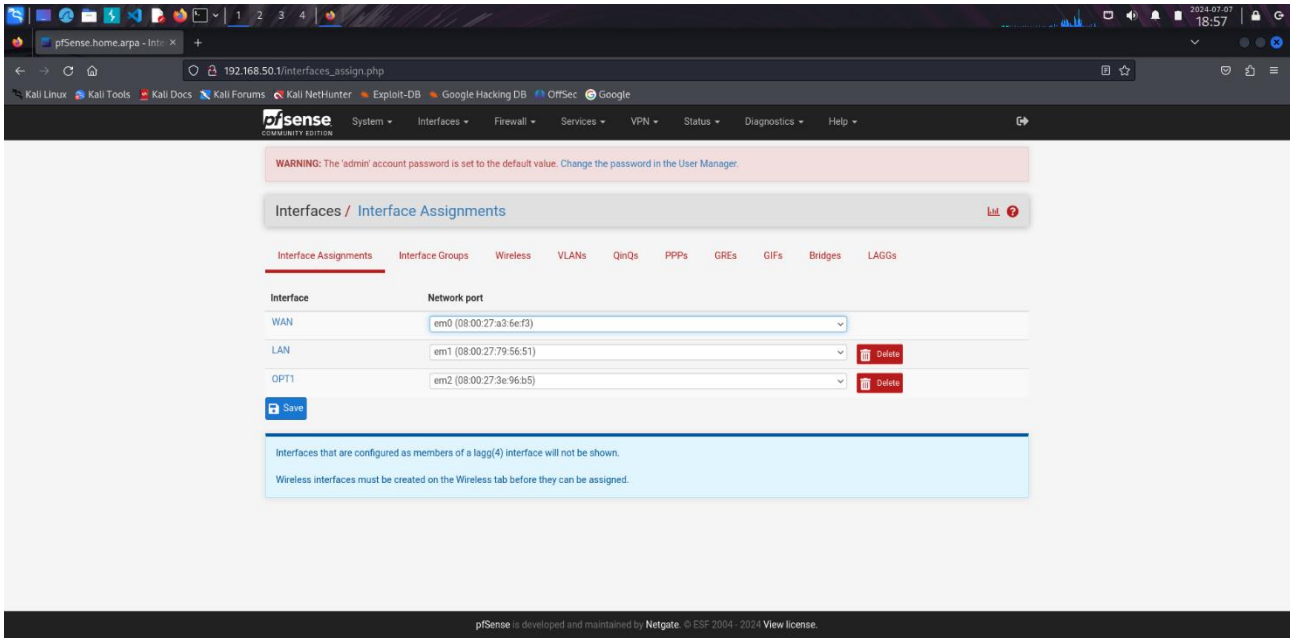
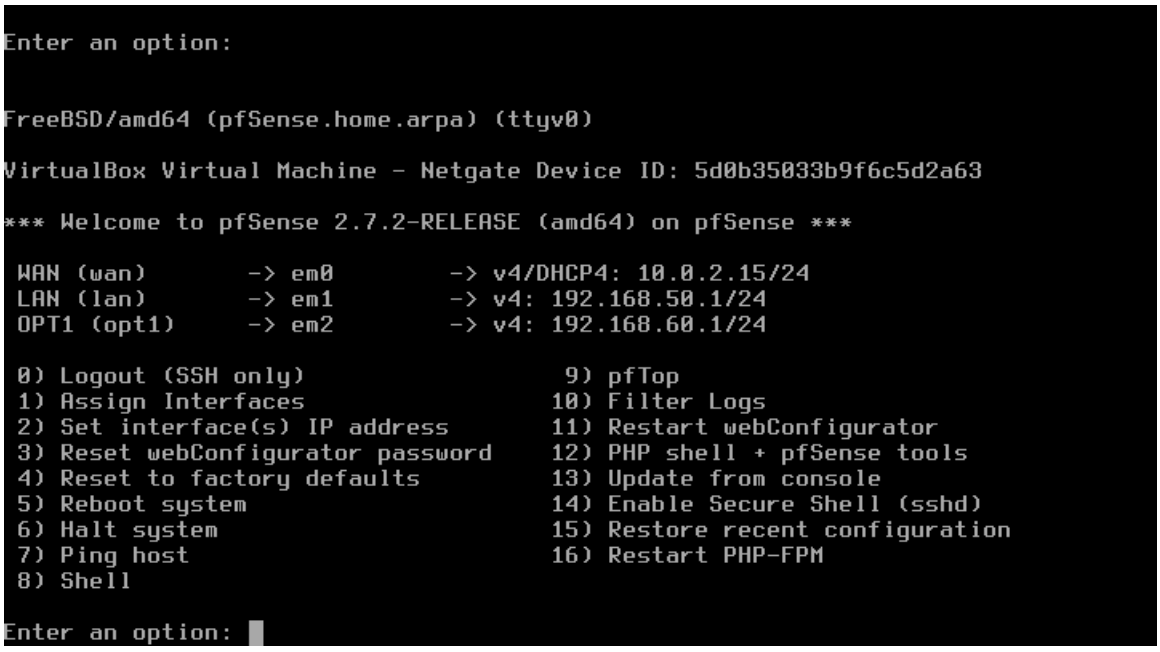
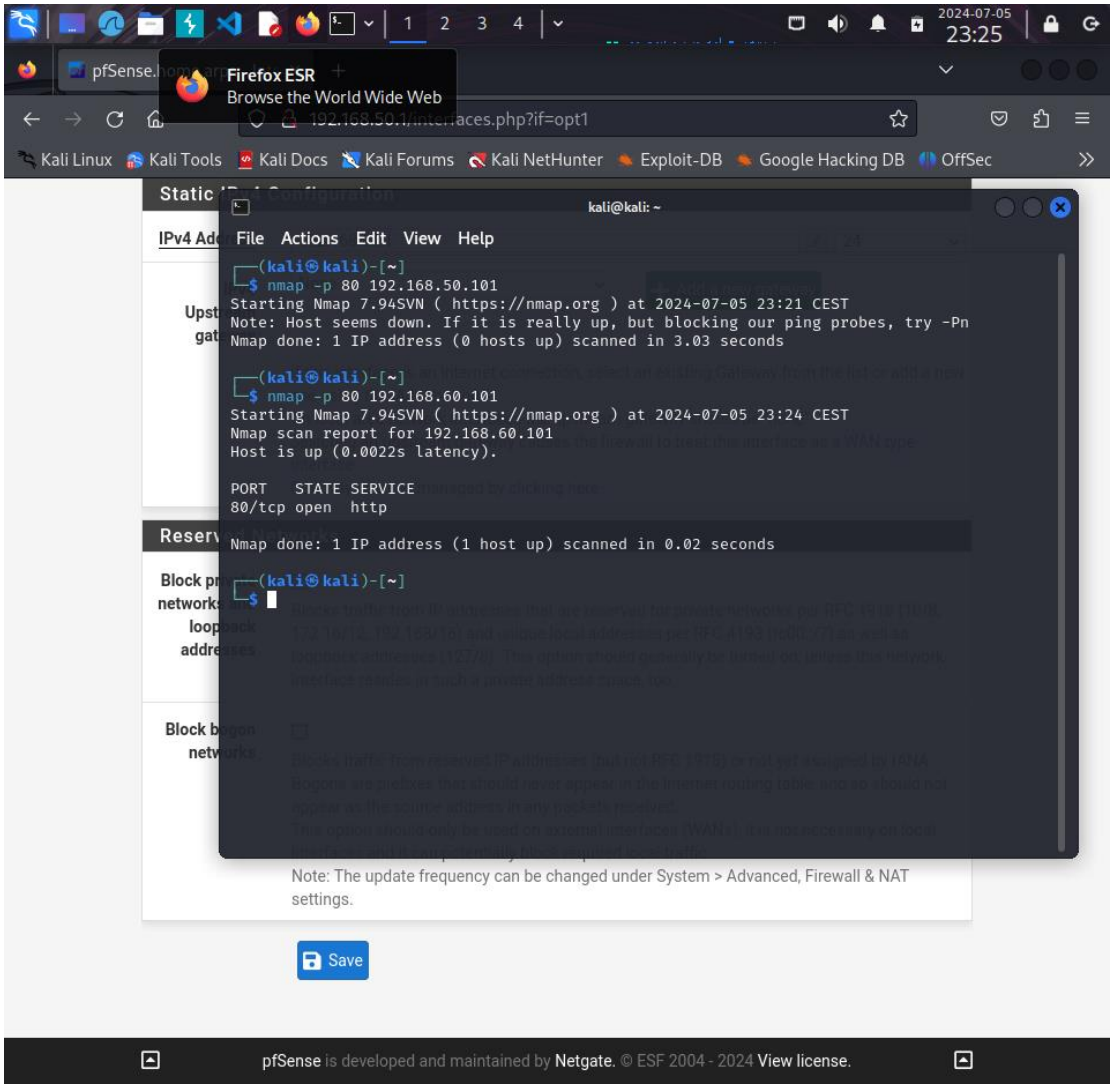
Aggiungo l’interfaccia OPT1, che appartiene alla macchina Metasploitable



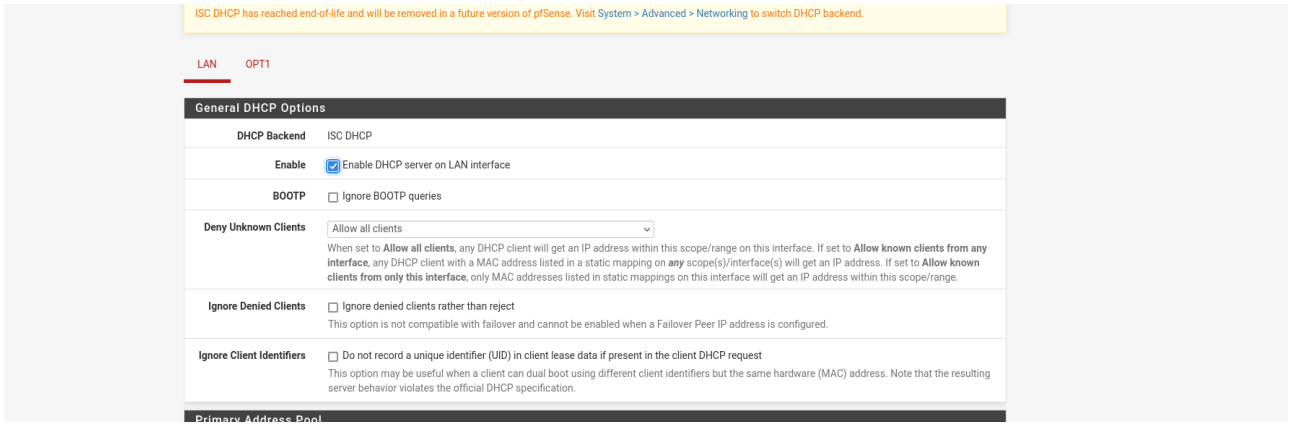
La nuova interfaccia compare anche su pfsense mv, che appartiere alla sottorete che abbiamo creato

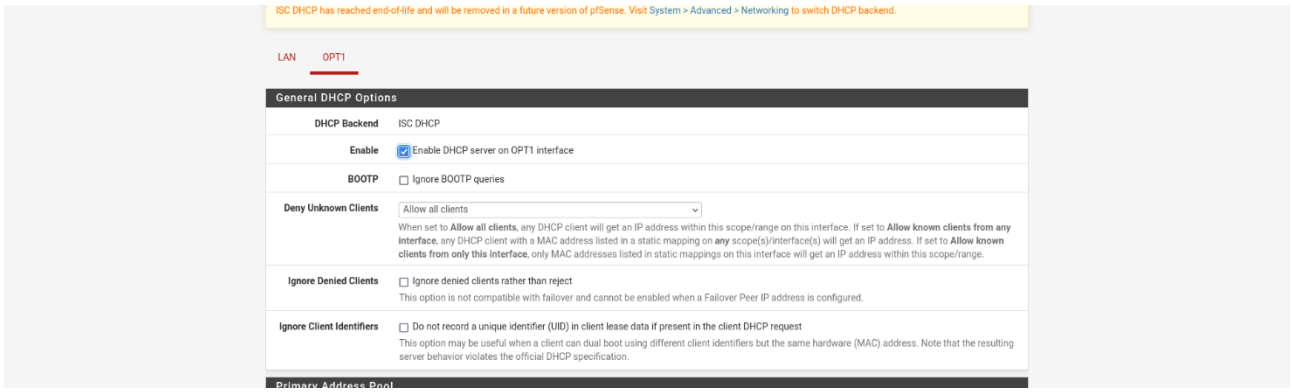


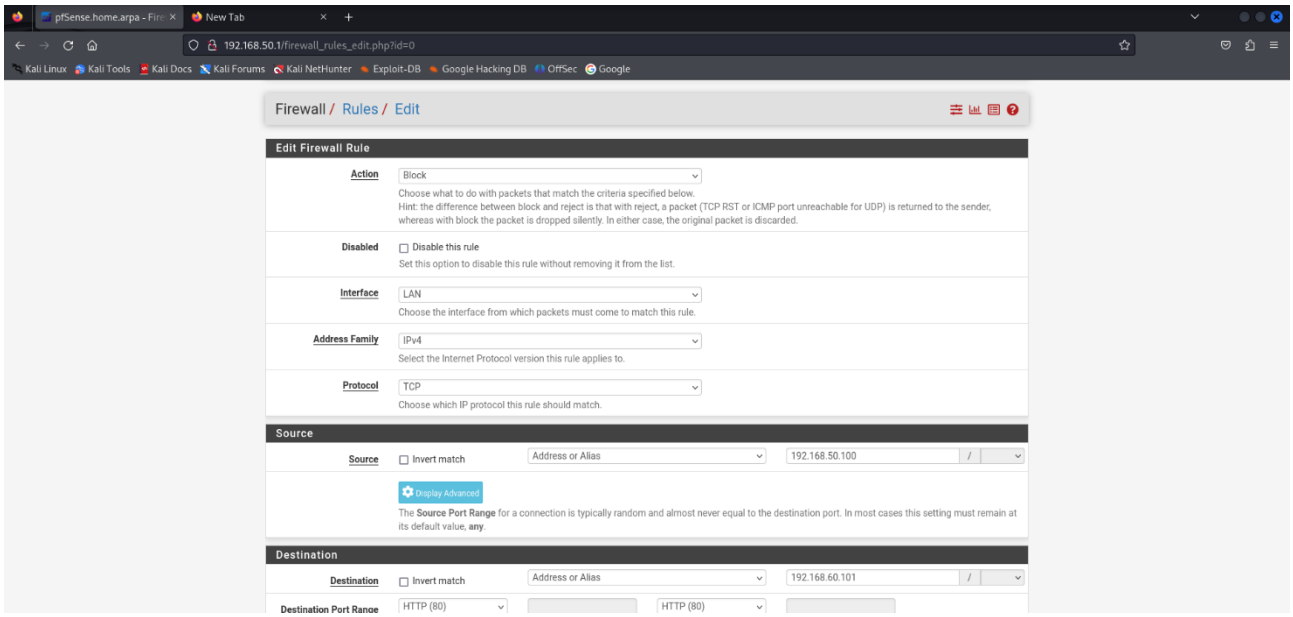
Faccio nmap sull’indirizzo della Meta prima di applicare la regola, la porta 80 risulta aperta

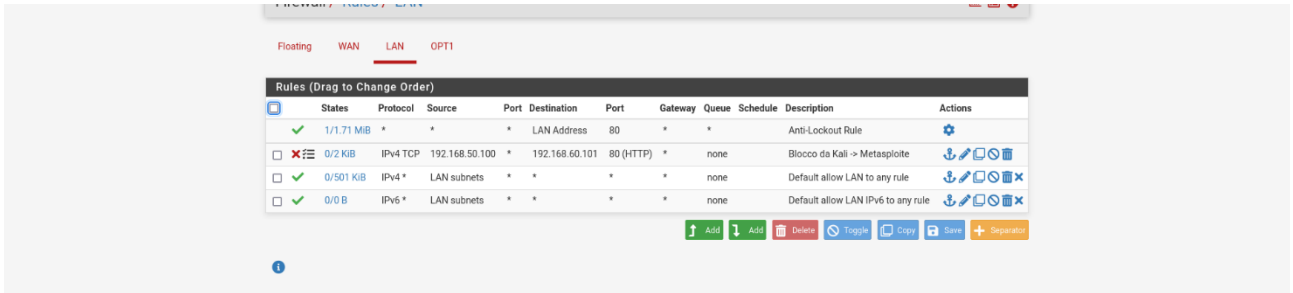


Abilito il DHCP server sia sull’interfaccia LAN che su OPT1 e creo la regola sull’interfaccia LAN

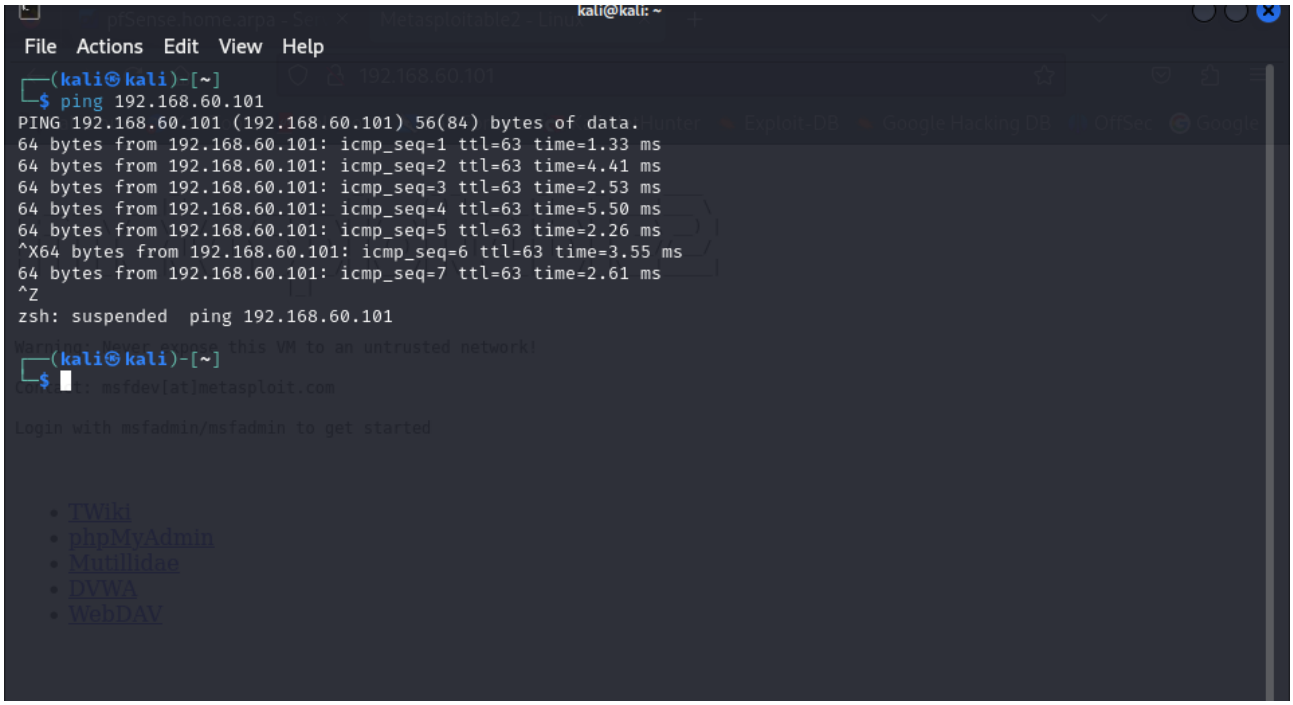


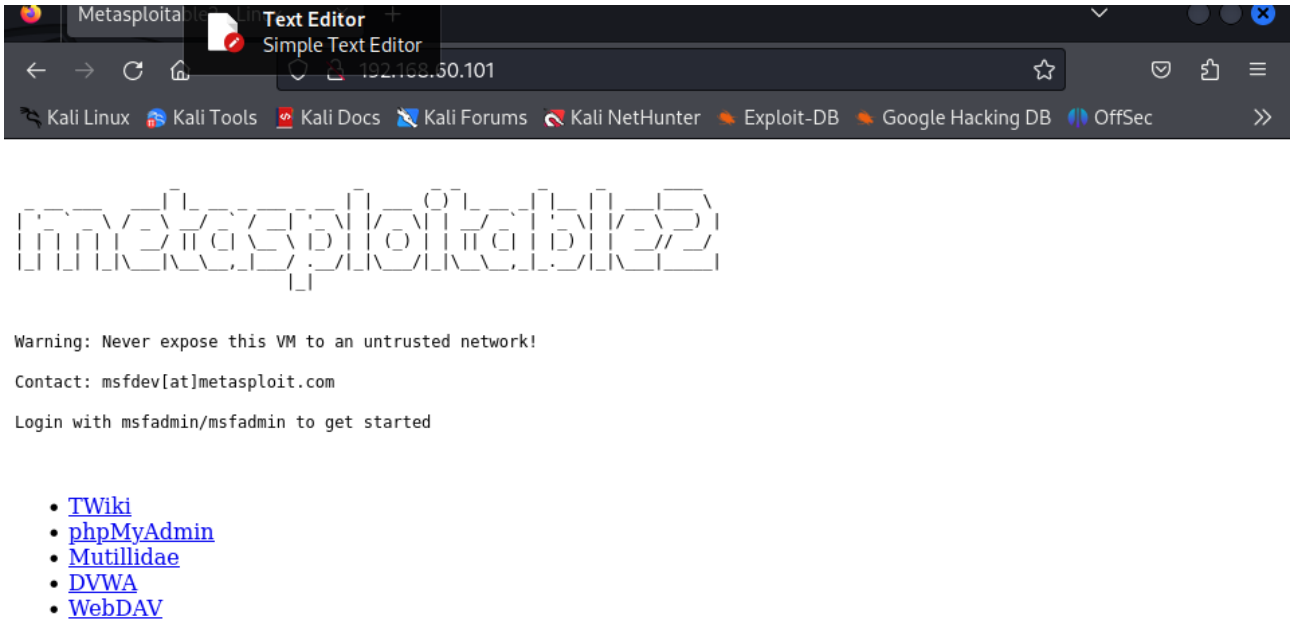

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.
LAN
OPT1
General DHCP Options
DHCP Backend
ISC DHCP
Enable
Enable DHCP server on OPT1 interface
BOOTP
Ignore BOOTP queries
Deny Unknown Clients
Allow all clients
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


pfSense.home.arpa - Fire
New Tab
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
Google
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
192.168.60.101
Destination Port Range
HTTP (80)
HTTP (80)

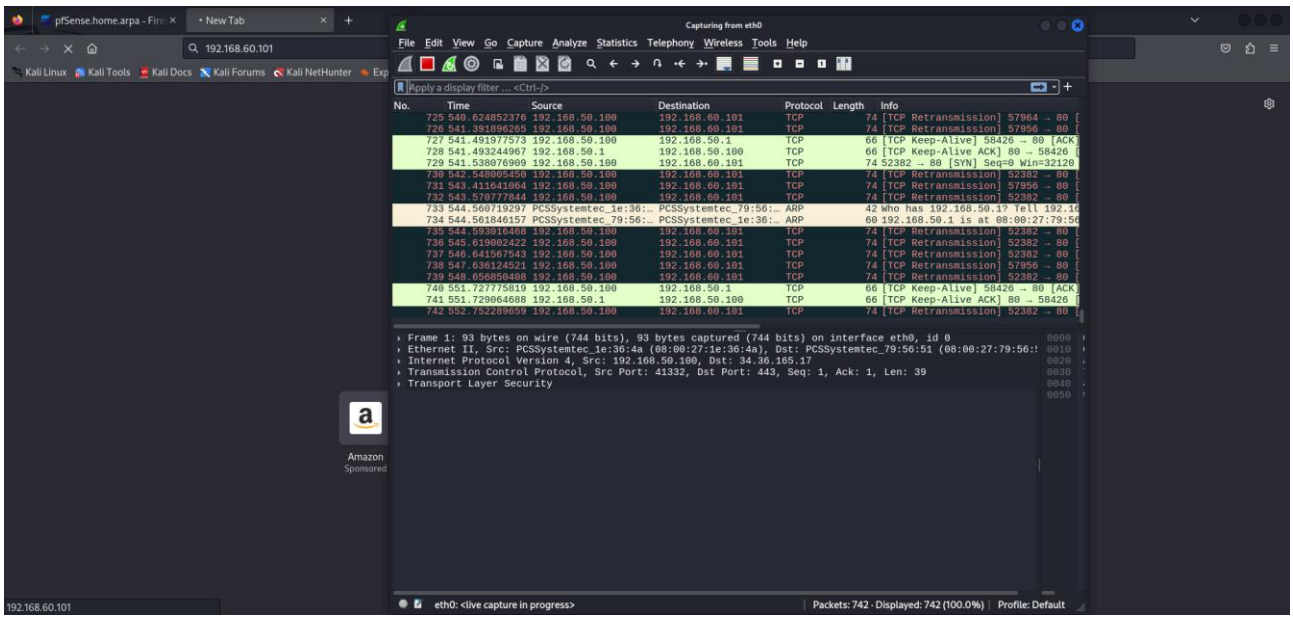

Floating
WAN
LAN
OPT1
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
1/1.71 MiB * * * LAN Address 80 * * Anti-Lockout Rule
0/2 KiB IPv4 TCP 192.168.50.100 * 192.168.60.101 80 (HTTP) * none Blocco da Kali -> Metasploite
0/501 KiB IPv4 * 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

Prima di abilitare la regola controllo da Kali che la Metasploitable sia raggiungibile

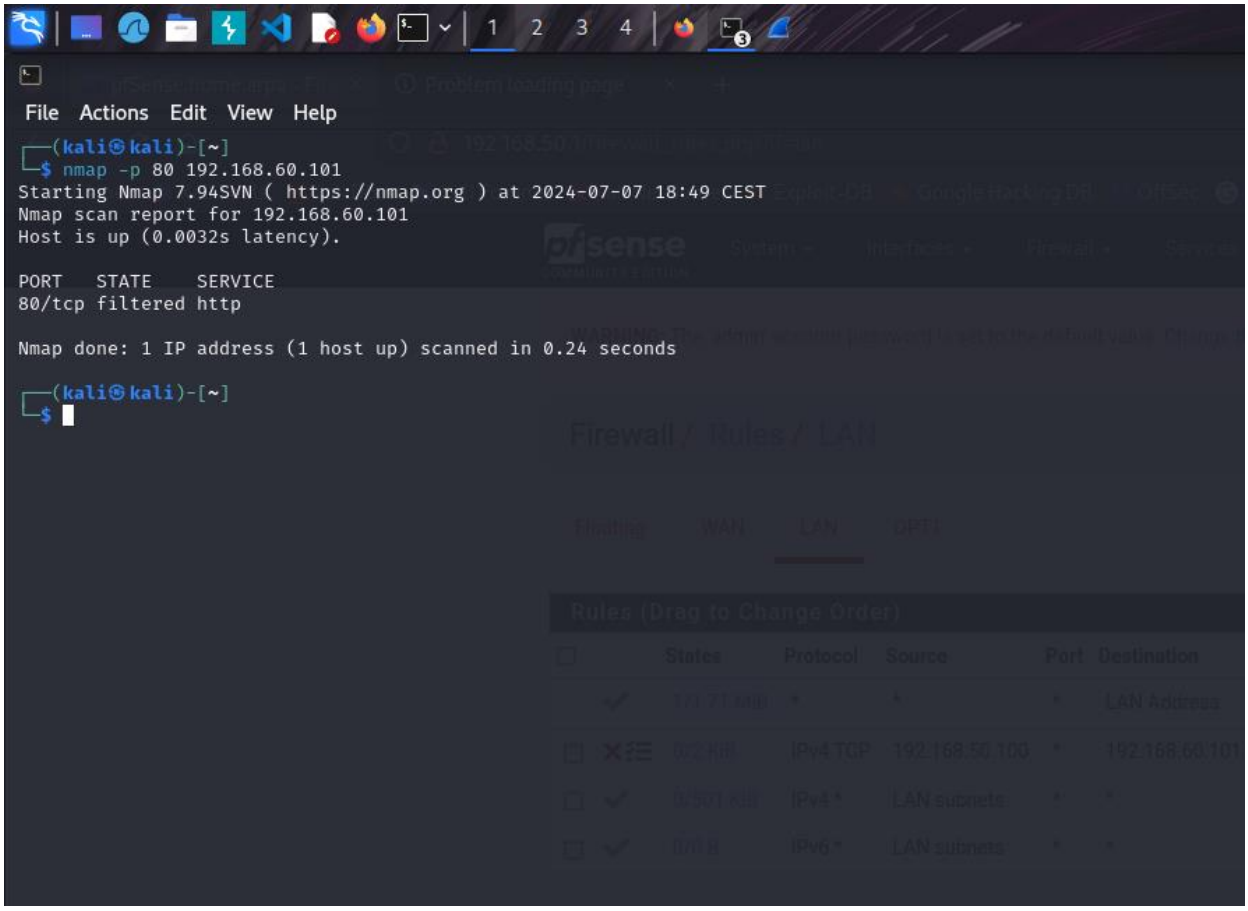




Adesso abilito la regola e provo a ricollegarmi sulla DVWA di Metasploitable ma non si collegherà e possiamo vedere, grazie a wireshark, che la connessione con TCP non va a buon fine.



Riprovo nmap e vedo che lo stato della porta 80 risulterà ‘filtred’ e non più open



Ispezione dei log del Firewall