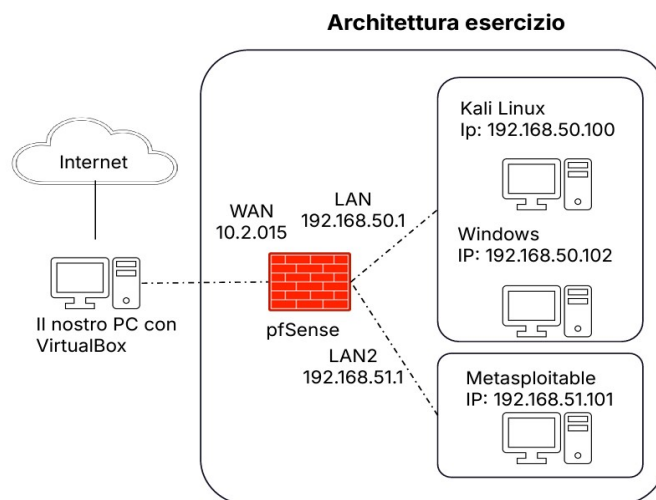


# CSPT0524IT – W9D4

## Obiettivo dell'Esercizio

- Simulare lo stesso ambiente virtuale
- Bloccare a Kali l'accesso alla DVWA, ospitata su Metasploitable.
- Garantire che le due macchine (Kali e Metasploitable) si trovino in subnet separate e siano gestite da pfSense.
- Dimostrare, attraverso screenshot, l'efficacia della regola firewall configurata.
- Facoltativamente Ispezione dei Log del Firewall e fare Troubleshooting.



In questo progetto, ho configurato una nuova infrastruttura di rete basata su pfSense per gestire un ambiente di laboratorio virtuale dedicato. Partendo da un'installazione già esistente di pfSense (denominato "pfSense principale"), è stata creata una subnet dedicata e un secondo pfSense ("pfSense figlio") all'interno di tale subnet. Questa configurazione permette di isolare e ottimizzare la gestione del laboratorio virtuale.

- La WAN del pfSense figlio si collega alla subnet del pfSense principale. (/29 per eventuali host)
- La LAN del pfSense figlio è dedicata alle macchine virtuali del laboratorio, consentendo loro accesso controllato a internet.

Svolgimento dell'Esercizio

1. Configurazione della Rete





Reti Create:

- WAN -> 192.168.15.0/24
- LAN -> 192.168.50.0/24
- DMZ -> 192.168.51.0/24




```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on Epic-pfSense ***

WAN (wan)      -> vmx0      -> v4/DHCP4: 192.168.15.252/29
LAN (lan)      -> vmx1.6    -> v4: 192.168.50.1/24
DMZ (opt1)     -> vmx1.7    -> v4: 192.168.51.1/24
```

VLANs:



Interface Assignments	Interface Groups	Wireless	VLANs	QinQs	PPPs	GREs	GIFs	Bridges	LAGGs
VLAN Interfaces									
Interface	VLAN tag	Priority	Description	Actions					
vmx1	6	1	LAN	 					
vmx1	7	2	DMZ	 					

Interfacce Assegnate:







Interface	Network port
WAN	vmx0 (00:0c:29:20:60:39)
LAN	VLAN 6 on vmx1 (LAN) 
DMZ	VLAN 7 on vmx1 (DMZ) 
Available network ports:	vmx1 (00:0c:29:20:60:43) 

Gateway e Interfacce:

Gateways






















Name	RTT	RTTsd	Loss	Status
 WAN_DHCP  192.168.15.251	0.3ms	0.1ms	0.0%	Online

Interfaces











 WAN		autoselect	192.168.15.252
 LAN		autoselect	192.168.50.1
 DMZ		autoselect	192.168.51.1

## 2. Configurazione Alias e DNS

Alias:

Firewall Aliases IP				
Name	Type	Values	Description	Actions
DMZ_Network	Network(s)	192.168.51.0/24	DMZ_Network	  
Epic_Kali	Host(s)	192.168.50.100	Kali VM	  
Epic_Metasploitable	Host(s)	192.168.51.101	Metasploitable VM	  
Epic_pfSense	Host(s)	192.168.15.252, 192.168.50.1, 192.168.51.1	pfSense_02	  
Epic_Win7	Host(s)	192.168.50.103	Win7 VM	  
Epic_Win10	Host(s)	192.168.50.102	Win10 VM	  
LAN_Network	Network(s)	192.168.50.0/24	LAN_Network	  








DNS Resolver:

Host Overrides				
Host	Parent domain of host	IP to return for host	Description	Actions
Epic-Kali	epicode	192.168.50.100	Kali DNS	 
Epic-Metasploitable	epicode	192.168.51.101	Metasploitable DNS	 
Epic-pfSense	epicode	192.168.15.252,192.168.50.1,192.168.51.1	pfSense_02 DNS	 
Epic-Win10	epicode	192.168.50.102	Win10 DNS	 
Epic-Win7	epicode	192.168.50.103	Win7 DNS	 

## 3. Configurazione delle Regole







LAN:

- Regola 1: Anti-Lockout di Default per l'interfaccia LAN
- Regola 2: Consenti a Kali di accedere a tutta la rete (Online e VLANs) su tutti i protocolli via IPv4

Floating   WAN   LAN   DMZ											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓	1/2.19 MiB	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓	4/16 KiB	IPv4 *	Epic_Kali	*	*	*	none		Allow   Kali VM -> Any	     

DMZ:

- Regola 1: Nega a tutta la rete DMZ di raggiungere tutta la rete LAN

Floating   WAN   LAN   DMZ											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗	0/0 B	IPv4+6 *	DMZ subnets	*	LAN subnets	*	none		Deny   DMZ -> LAN	     

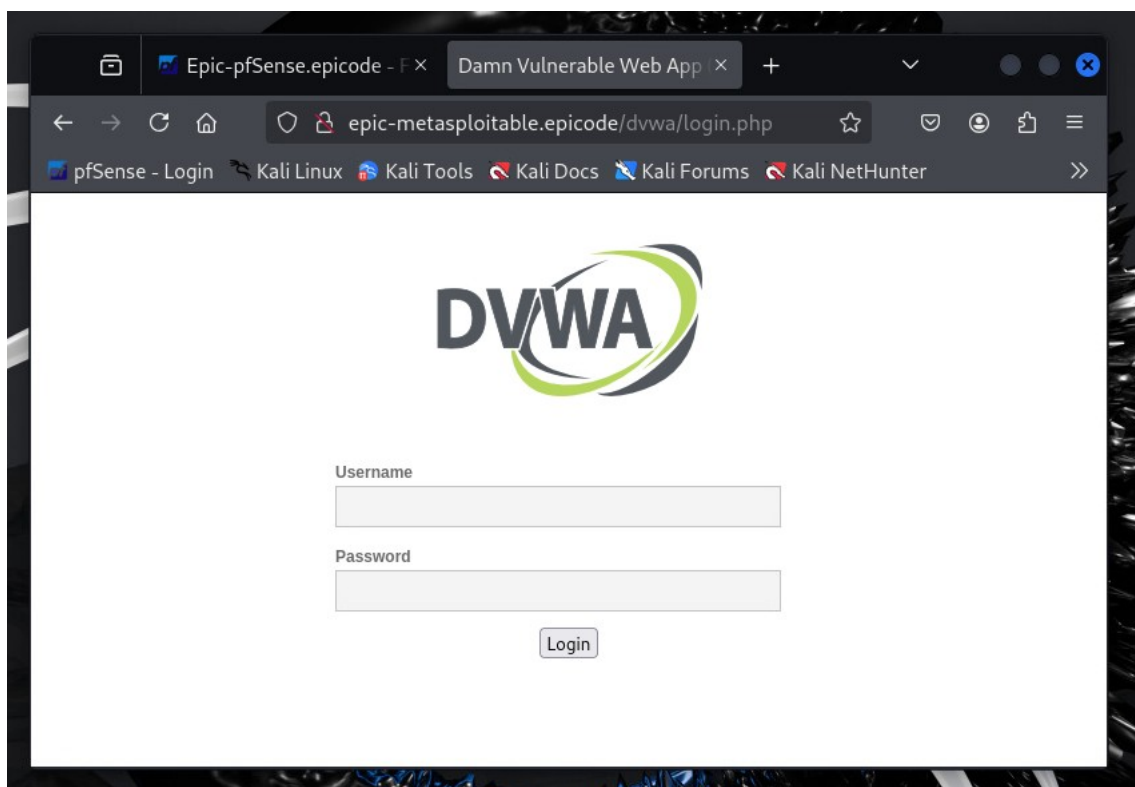
## 4. Test di Comunicazione e Scansione Nmap

KALI:

- Kali raggiunge con successo metasploitable via PING

```
(kali㉿kali)-[~]  
$ ping epic-metasploitable.epicode  
PING epic-metasploitable.epicode (192.168.51.101) 56(84) bytes of data.  
64 bytes from Epic-Metasploitable.epicode (192.168.51.101): icmp_seq=1 ttl=63 time=8.79 ms  
64 bytes from Epic-Metasploitable.epicode (192.168.51.101): icmp_seq=2 ttl=63 time=0.397 ms  
64 bytes from Epic-Metasploitable.epicode (192.168.51.101): icmp_seq=3 ttl=63 time=0.456 ms  
^C  
--- epic-metasploitable.epicode ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2007ms  
rtt min/avg/max/mdev = 0.397/3.213/8.787/3.941 ms
```

- Kali raggiunge con successo metasploitable via BROWSER sulla porta 80



Scansione SYN/TCP su porta 80 di Metasploitable

- **Comando** scan 1: `nmap -sV -sS -p 80 192.168.51.101`
- **Comando** scan 2: `nmap -sV -sT -p 80 192.168.51.101`
- **Output** = '80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)'

## La porta 80/TCP è aperta con servizio http Apache v2.2.8

```
(kali@kali)-[~]
$ nmap -sV -sS -p 80 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-20 18:22 CET
Nmap scan report for Epic-Metasploitable.epicode (192.168.51.101)
Host is up (0.00040s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.59 seconds

(kali@kali)-[~]
$ nmap -sV -sT -p 80 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-20 18:22 CET
Nmap scan report for Epic-Metasploitable.epicode (192.168.51.101)
Host is up (0.00043s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.51 seconds
```

## 5. Blocca Porta 80 di Metasploitable a Kali

Regola di Reject :

La Regola riportata NEGA a Kali l'Accesso sulla porta 80 di Metasploitable mostrandola chiusa, in realtà Metasploitable risponde, con un RST

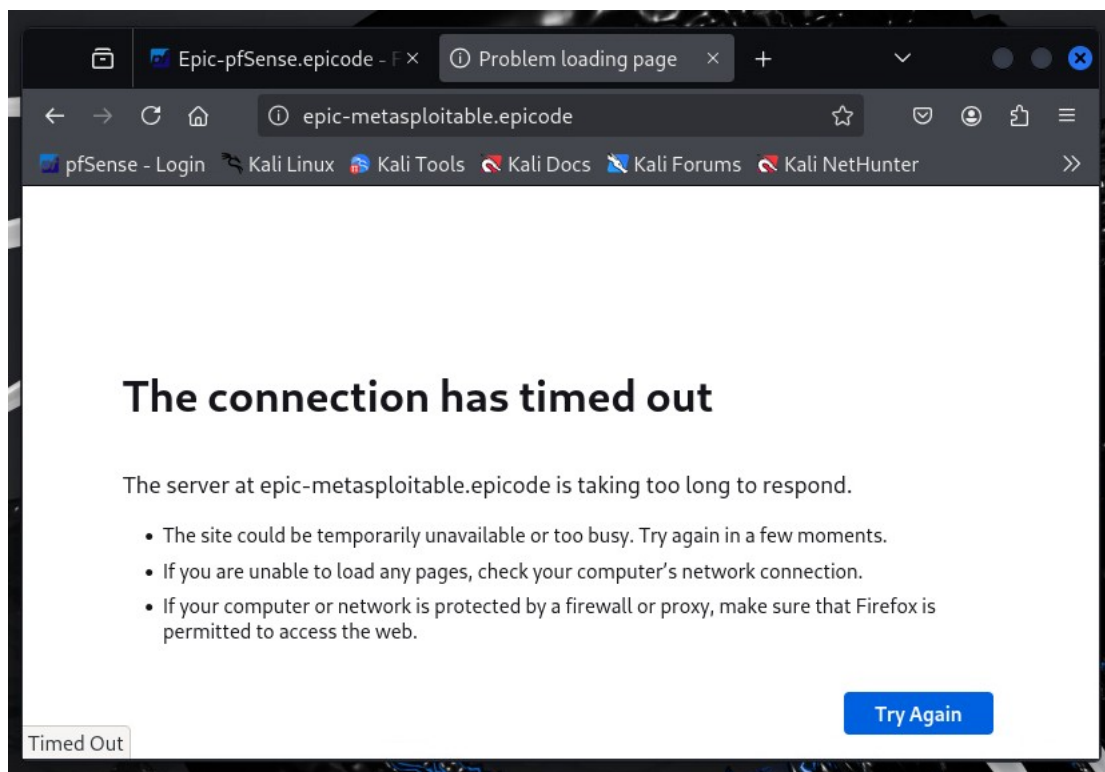
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/664 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/88 B	IPv4+6 TCP	Epic_Kali	*	Epic_Metasploitable	80 (HTTP)	*	none		Deny   Kali VM -> Port 80 - Metasploitable	
<input type="checkbox"/>	4/302 KiB	IPv4 *	Epic_Kali	*	*	*	*	none		Allow   Kali VM -> Any	

La Regola Block invece mostra la porta filtrata a Nmap, quindi si accorge che il traffico su quella porta è filtrato

## 6. Re-Test Browser e Re-Scan Nmap

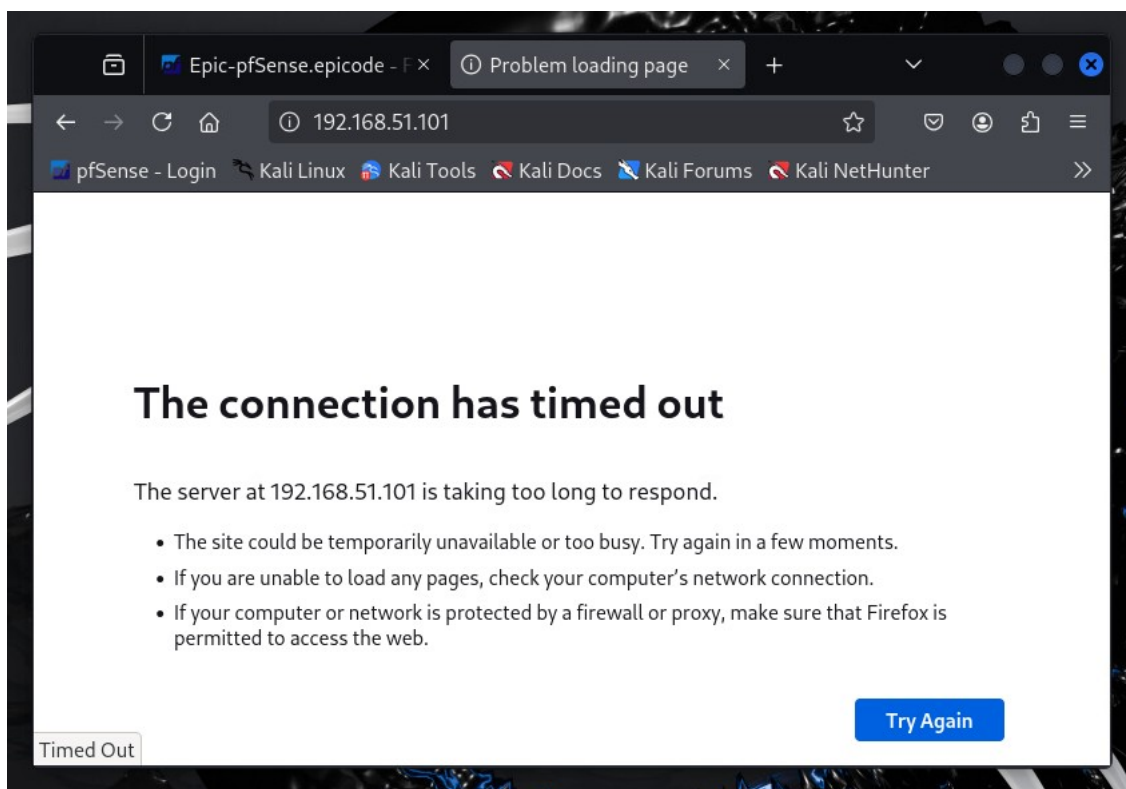
DNS

**Kali non ha più accesso alla porta 80 di Metasploitable**



IP

**Kali non ha più accesso alla porta 80 di Metasploitable**





Re-Scan SYN/TCP su porta 80 di Metasploitable

- **Comando** scan 1: `nmap -sV -sS -p 80 192.168.51.101`
- **Comando** scan 2: `nmap -sV -sT -p 80 192.168.51.101`
- **Output** = ‘80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)’

**La porta 80/TCP è filtrata (Nmap non può stabilire se è aperta perche il traffico è bloccato),  
Si nota che il servizio Apache e la sua versione non è più visibile da Nmap**

```
(kali@kali)-[~]
$ nmap -sV -sS -p 80 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-20 18:49 CET
Nmap scan report for Epic-Metasploitable.epicode (192.168.51.101)
Host is up (0.00040s latency).

PORT      STATE      SERVICE VERSION
80/tcp    filtered  http

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

(kali@kali)-[~]
$ nmap -sV -sT -p 80 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-20 18:51 CET
Nmap scan report for Epic-Metasploitable.epicode (192.168.51.101)
Host is up (0.00044s latency).

PORT      STATE      SERVICE VERSION
80/tcp    filtered  http

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
```

7. Ispezione Log

✖	Jan 20 22:41:38	LAN	192.168.50.100:48686	192.168.51.101:80	TCP:A
✖	Jan 20 22:41:55	LAN	192.168.50.100:51819	192.168.51.101:80	TCP:A
✖	Jan 20 22:51:55	LAN	192.168.50.100:44329	192.168.51.101:80	TCP:A
✖	Jan 20 22:51:55	LAN	192.168.50.100:44585	192.168.51.101:80	TCP:S
✖	Jan 20 22:52:41	LAN	192.168.50.100:45989	192.168.51.101:80	TCP:A
✖	Jan 20 22:52:41	LAN	192.168.50.100:39526	192.168.51.101:80	TCP:S
✖	Jan 20 22:54:38	LAN	192.168.50.100:57922	192.168.51.101:80	TCP:A
✖	Jan 20 22:54:38	LAN	192.168.50.100:56516	192.168.51.101:80	TCP:S
✖	Jan 20 22:55:20	LAN	192.168.50.100:64710	192.168.51.101:80	TCP:A
✖	Jan 20 22:55:20	LAN	192.168.50.100:34934	192.168.51.101:80	TCP:S
✖	Jan 20 22:55:28	LAN	192.168.50.100:37849	192.168.51.101:80	TCP:A
✖	Jan 20 22:55:28	LAN	192.168.50.100:41770	192.168.51.101:80	TCP:S
✖	Jan 20 22:57:09	LAN	192.168.50.100:55447	192.168.51.101:80	TCP:A
✖	Jan 20 22:57:09	LAN	192.168.50.100:35036	192.168.51.101:80	TCP:S

### ***Obiettivi Raggiunti:***

- Simulato lo stesso ambiente virtuale
- Negato a Kali l'accesso sulla porta 80 di Metasploitable
- Garantire che le due macchine (Kali e Metasploitable) si trovino in subnet separate e siano gestite da pfSense.
- Dimostrato, attraverso Screenshot, l'efficacia della regola firewall configurata.
- Facoltativamente Ispezionato i Log del Firewall.

Francesco Rinaldi