

W9D4



Interfaces / OPT1 (em2)

General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumsta

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

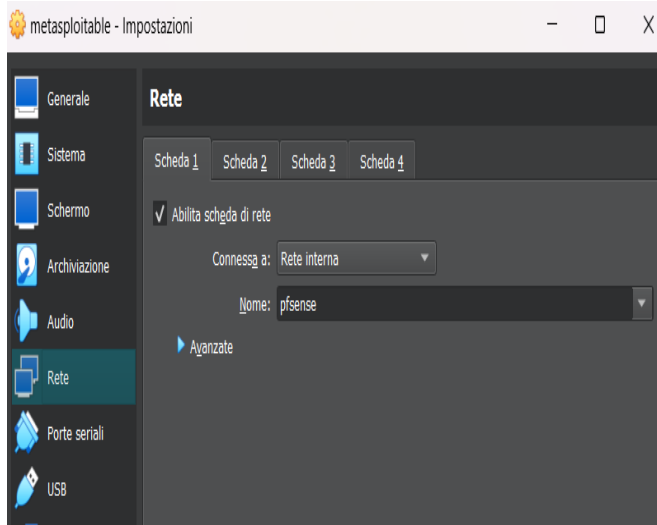
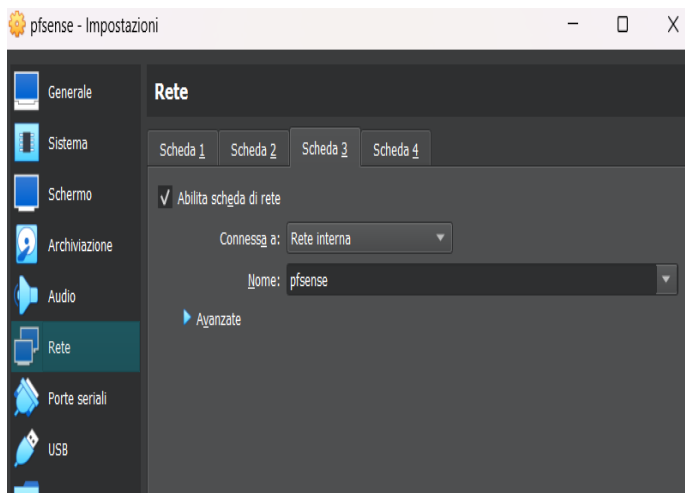
Speed and Duplex
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has it

Static IPv4 Configuration

IPv4 Address

IPv4 Upstream gateway [+ Add a new gateway](#)

Aggiunto e configurato una nuova interfaccia su pfSense.



Modifiche sulle impostazioni delle interfacce di metasploitable e pfsense per averle sulla stessa sotto rete.

Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on OPT1 interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Allowed Clients	<div>Allow all clients</div> <p>When set to Allow all clients, any DHCP client will get an IP address with interface, any DHCP client with a MAC address listed in a static mapping clients from only this interface, only MAC addresses listed in static mapping</p>
Deny Clients	<input type="checkbox"/> Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when
Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in This option may be useful when a client can dual boot using different client identifiers. server behavior violates the official DHCP specification.
Address Pool	
Subnet	192.168.50.0/24
IP Address Range	192.168.50.1 - 192.168.50.254
Excluded IP Address Range	<div>192.168.50.100</div> <p>From</p> <p>The specified range for this pool must not be within the range configured for the subnet.</p>
Additional Pools	<div>+ Add Address Pool</div> <p>If additional pools of addresses are needed inside of this subnet outside of the</p>

Abilitazione del servizio DHCP sull'interfaccia appena creata.

```

GNU nano 2.9.7 File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

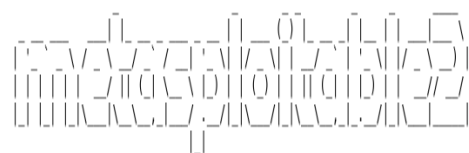
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp

#iface eth0 inet static
#address 192.168.50.101
# network 192.168.50.0
#netmask 255.255.255.0
# broadcast 192.168.50.255
#gateway 192.168.50.1

```

Modifica delle impostazioni di rete di metasploitable da static in dhcp.



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

```

(kali@kali)-[~]
$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data:
64 bytes from 192.168.50.100: icmp_seq=1 ttl=63 time=4.24 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=4.82 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=6.36 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=63 time=3.08 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=63 time=4.38 ms
64 bytes from 192.168.50.100: icmp_seq=6 ttl=63 time=3.23 ms
^C
— 192.168.50.100 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5015ms
rtt min/avg/max/mdev = 3.076/4.353/6.361/1.091 ms

(kali@kali)-[~]
$

```

Verifica della connettività tra kali e metasploitable anche verso DVWA.

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 192.168.1.100 /

[Display Advanced](#)

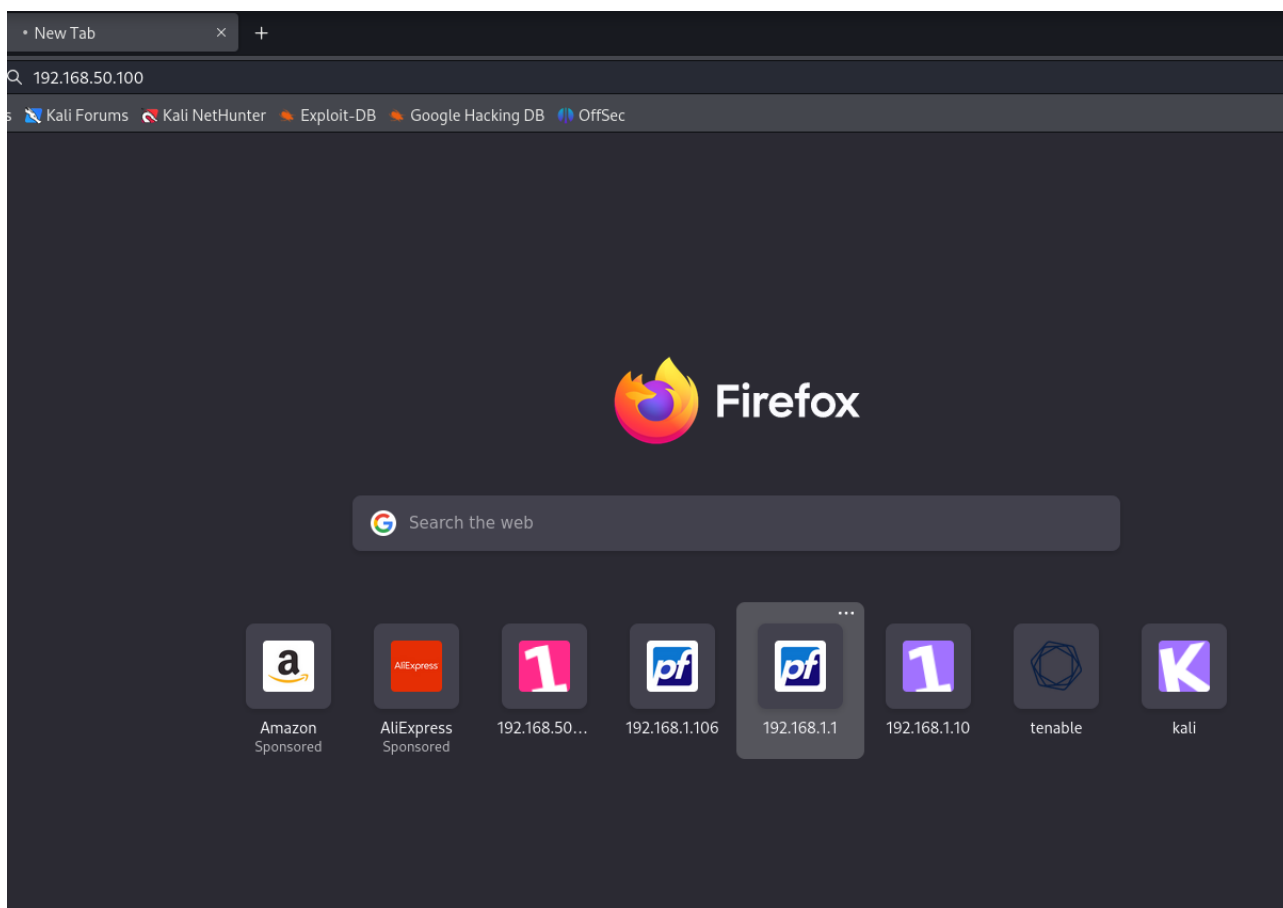
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

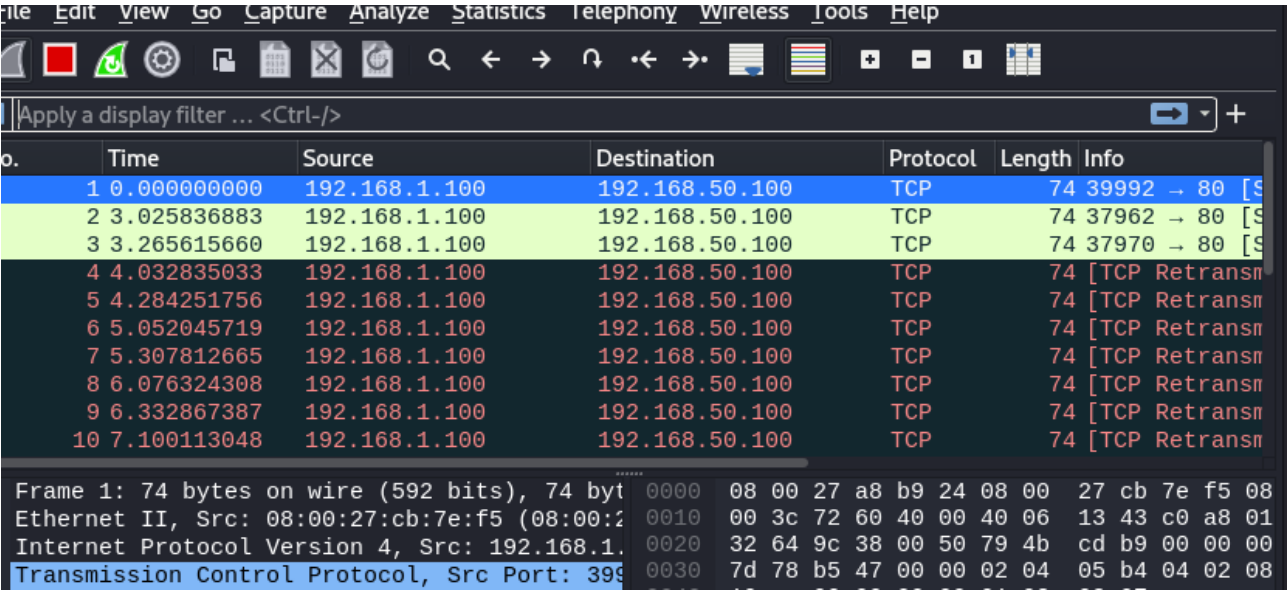
Destination ☐ Invert match Address or Alias 192.168.50.100 /

Destination Port Range HTTP (80) HTTP (80)

Creazione della regola per bloccare il traffico sulla porta 80 da kali a metasploitable. Sto di fatto rendendo la DVWA non accessibile da Kali. Abilitando il log così posso vedere il traffico che viene gestito dalla regola.



In questo screen sto provando a raggiungere nuovamente la DVWA. Ho effettuato correttamente le configurazioni, infatti, non riesco più più raggiungere la DVWA.

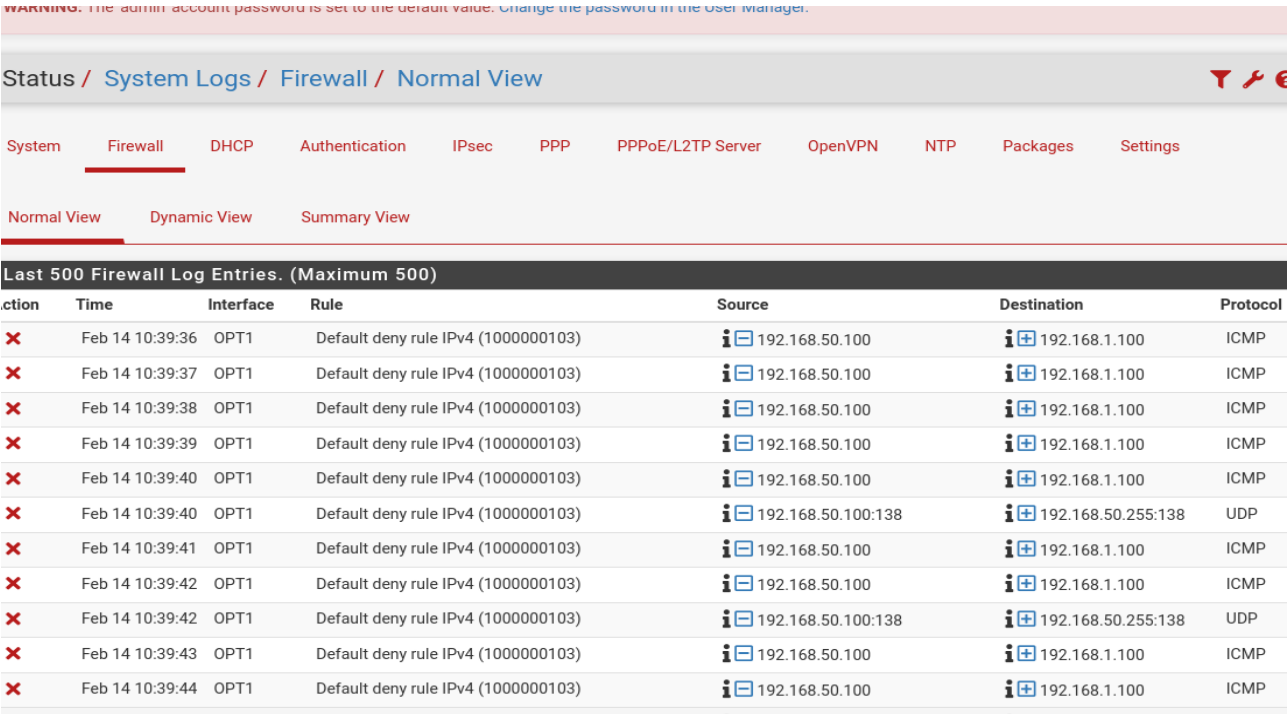


The screenshot shows a Wireshark packet capture with a display filter of 'Apply a display filter ... <Ctrl-/>'. The packet list shows 10 packets, all of which are TCP retransmissions from source 192.168.1.100 to destination 192.168.50.100 on port 80. The packet details pane shows the first packet (Frame 1) with a length of 74 bytes on wire (592 bits). The protocol stack is Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol, Src Port: 39992.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.100	192.168.50.100	TCP	74	39992 → 80 [S
2	3.025836883	192.168.1.100	192.168.50.100	TCP	74	37962 → 80 [S
3	3.265615660	192.168.1.100	192.168.50.100	TCP	74	37970 → 80 [S
4	4.032835033	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransm
5	4.284251756	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransm
6	5.052045719	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransm
7	5.307812665	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransm
8	6.076324308	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransm
9	6.332867387	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransm
10	7.100113048	192.168.1.100	192.168.50.100	TCP	74	[TCP Retransm

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0, 0 packets captured, 0 packets dropped on interface 0
Ethernet II, Src: 08:00:27:cb:7e:f5 (08:00:27:cb:7e:f5), Dst: 08:00:27:cb:7e:f5 (08:00:27:cb:7e:f5), Protocol: Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.50.100
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.50.100
Transmission Control Protocol, Src Port: 39992, Dst Port: 80, Seq: 37962, Len: 0

Da Wireshark ho la prova che la destinazione non ci sta rispondendo, ed il browser continua ad effettuare tentativi di connessione, senza ricevere alcuna risposta.



The screenshot shows the Firewall log in the 'Normal View' tab. The log displays the last 500 Firewall Log Entries, showing multiple denied connections from source 192.168.50.100 to destination 192.168.1.100. The log entries are filtered by the rule 'Default deny rule IPv4 (1000000103)'.

Action	Time	Interface	Rule	Source	Destination	Protocol
Deny	Feb 14 10:39:36	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100	192.168.1.100	ICMP
Deny	Feb 14 10:39:37	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100	192.168.1.100	ICMP
Deny	Feb 14 10:39:38	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100	192.168.1.100	ICMP
Deny	Feb 14 10:39:39	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100	192.168.1.100	ICMP
Deny	Feb 14 10:39:40	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100	192.168.1.100	ICMP
Deny	Feb 14 10:39:40	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100:138	192.168.50.255:138	UDP
Deny	Feb 14 10:39:41	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100	192.168.1.100	ICMP
Deny	Feb 14 10:39:42	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100	192.168.1.100	ICMP
Deny	Feb 14 10:39:42	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100:138	192.168.50.255:138	UDP
Deny	Feb 14 10:39:43	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100	192.168.1.100	ICMP
Deny	Feb 14 10:39:44	OPT1	Default deny rule IPv4 (1000000103)	192.168.50.100	192.168.1.100	ICMP

Infine, dai log del Firewall ho la conferma che la mia regola, DVWA from Kali, sta effettivamente bloccando il traffico da Kali verso la DVWA.