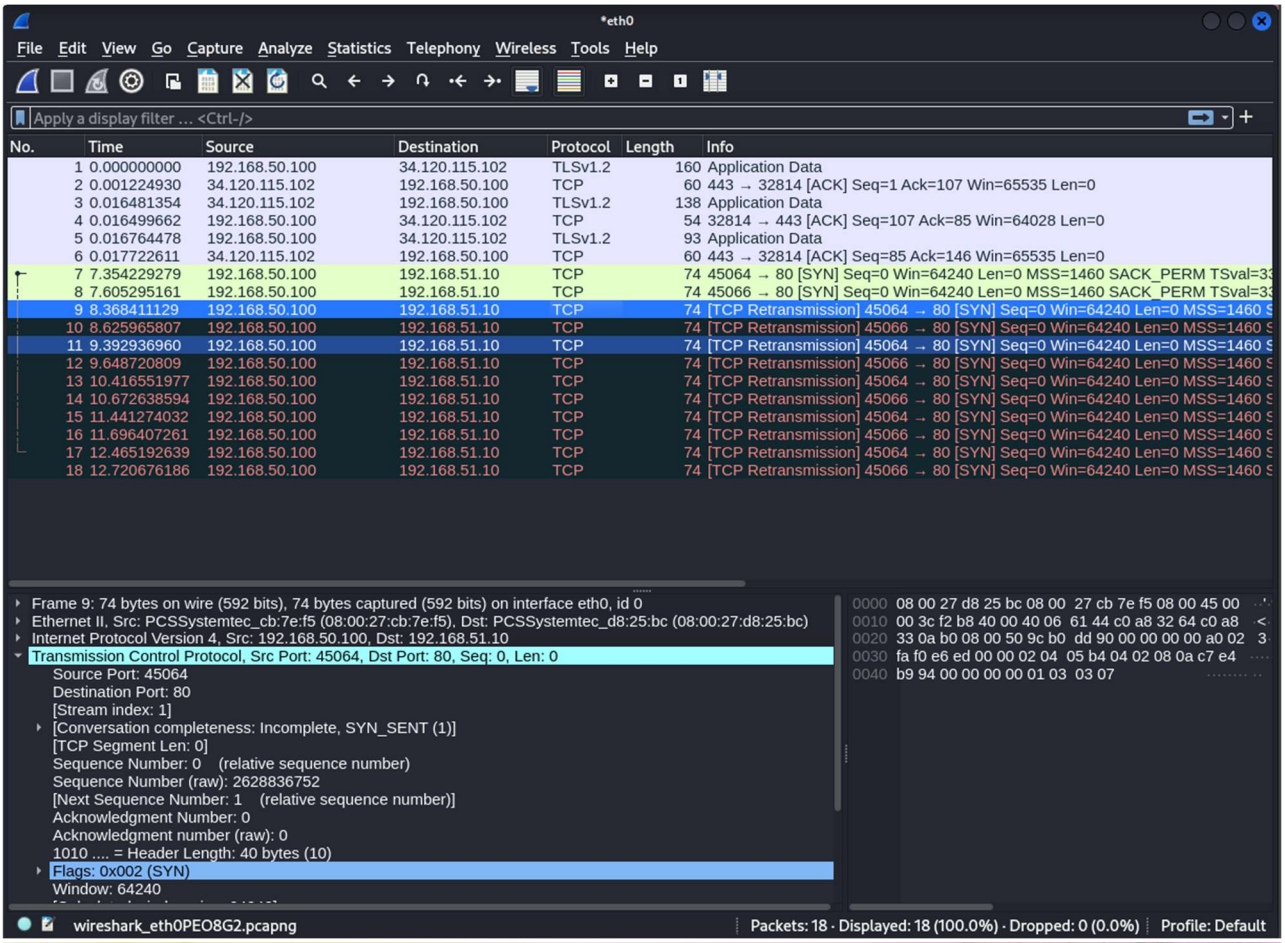

pfSense.home.arpa - Fire
192.168.50.1/firewall_rules.php?if=lan
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Firewall / Rules / LAN
Floating WAN LAN LAN2
Rules (Drag to Change Order)
States Protocol Source Port Destination Port Gateway Queue Schedule Description Actions
0/1.03 MiB * * * LAN Address 80 * * Anti-Lockout Rule
0/0 B IPv4 TCP 192.168.50.100 * 192.168.51.10 80 (HTTP) * none
0/124 KiB IPv4 * LAN subnets * * * * none Default allow LAN to any rule
0/0 B IPv6 * LAN subnets * * * * none Default allow LAN IPv6 to any rule
Add Add Delete Toggle Copy Save Separator

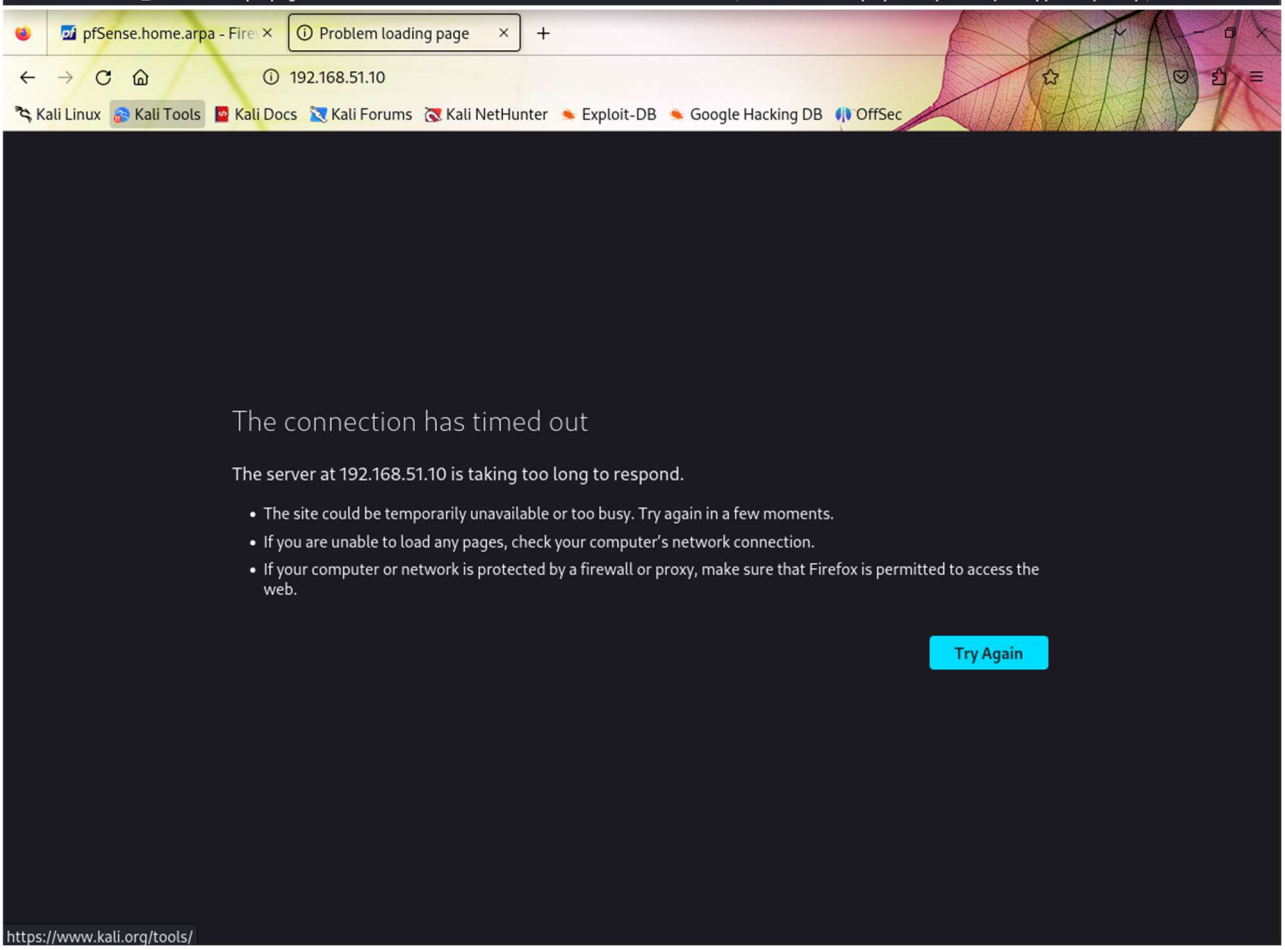

pfSense.home.arpa - Fire
192.168.50.1/firewall_rules_edit.php?id=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Firewall / Rules / 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 192.168.51.10
Destination Port Range HTTP (80) From Custom HTTP (80) 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.

Verifico che venga bloccata la richiesta di apertura della pagina



Come si può vedere da immagini di seguito la richiesta che esegue Kali verso Metasploitable viene bloccata. Di fatto Kali tenta di effettuara la three-way-handshake ma la richiesta rimane bloccata. Quelli a seguire sono le attese di SYN-ACK. Quando passa troppo tempo dalla richiesta, il browser genera errore.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.50.100 34.120.115.102 TLSv1.2 160 Application Data
2 0.001224930 34.120.115.102 192.168.50.100 TCP 60 443 → 32814 [ACK] Seq=1 Ack=107 Win=65535 Len=0
3 0.016481354 34.120.115.102 192.168.50.100 TLSv1.2 138 Application Data
4 0.016499662 192.168.50.100 34.120.115.102 TCP 54 32814 → 443 [ACK] Seq=107 Ack=85 Win=64028 Len=0
5 0.016764478 192.168.50.100 34.120.115.102 TLSv1.2 93 Application Data
6 0.017722611 34.120.115.102 192.168.50.100 TCP 60 443 → 32814 [ACK] Seq=85 Ack=146 Win=65535 Len=0
7 7.354229279 192.168.50.100 192.168.51.10 TCP 74 45064 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=33
8 7.605295161 192.168.50.100 192.168.51.10 TCP 74 45066 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=33
9 8.368411129 192.168.50.100 192.168.51.10 TCP 74 [TCP Retransmission] 45064 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
10 8.625965807 192.168.50.100 192.168.51.10 TCP 74 [TCP Retransmission] 45066 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
11 9.392936960 192.168.50.100 192.168.51.10 TCP 74 [TCP Retransmission] 45064 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
12 9.648720809 192.168.50.100 192.168.51.10 TCP 74 [TCP Retransmission] 45066 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
13 10.416551977 192.168.50.100 192.168.51.10 TCP 74 [TCP Retransmission] 45064 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
14 10.672638594 192.168.50.100 192.168.51.10 TCP 74 [TCP Retransmission] 45066 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
15 11.441274032 192.168.50.100 192.168.51.10 TCP 74 [TCP Retransmission] 45064 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
16 11.696407261 192.168.50.100 192.168.51.10 TCP 74 [TCP Retransmission] 45066 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
17 12.465192639 192.168.50.100 192.168.51.10 TCP 74 [TCP Retransmission] 45064 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
18 12.720676186 192.168.50.100 192.168.51.10 TCP 74 [TCP Retransmission] 45066 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: PCSSystemtec_d8:25:bc (08:00:27:d8:25:bc)
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.51.10
Transmission Control Protocol, Src Port: 45064, Dst Port: 80, Seq: 0, Len: 0
Source Port: 45064
Destination Port: 80
[Stream index: 1]
[Conversation completeness: Incomplete, SYN_SENT (1)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2628836752
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1010 .... = Header Length: 40 bytes (10)
Flags: 0x002 (SYN)
Window: 64240
0000 08 00 27 d8 25 bc 08 00 27 cb 7e f5 08 00 45 00
0010 00 3c f2 b8 40 00 40 06 61 44 c0 a8 32 64 c0 a8
0020 33 0a b0 08 00 50 9c b0 dd 90 00 00 00 00 a0 02
0030 fa f0 e6 ed 00 00 02 04 05 b4 04 02 08 0a c7 e4
0040 b9 94 00 00 00 00 01 03 03 07
wireshark_eth0PEO8G2.pcapng
Packets: 18 · Displayed: 18 (100.0%) · Dropped: 0 (0.0%)
Profile: Default


pfSense.home.arpa - Fire
Problem loading page
192.168.51.10
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
The connection has timed out
The server at 192.168.51.10 is taking too long to respond.
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
https://www.kali.org/tools/

MATTIA SATTIN M3W1D5