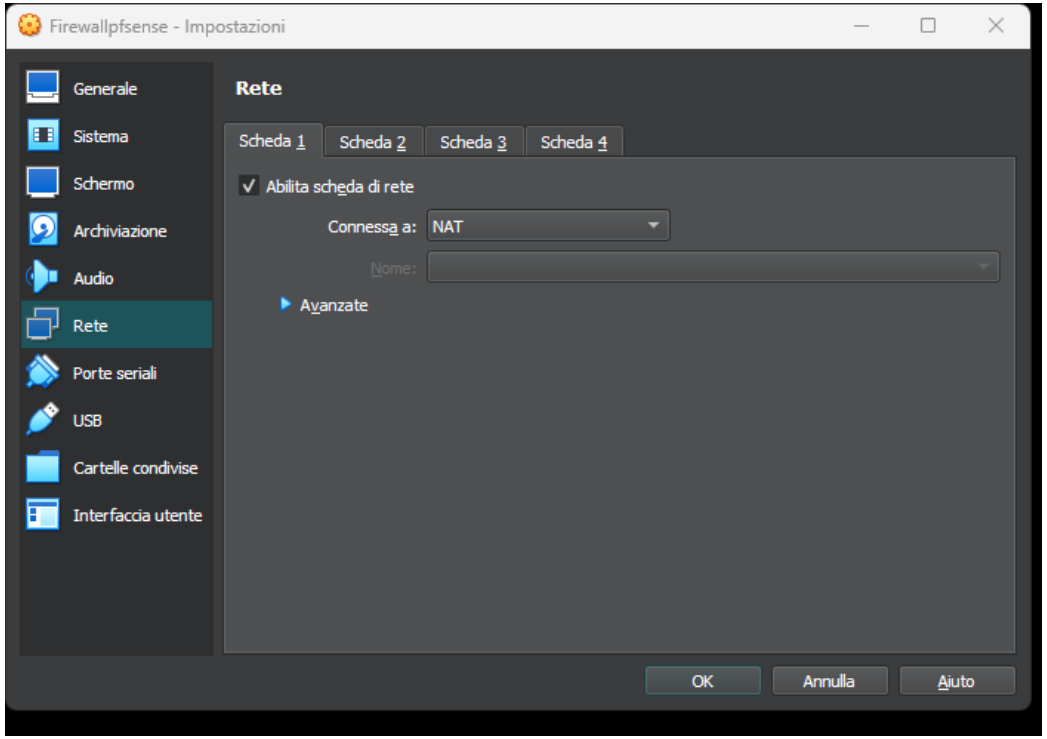
S5 L1

Imposto le 3 schede di rete di pfsense.

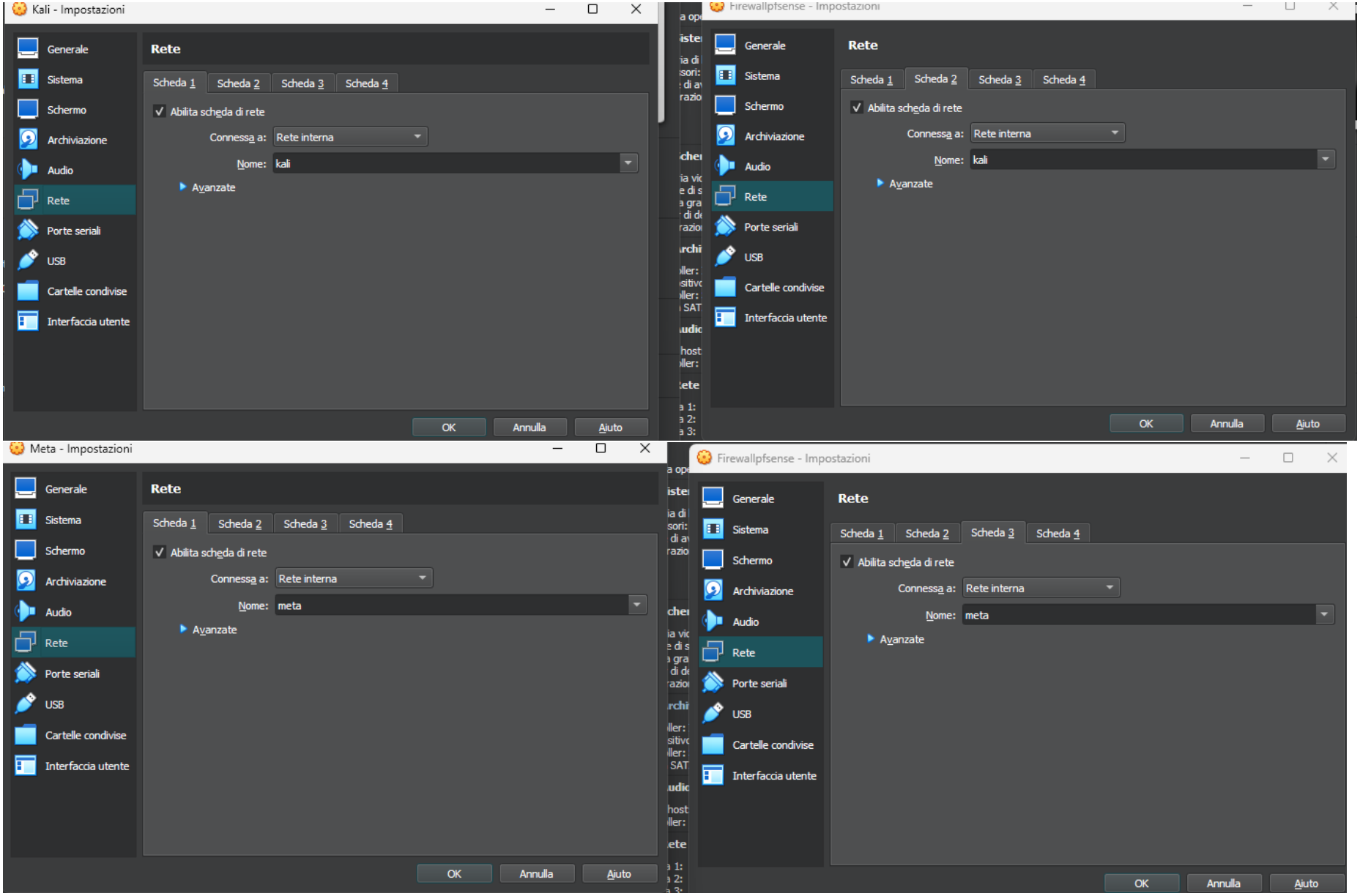
La prima su NAT

La seconda col nome kali, sarà la rete dov'è presente la vm kali

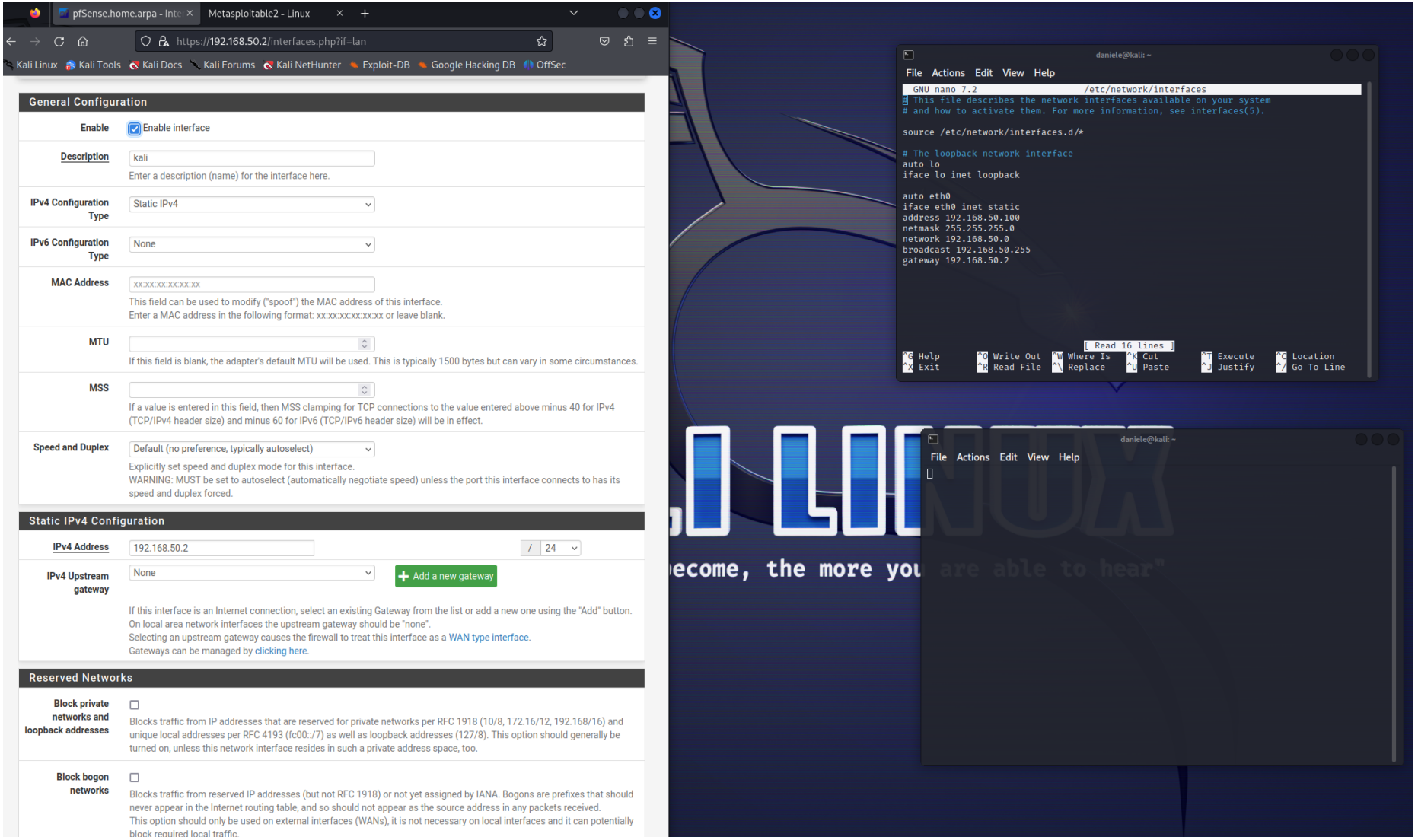
La terza dove sarà presente la vm meta



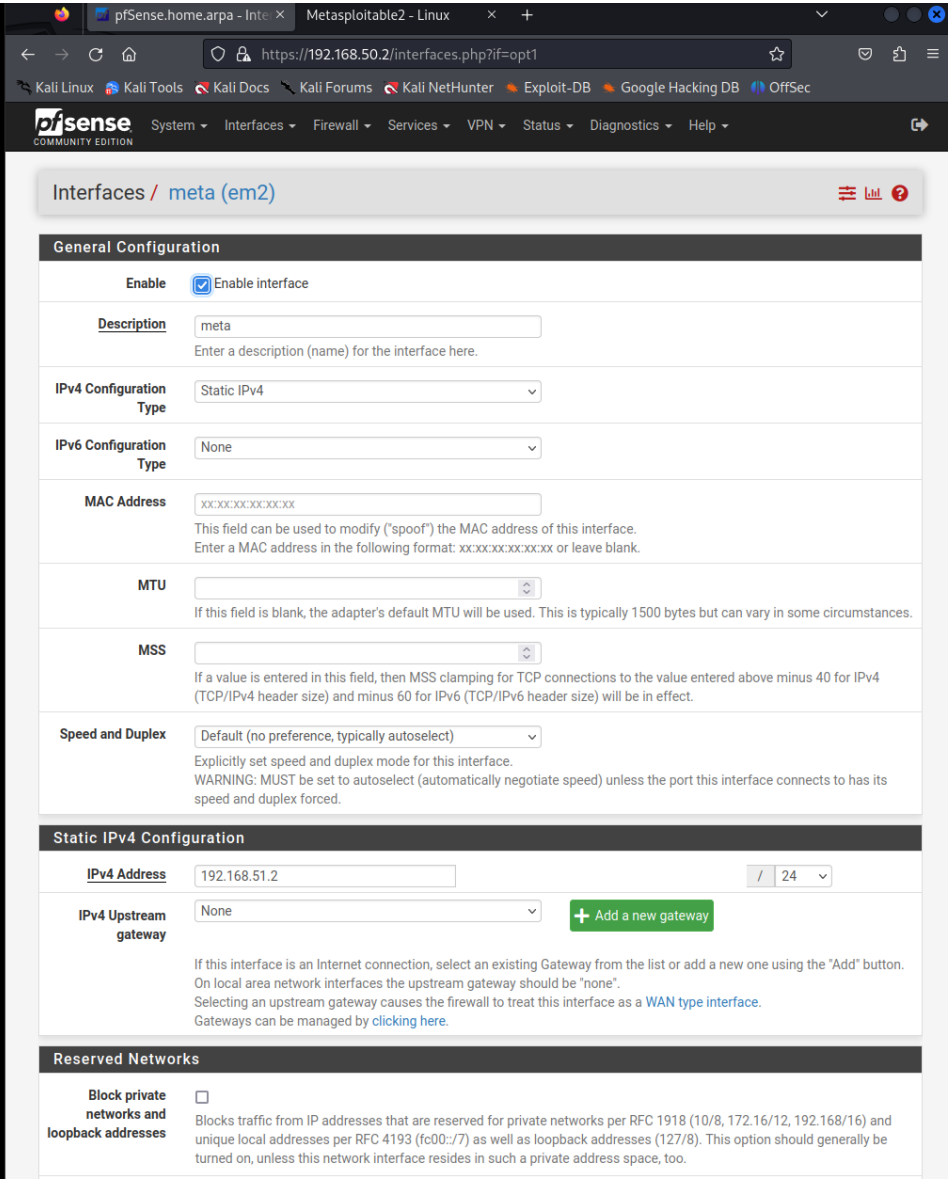
Configuro le macchine, affinchè siano sotto la rete giusta



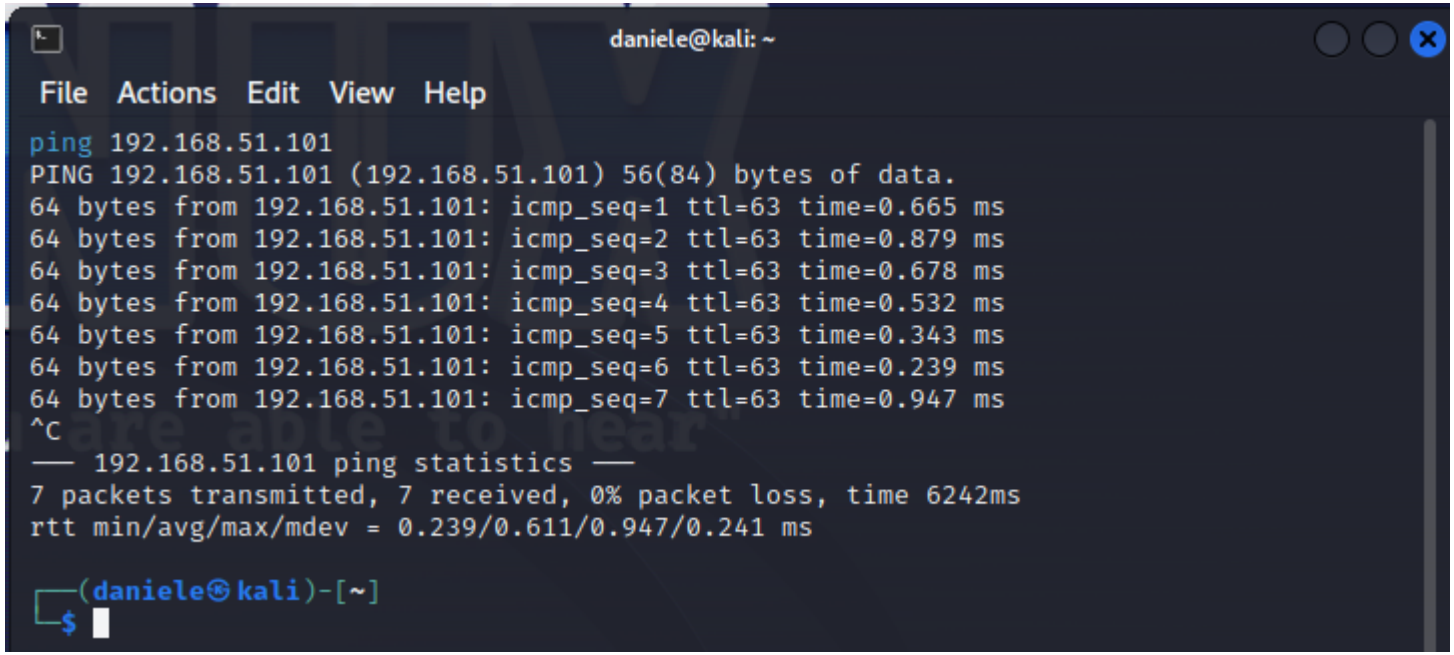
Configuro la macchina kali, dove imposto come default gateway, l'ip di pfsense. E configuro l'interfaccia relativa alla scheda di rete.



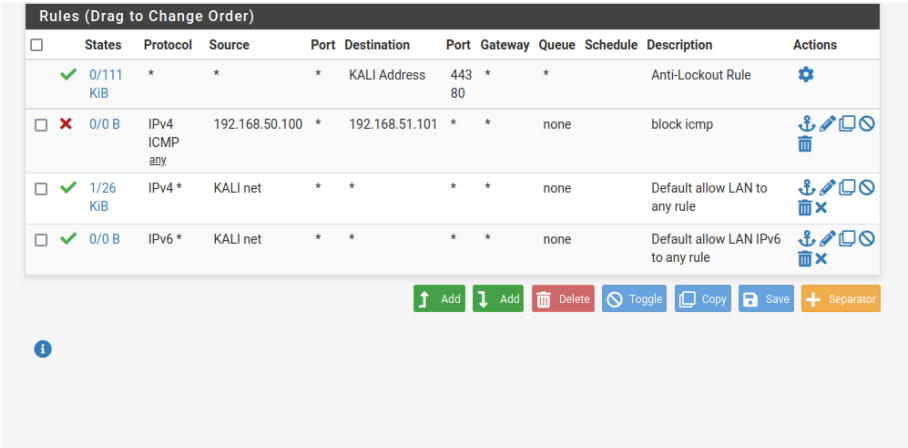
Faccio lo stesso per metasploit e relativa scheda di rete pfsense

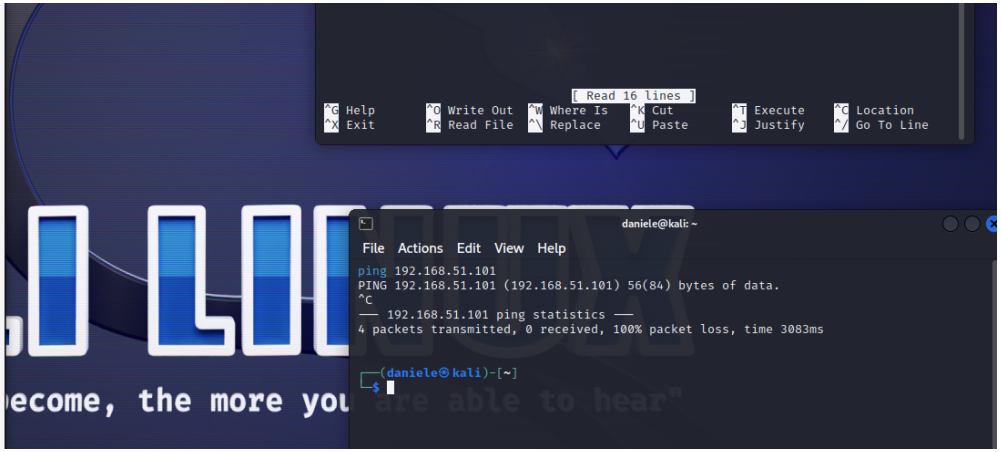


Possiamo notare che da kali avviene il ping verso meta, pur essendo su di una rete diversa.

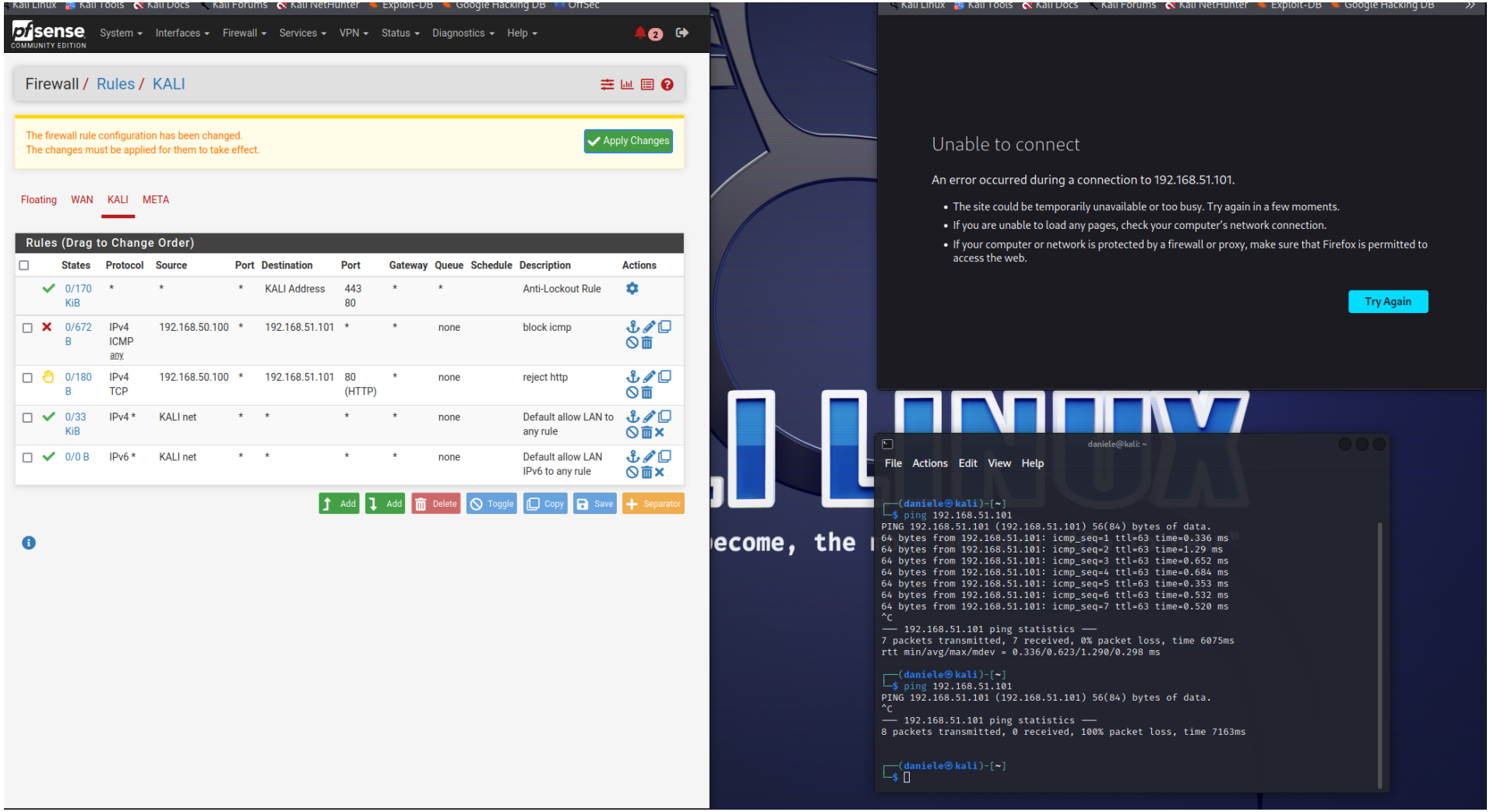


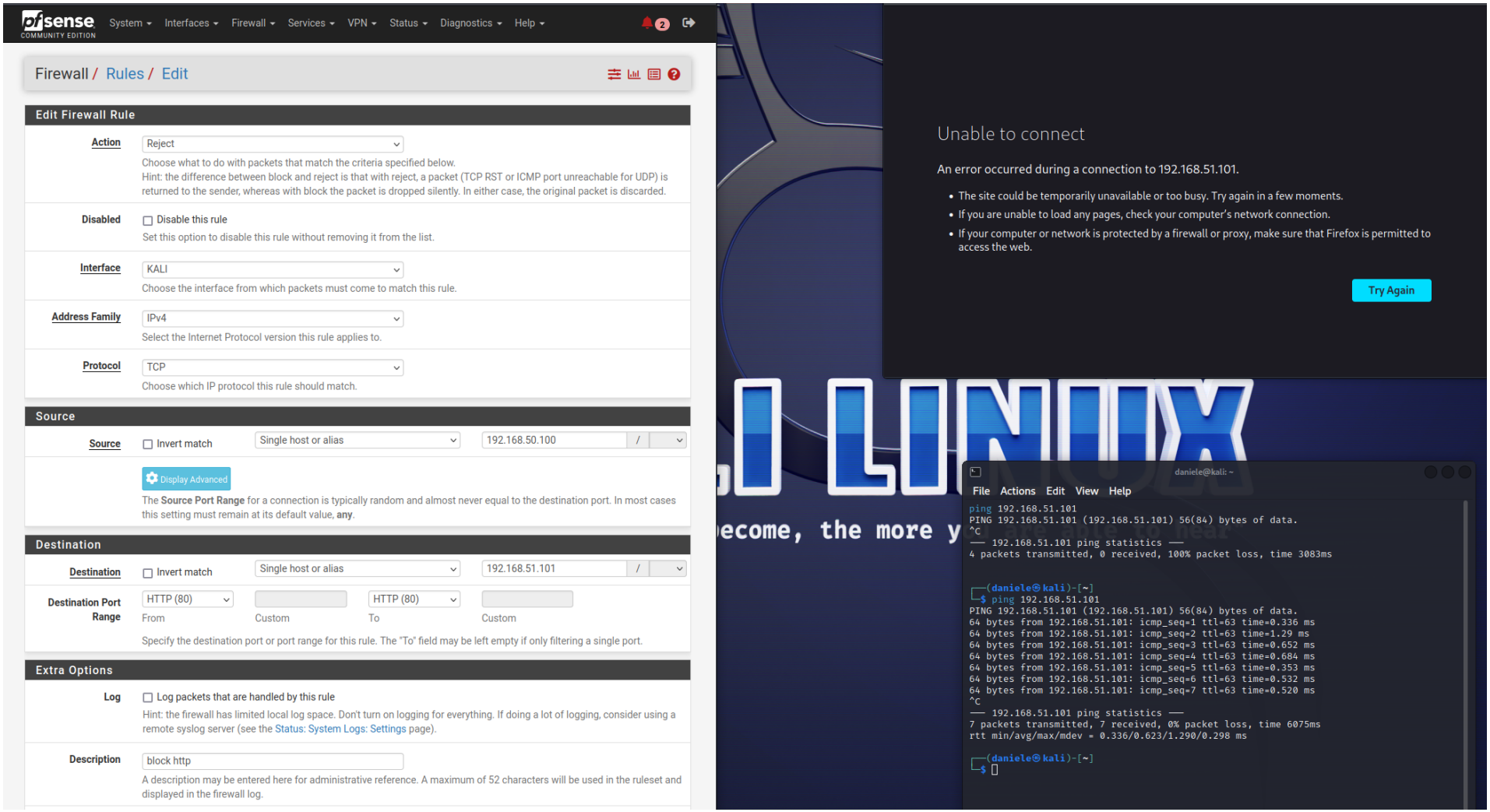
Imposto una regola firewall per blocca pacchetti di tipo icmp da kali verso meta.

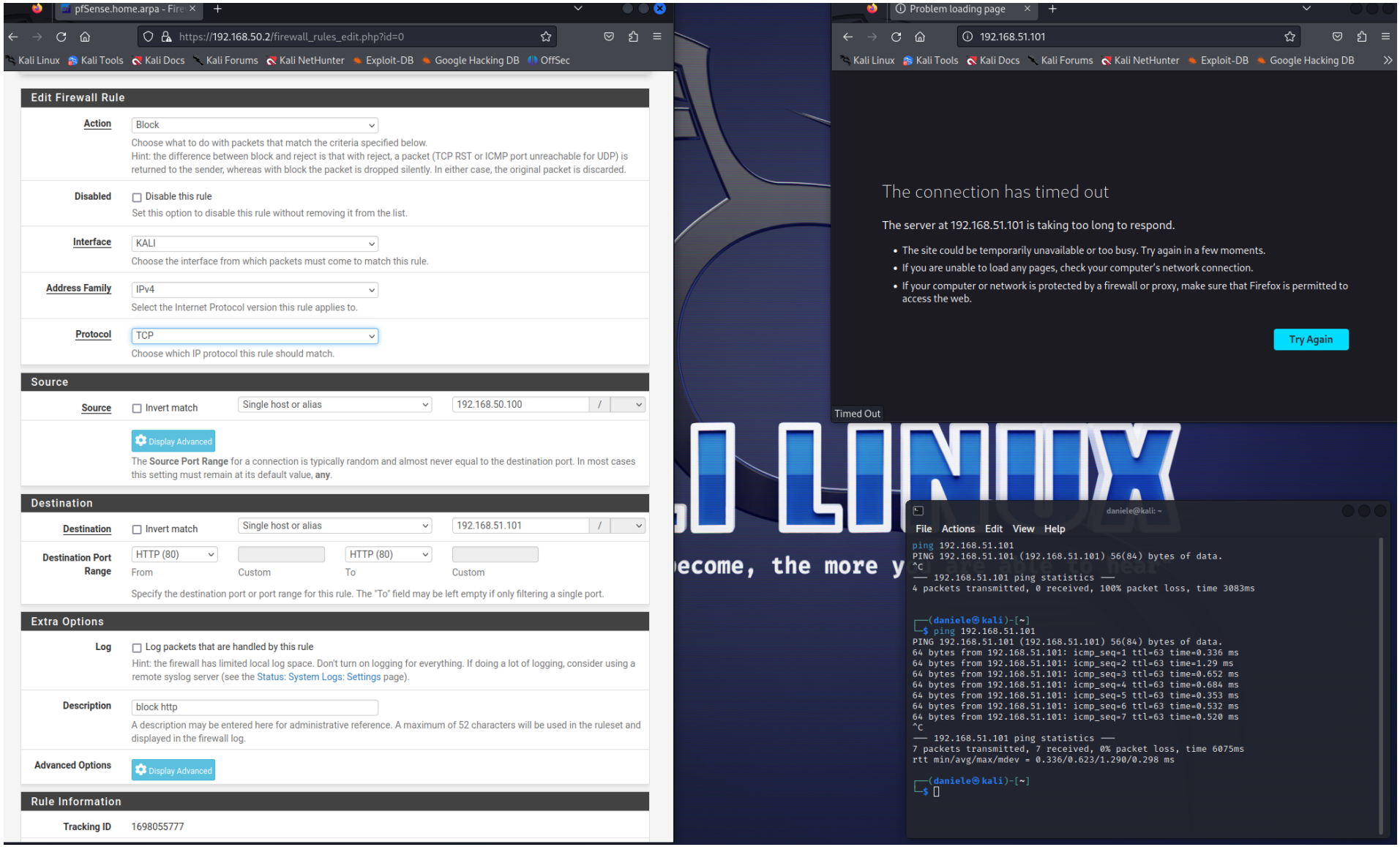




Ho impostato una regola per bloccare le richieste sulla porta 80 da kali verso metasploit. Utilizzando reject, avremo subito risposta dal browser con unable to connect. Con la regola block, invece ci sarà un lungo caricamento della pagina, finchè la connessione non và in timeout.




pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
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.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
KALI
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
Single host 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
Single host or alias
192.168.51.101
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.
Extra Options
Log
Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description
block http
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Unable to connect
An error occurred during a connection to 192.168.51.101.
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
daniele@kali: ~
File Actions Edit View Help
ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
^C
— 192.168.51.101 ping statistics —
4 packets transmitted, 0 received, 100% packet loss, time 3083ms
(daniele㉿kali)-[~]
$ ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=63 time=0.336 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=1.29 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=0.652 ms
64 bytes from 192.168.51.101: icmp_seq=4 ttl=63 time=0.684 ms
64 bytes from 192.168.51.101: icmp_seq=5 ttl=63 time=0.353 ms
64 bytes from 192.168.51.101: icmp_seq=6 ttl=63 time=0.532 ms
64 bytes from 192.168.51.101: icmp_seq=7 ttl=63 time=0.520 ms
^C
— 192.168.51.101 ping statistics —
7 packets transmitted, 7 received, 0% packet loss, time 6075ms
rtt min/avg/max/mdev = 0.336/0.623/1.290/0.298 ms
(daniele㉿kali)-[~]
$


pfSense.home.arpa - Fire
https://192.168.50.2/firewall_rules_edit.php?id=0
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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
KALI
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
Single host 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
Single host or alias
192.168.51.101
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.
Extra Options
Log
Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description
block http
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options
Display Advanced
Rule Information
Tracking ID
1698055777
Problem loading page
192.168.51.101
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
The connection has timed out
The server at 192.168.51.101 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
Timed Out
LINUX
ecome, the more y
daniele@kali: ~
File Actions Edit View Help
ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
^C
— 192.168.51.101 ping statistics —
4 packets transmitted, 0 received, 100% packet loss, time 3083ms
(daniele㉿kali)-[~]
$ ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=63 time=0.336 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=1.29 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=0.652 ms
64 bytes from 192.168.51.101: icmp_seq=4 ttl=63 time=0.684 ms
64 bytes from 192.168.51.101: icmp_seq=5 ttl=63 time=0.353 ms
64 bytes from 192.168.51.101: icmp_seq=6 ttl=63 time=0.532 ms
64 bytes from 192.168.51.101: icmp_seq=7 ttl=63 time=0.520 ms
^C
— 192.168.51.101 ping statistics —
7 packets transmitted, 7 received, 0% packet loss, time 6075ms
rtt min/avg/max/mdev = 0.336/0.623/1.290/0.298 ms
(daniele㉿kali)-[~]
$