



# Esercizio S5L1

Penetration testing

## Parte 1: Assegnazione degli indirizzi IP

### Macchine virtuali interessate:

- Metasploitable
- PfSense
- Kali Linux

**Cosa viene assegnato:** dopo aver creato la 3° rete sui dispositivi, attivando sulla 1° di metasploitable e 3° di PfSense la rete interna.

- Si assegna un indirizzo IP alla LAN di PfSense;
- Si assegna l'indirizzo IP della LAN di PfSense al gateway di Kali Linux;
- Si assegna il gateway di metasploitable alla 3° rete di PfSense(opt1);
- Si assegna un indirizzo IP a Kali che faccia parte della stessa rete dell'indirizzo della LAN di PfSense e diversa rete di Metasploitable.

Kali Linux

```
kali㉿kali: ~
File Actions Edit View Help
GNU nano 7.2          /etc/network/interfaces
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 192.168.40.100
    netmask 255.255.255.0
    network 192.168.40.0
    broadcast 192.168.40.255
    gateway 192.168.40.2
```

PfSense

```

WAN (wan)      -> en0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> en1      -> v4: 192.168.40.2/24
OPT1 (opt1)    -> en2      -> v4: 192.168.50.1/24

8) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

```

## Metasploitable

```

GNU nano 2.0.7  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 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

```

## Parte 2: Controllo di comunicazione tra macchine

Terminal window (kali㉿kali: ~)

```

$ ping 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=63 time=5.13 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=63 time=1.64 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=63 time=8.01 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=63 time=2.24 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=63 time=3.03 ms

```

Browser window (Warning: Never expose this VM to an untrusted network!)

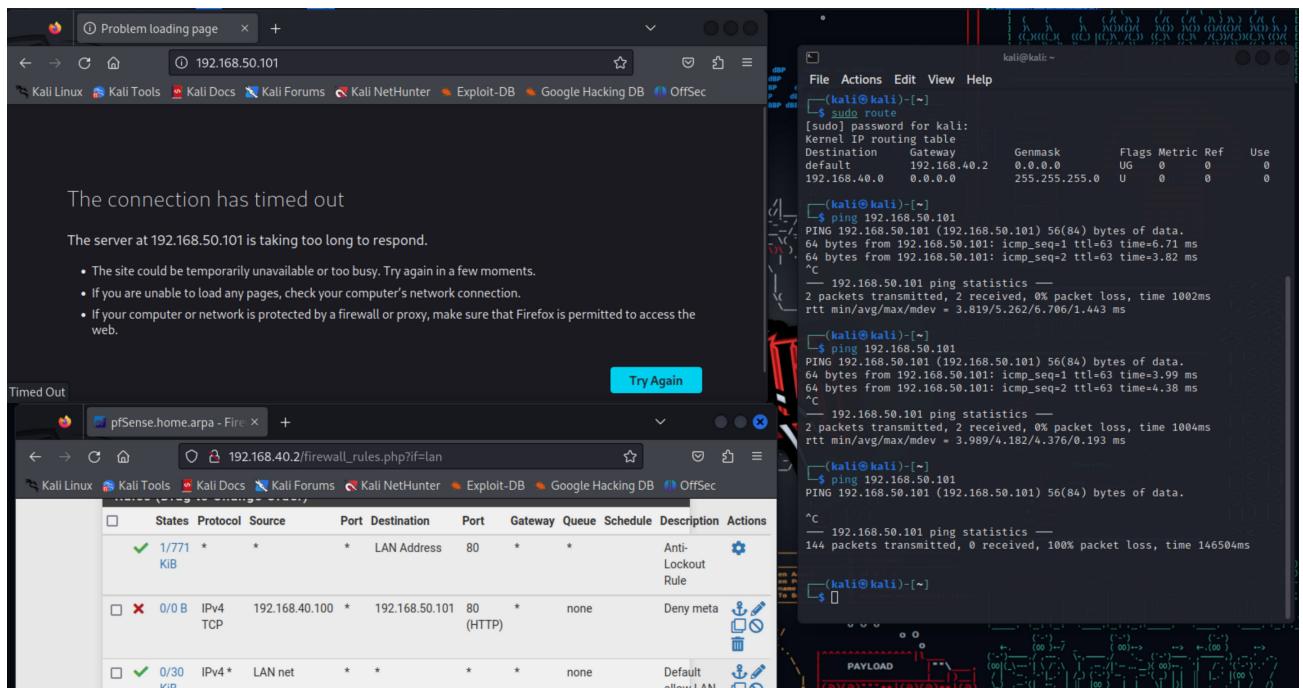
Browser window (pfSense.home.arpa - Firefox)

Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2/1.46 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✓ 0/3 KIB	IPv4 TCP	192.168.40.100	*	192.168.50.101	*	*	none		Pass meta	
✓ 18/97 KIB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓ 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6	

## Parte 3: Creazione della regola su Pfsense

<b>Action</b>	<input type="button" value="Block"/> 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.					
<b>Disabled</b>	<input type="checkbox"/> Disable this rule				
Set this option to disable this rule without removing it from the list.					
<b>Interface</b>	<input type="button" value="LAN"/> LAN				
Choose the interface from which packets must come to match this rule.					
<b>Address Family</b>	<input type="button" value="IPv4"/> IPv4				
Select the Internet Protocol version this rule applies to.					
<b>Protocol</b>	<input type="button" value="TCP"/> TCP				
Choose which IP protocol this rule should match.					
<b>Source</b>					
<b>Source</b>	<input type="checkbox"/> Invert match	<input type="button" value="Single host or alias"/> Single host or alias	<input type="button" value="192.168.40.100"/> 192.168.40.100	/	<input type="button" value="Display Advanced"/> 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.					
<b>Destination</b>					
<b>Destination</b>	<input type="checkbox"/> Invert match	<input type="button" value="Single host or alias"/> Single host or alias	<input type="button" value="192.168.50.101"/> 192.168.50.101	/	<input type="button" value="Display Advanced"/> Display Advanced
<b>Destination Port Range</b>	<input type="button" value="any"/> any	<input type="button" value="any"/> any	<input type="button" value="From"/> From	<input type="button" value="To"/> To	<input type="button" value="Custom"/> Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.					
<b>Extra Options</b>					
<b>Log</b>	<input type="checkbox"/> 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 <a href="#">Status: System Logs: Settings</a> page).					
<b>Description</b>	<input type="button" value="Deny meta"/> Deny meta				

## Parte 4: Controllo post-creazione regola



THE  
END