

# PENETRATION TESTING

## TASK

- Dopo aver configurato Kali, Metasploitable e PfSense, tra cui, le prime due in rete Interna e l'ultima abilitando altre due reti aggiuntive, dobbiamo permettere che le tre macchine possano pingarsi tra di loro (dimostrazione successivamente). Pertanto è necessario che le macchine Kali e Metasploitable siano su reti diverse.
- Creare una regola Firewall che non consenta l'accesso alla DVWA da Kali e ne impedisca lo scan.

## ANALISI E VALUTAZIONI:

Per prima cosa andiamo a configurare kali e metasploitable con due reti differenti, rispettivamente con questi indirizzi:

MACCHINA	INDIRIZZO IP ADDRESS	RETE
Kali	192.168.50.100	Rete 1 (LAN1)
Metasploitable	192.168.90.101	Rete 2 (LAN2)
Pfsense	192.168.50.103	NAT, Rete 1 (LAN1), Rete 2 (LAN2)

Per entrare nel sito di pfsense da kali dobbiamo inserire l'indirizzo ipv4 per la macchina e per farlo basta inserire nel terminale di pfsense il tasto "1" per la modifica dell'indirizzo e inseriamo rispettivamente solo per l'indirizzo Ipv4 192.168.50.103.

Successivamente possiamo andare ad impostare una nuova rete per pfsense e per farlo entriamo nel sito da Kali utilizzando il suo indirizzo IP impostato. La nuova rete servirà per poter collegare rispettivamente le due macchine Kali e Metasploitable, di fatti la configurazione per la LAN1 e la LAN2 (rete che creeremo cliccando su ADD da "Interfaces → Assignment") sarà rispettivamente questa:

- LAN1

The screenshot shows the pfSense web interface. At the top, there is a navigation bar with the pfSense logo and various menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation bar, a warning message states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The main content area is titled "Interfaces / LAN1 (em1)". Under the "General Configuration" section, the "Enable" checkbox is checked, and the "Description" field is set to "LAN1". The "IPv4 Configuration Type" is set to "Static IPv4", and the "IPv6 Configuration Type" is set to "None". The "MAC Address" field is set to "xxxxxxxxxxxx".

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	192.168.50.103	/ 24
IPv4 Upstream gateway	None	<a href="#">+ Add a new gateway</a>

- LAN2

**pfSense** COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

## Interfaces / LAN2 (em2)

### General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	LAN2 <small>Enter a description (name) for the interface here.</small>
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xxxxxxxxxxxx <small>This field can be used to modify ("spoof") the MAC address of this interface.</small>

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	192.168.90.103	/ 24
IPv4 Upstream gateway	None	<a href="#">+ Add a new gateway</a>

Dopo di che facciamo un scansione di DVWA con nmap -sS e andiamo a vedere le porte aperte sull'indirizzo IP target. Il risultato sarà pressocchè questo:

```
(kali@kali)-[~]
$ sudo nmap 192.168.90.101 -sS
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 13:10 EST
Nmap scan report for 192.168.90.101 (192.168.90.101)
Host is up (0.0039s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.02 seconds
```

Il risultato che dovremmo ottenere dal firewall che andremo a creare sarà il filtraggio sulla porta 80. Per la creazione del firewall basterà entrare sempre su pfSense e andare su "Firewall":

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** LAN1  
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 Single host or alias 192.168.50.100 /

[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 Single host or alias 192.168.90.101 /

**Destination Port Range** HTTP (80)  HTTP (80)   
From Custom 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 the [Status: System Logs: Settings](#) page).

**Description**

Così facendo andiamo a fare nuovamente un test per vedere se le macchine Kali e Metasploitable continuano a pingarsi tra loro:

```
(kali㉿kali)-[~]
$ ping 192.168.90.101
PING 192.168.90.101 (192.168.90.101) 56(84) bytes of data.
64 bytes from 192.168.90.101: icmp_seq=1 ttl=63 time=1.07 ms
64 bytes from 192.168.90.101: icmp_seq=2 ttl=63 time=0.984 ms
64 bytes from 192.168.90.101: icmp_seq=3 ttl=63 time=1.62 ms
^Z
zsh: suspended ping 192.168.90.101
```

Il ping funziona e di conseguenza il firewall però blocca l'accesso al sito dvwa e ora andando a testare la scansione, il firewall va a filtrare i pacchetti della porta 80 di cui abbiamo inserito:

```
(kali㉿kali)-[~]
└─$ sudo nmap 192.168.90.101 -sS
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 13:16 EST
Nmap scan report for 192.168.90.101 (192.168.90.101)
Host is up (0.014s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    filtered http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds
```