

S5L1 firewall Pfsense

L'esercizio di oggi è iniziato installando Pfsense, inserendo 3 schede di rete (la prima in NAT, le altre 2 interne per Kali e Meta) e avviando la macchina virtuale.

Come da consegna, ho modificato gli indirizzi ip delle macchine virtuali per fare in modo che kali e metasploitable2 appartenessero a reti diverse.

General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="LAN"/> Enter a description (name) for the interface here.
IPv4 Configuration Type	<input type="text" value="Static IPv4"/>
IPv6 Configuration Type	<input type="text" value="Track Interface"/>
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:xx:xx 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), 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="192.168.1.1"/> / <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 clicking here .	

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	<input type="text" value="Static IPv4"/>
IPv6 Configuration Type	<input type="text" value="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:xx:xx 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="192.168.32.1"/> / <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 clicking here .	

dopo aver aggiunto le interfacce procediamo a impostare il loro indirizzo di gateway, per fare in modo che le Kali e Meta possano comunicare

Muovendosi nella sezione firewall>rules e cliccando sulla freccia verde creiamo una regola che blocchi l'invio di pacchetti che utilizzano i protocolli TCP/UDP da Kali verso Meta, specificando i loro indirizzi ip all'interno di "source" e "destination"

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/UDP

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

192.168.32.101

/

Destination Port Range

any

From

Custom

any

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

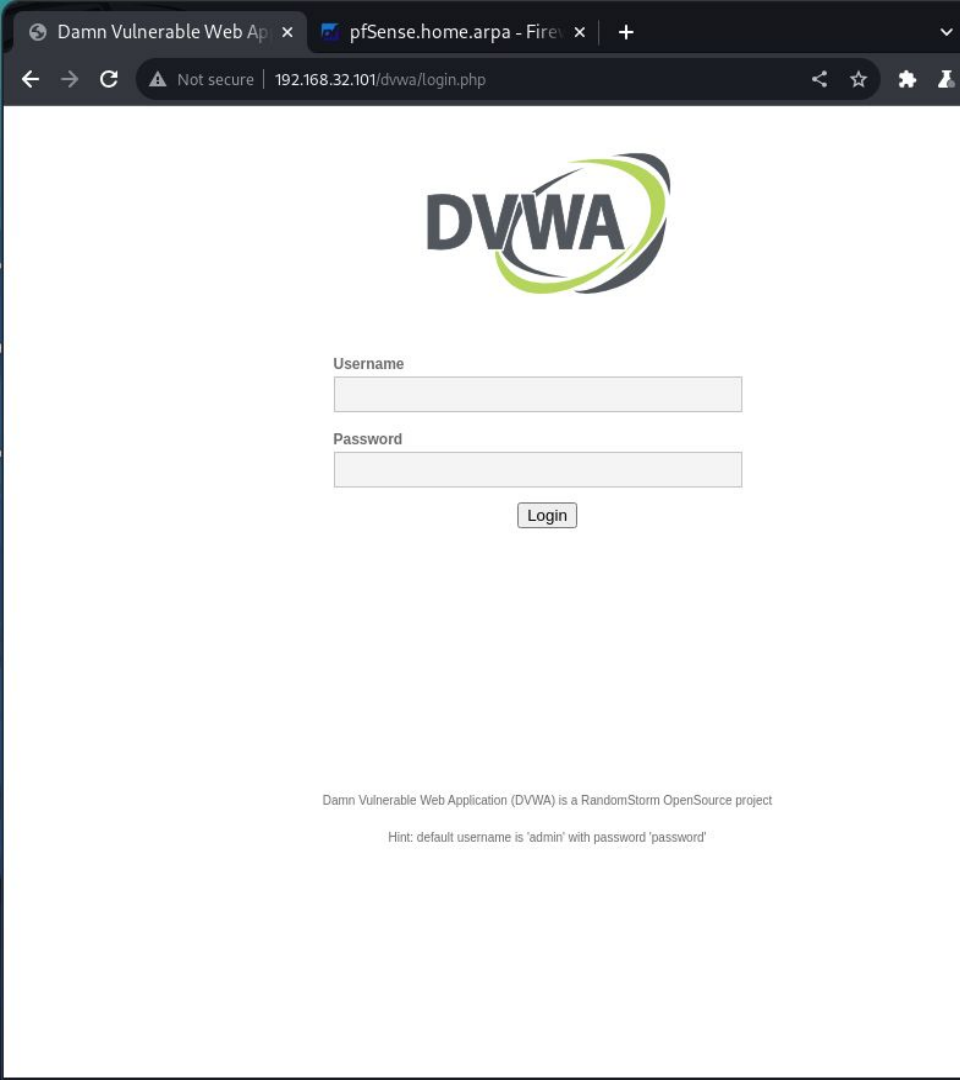
☐ Log packets that are handled by this rule

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

Quando la regola è disattivata (come riportato sotto) è ancora possibile collegarsi a Metasploitable2 e alla pagina DVWA

Floating WAN LAN LAN2

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 2/3.68 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/86 KiB	IPv4 TCP/UDP	192.168.1.100	*	192.168.32.101	*	*	none			
<input type="checkbox"/>	✓ 0/6.68 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	



Riattivandola invece, non è più possibile accedere all'indirizzo ip di Meta, oltretutto la scansione nmap non riesce a rilevare porte aperte o chiuse: risultano tutte filtrate.

```
(kali@kali)~[~]  
$ sudo nmap 192.168.32.101  
[sudo] password for kali:  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-18 13:53 CET  
Nmap scan report for 192.168.32.101  
Host is up (0.0025s latency).  
All 1000 scanned ports on 192.168.32.101 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
  
Nmap done: 1 IP address (1 host up) scanned in 39.13 seconds
```

