

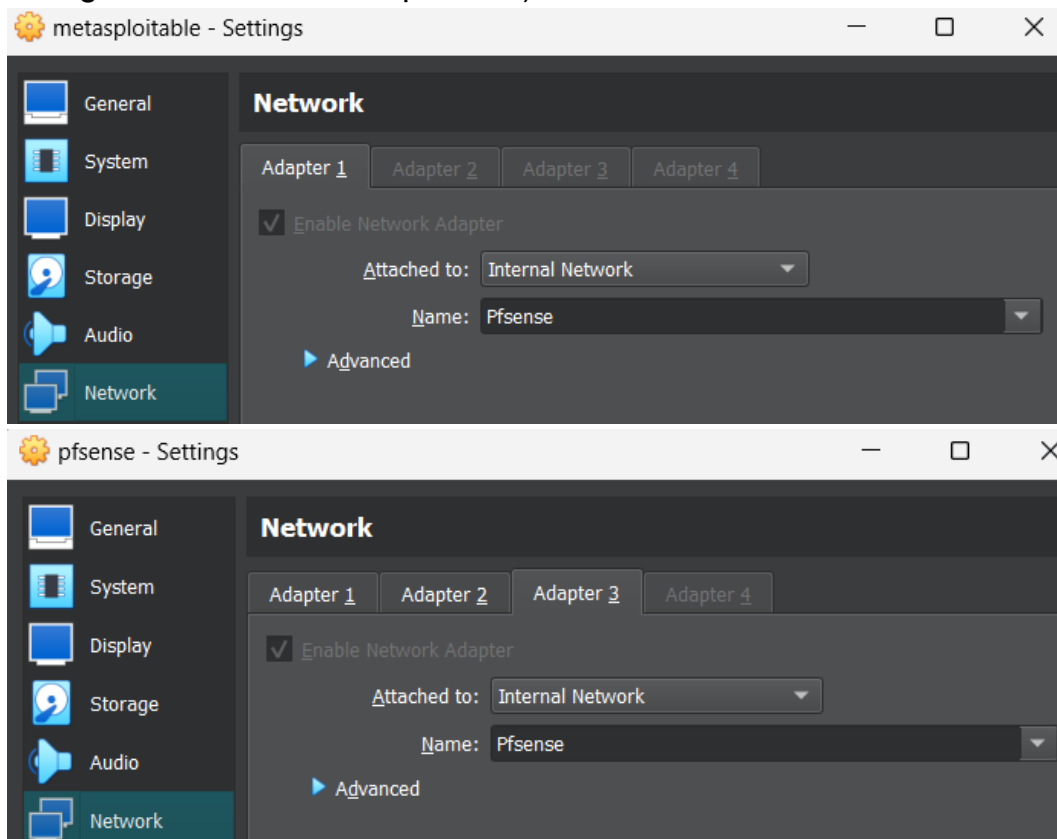
Creazione Policy PFSense

Traccia: Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse.

Svolgimento: Per prima cosa, andiamo ad aggiungere una nuova interfaccia di rete su PFSense che si chiamerà OPT1.

```
WAN (wan)          -> em0          -> 10.0.2.15 (DHCP)
LAN (lan)           -> em1          -> 192.168.49.1
OPT1 (opt1)         -> em2          -> 192.168.50.1
```

Dopodiché, colleghiamo Metasploitable ad OPT1, con la rete pfsense (a cui è collegato anche il firewall pfsense).



A questo punto, andiamo a configurare l'ip statico di Metasploitable in modo che faccia parte della rete interna di OPT1.

```
# 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 static
address 192.168.50.101
netmask 255.255.255.0
network 192.168.50.0
broadcast 192.168.50.255
gateway 192.168.50.1
```

Kali Linux invece è impostato con l'IP 192.168.49.101 e perciò fa parte di un'altra subnet.


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

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.49.100
netmask 255.255.255.0
gateway 192.168.49.1
```

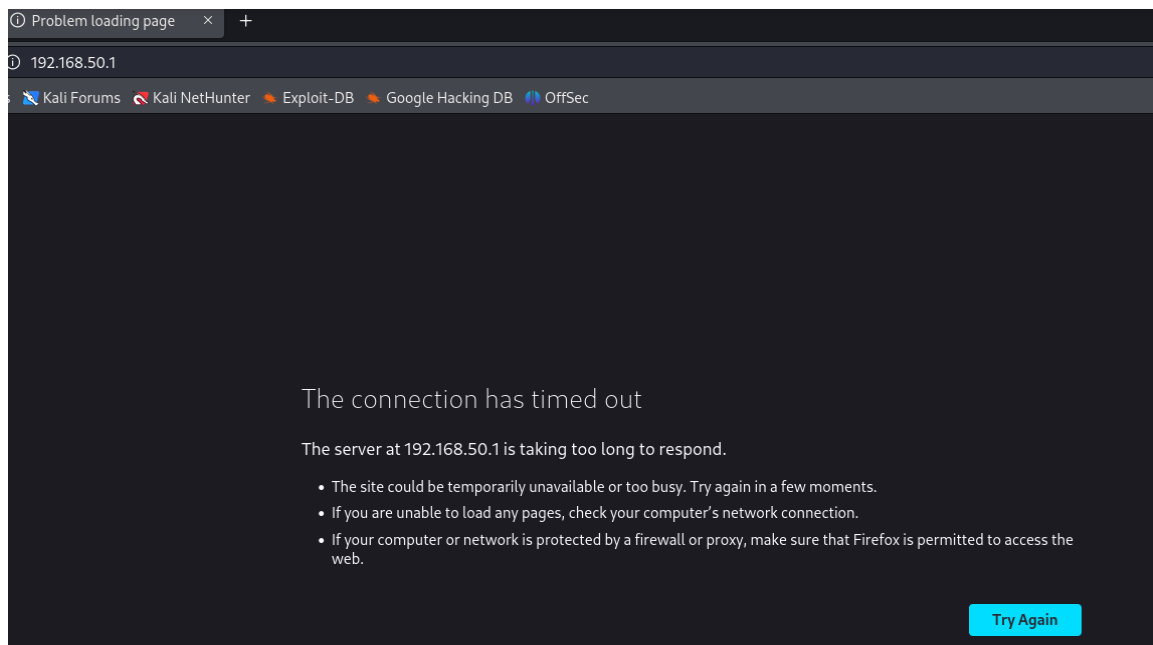
Una volta configurate le due reti, andiamo sul GUI Web di PFSense per impostare una nuova regola per bloccare lo scan delle porte e la connettività alla DVWA da parte di Kali Linux.

Edit Firewall rule	
Action	<div>Block ▾</div> <p>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.</p>
Disabled	<div><input type="checkbox"/> Disable this rule</div> <p>Set this option to disable this rule without removing it from the list.</p>
Interface	<div>LAN ▾</div> <p>Choose on which interface packets must come in to match this rule.</p>
Protocol	<div>TCP ▾</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
Source	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>Single host or alias ▾</div></p> <p>Address: <div>192.168.49.101</div> / ▾</p> <p><div>Advanced</div> - Show source port range</p>
Destination	<div><input type="checkbox"/> not</div> <p>Use this option to invert the sense of the match.</p> <p>Type: <div>Single host or alias ▾</div></p> <p>Address: <div>192.168.50.101</div> / ▾</p>
Destination port range	<p>from: <div>SSH ▾</div></p> <p>to: <div>HTTP ▾</div></p> <p>Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port</p>
Log	<div><input type="checkbox"/> Log packets that are handled by this rule</div> <p>Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).</p>
Description	<div></div> <p>You may enter a description here for your reference.</p>

Save

Cancel

Impostando l'interfaccia LAN (che corrisponde alla subnet di Kali), il protocollo TCP, il source IP di Kali, il destination IP di Meta e poi il range delle porte da SSH (22) a HTTP (80), il collegamento tra le due sarà interrotto. Provando a connettersi tramite browser Firefox, la connessione non viene stabilita.



Attraverso i log di sistema del firewall, possiamo vedere come la nuova regola sia efficace e blocchi i tentativi di connessione.

	May 6 16:10:49	LAN	192.168.49.100:39124	192.168.50.101:80	TCP:S
	May 6 16:10:49	LAN	192.168.49.100:39140	192.168.50.101:80	TCP:S
	May 6 16:10:53	LAN	192.168.49.100:39124	192.168.50.101:80	TCP:S
	May 6 16:10:53	LAN	192.168.49.100:39140	192.168.50.101:80	TCP:S