

# Esercitazione W9D4

## PfSense

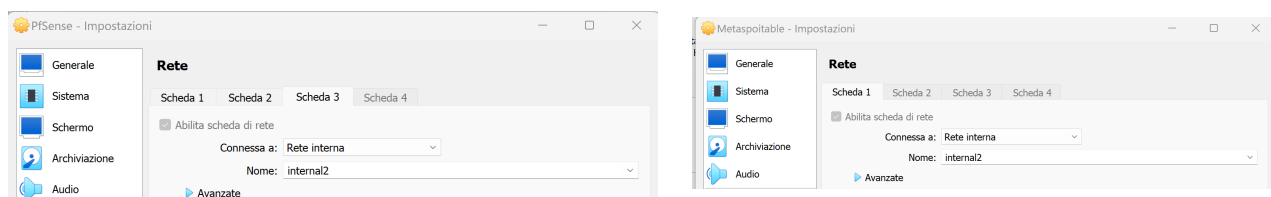
Fabio Benevento - 22/12/2023

### Traccia

Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan (fare uno screenshot che dimostri che prima lo scan per DVWA funzionava e ora non funziona più). Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a PfSense in modo tale da gestire una ulteriore rete.

### Implementazione

In primo luogo ho creato una nuova rete di tipo interna (internal 2) in VirtualBox e ho posizionato la macchina Metasploitable su questa seconda rete.



Ho abilitato l'interfaccia LAN2 tramite la pagina di configurazione di PfSense e ho abilitato il servizio DHCP in maniera da assegnare indirizzi nel range 192.168.50.100-192.168.50.220

Interfaces / LAN2 (em2)

The changes have been applied successfully.

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="LAN2"/> Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	<input type="text" value="xxxxxxxxxxxx"/> This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxx:xxxx:xxxx or leave blank.
MTU	<input type="text"/> If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	<input type="text"/> If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	<input type="text" value="Default (no preference, typically autoselect)"/> 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 its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address	<input type="text" value="192.168.50.1"/> <input type="text" value="/ 24"/>
IPv4 Upstream gateway	<input type="text" value="None"/> <input type="button" value="+ Add a new gateway"/> If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by <a href="#">clicking here</a> .

General DHCP Options

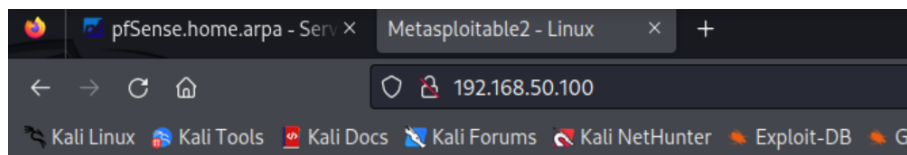
DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN2 interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<input type="text" value="Allow all clients"/> When set to <b>Allow all clients</b> , any DHCP client will get an IP address within this scope/range on this interface. If set to <b>Allow known clients from any interface</b> , any DHCP client with a MAC address listed in a static mapping on <b>any</b> scope(s)/interface(s) will get an IP address. If set to <b>Allow known clients from only this interface</b> , only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
Ignore Denied Clients	<input type="checkbox"/> 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	<input type="checkbox"/> 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	192.168.50.0/24
Subnet Range	192.168.50.1 - 192.168.50.254
Address Pool Range	<input type="text" value="192.168.50.100"/> <input type="text" value="192.168.50.220"/> From To The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools	<input type="button" value="+ Add Address Pool"/> If additional pools of addresses are needed inside of this subnet outside of the above range, they may be specified here.

Ho quindi verificato la corretta configurazione tramite ping e accesso alla pagina DVWA di Metasploitable all'indirizzo 192.168.50.100, che è l'indirizzo assegnato alla macchina Metasploitable

```
(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=4.25 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=11.0 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=6.95 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=63 time=3.83 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=63 time=4.42 ms
64 bytes from 192.168.50.100: icmp_seq=6 ttl=63 time=7.72 ms
64 bytes from 192.168.50.100: icmp_seq=7 ttl=63 time=3.26 ms
^C
— 192.168.50.100 ping statistics —
7 packets transmitted, 7 received, 0% packet loss, time 6052ms
rtt min/avg/max/mdev = 3.255/5.915/10.985/2.575 ms
```



A questo punto ho proceduto con la configurazione della regola di firewall su PfSense in maniera da bloccare l'accesso alla pagina DVWA da Kali. In particolar modo ho impostato una regola Block su protocollo TCP con source address 192.168.1.100 (macchina Kali) e destination address 192.168.50.100 (macchina Metasploitable) e port 80.

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)

From

Custom

To

HTTP (80)

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 DVWA from Kali

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

Accedendo via browser la pagina DVWA risulta ora in effetti irraggiungibile e dai log di PfSense viene mostrato l'intervento del firewall come mostrato in figura.

✗	Jan 7 10:04:43	LAN	Block DVWA from Kali (1704621613)	192.168.1.100:34294	192.168.50.100:80	TCP:S
✗	Jan 7 10:04:43	LAN	Block DVWA from Kali (1704621613)	192.168.1.100:34302	192.168.50.100:80	TCP:S
✗	Jan 7 10:04:44	LAN	Block DVWA from Kali (1704621613)	192.168.1.100:34294	192.168.50.100:80	TCP:S
✗	Jan 7 10:04:44	LAN	Block DVWA from Kali (1704621613)	192.168.1.100:34302	192.168.50.100:80	TCP:S
✗	Jan 7 10:04:46	LAN	Block DVWA from Kali (1704621613)	192.168.1.100:34294	192.168.50.100:80	TCP:S

