

Creazione Policy PfSense

Obiettivo: Creazione pratica di una regola Firewall che blocchi l'accesso a DVWA

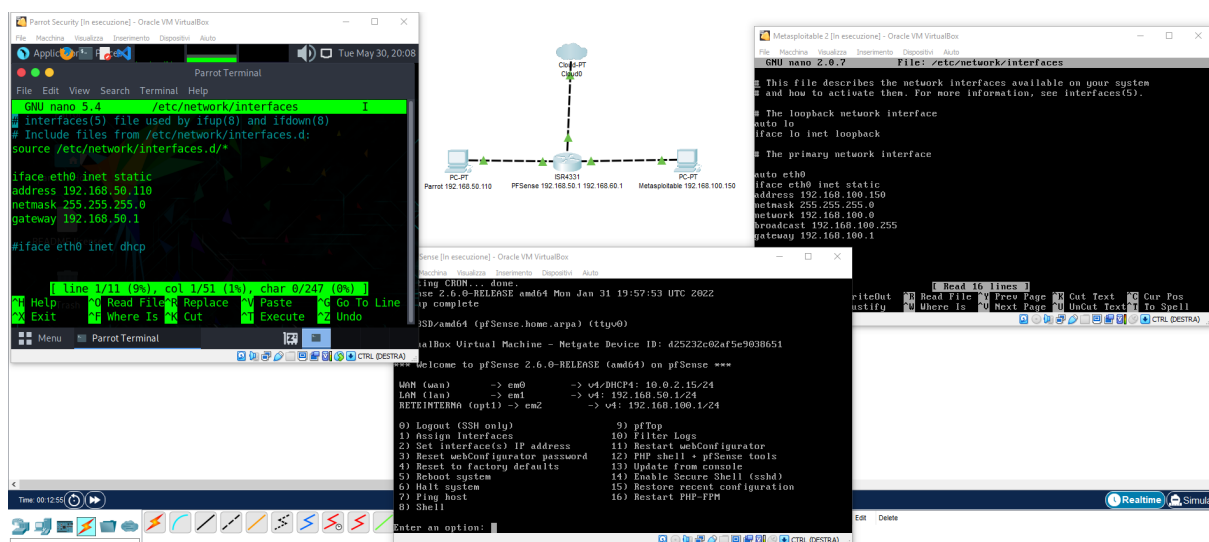
Software utilizzati:

- **Parrot OS**
- **PfSense** utilizzato in questo caso come Router e Firewall
- **Metasploitable 2** (dove si trova la DVWA)

1) Configurazione Indirizzi IP

Per iniziare l'esercizio ho dovuto settare per prima cosa gli indirizzi IP con annessi Gateway delle due macchine:

- **Parrot:** 192.168.50.110/24 - **Gateway:** 192.168.50.1
- **Metasploitable:** 192.168.100.150/24 - **Gateway:** 192.168.100.1



Ho configurato inoltre due reti interne su PfSense:

- **LAN** settata secondo il gateway della macchina **Parrot**
- **RETEINTERNA** collegata a **Metasploitable** simulando una rete estranea alla **LAN** (per esempio uno studio in casa)

2) Creazione Policy del Firewall

Per la creazione della regola del Firewall sono entrato da browser dentro **PfSense** utilizzando l'indirizzo **192.168.50.1** e cliccando su **Firewall/Rules** ho aggiunto sulla **RETEINTERNA** la regola che bloccava lo scambio di protocolli TCP provenienti da Parrot (source) con destinazione Metasploitable (porta 80). Ho dovuto settare la stessa regola posizionandola sopra tutte le altre sulla rete LAN perchè quest'ultime facevano comunicare lo stesso i due indirizzi IP.

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 RETEINTERNA
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 192.168.50.110 /

[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 192.168.100.150 /

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.

Questa è la regola usata per entrambe le reti interne.

Floating

WAN

LAN

RETEINTERNA

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 3.00 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	192.168.50.110	*	192.168.100.150	80 (HTTP)	*	none			
<input type="checkbox"/>	1 / 3 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add

Add

Delete

Save

Separator

Floating

WAN

LAN

RETEINTERNA

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 TCP	192.168.50.110	*	192.168.100.150	80 (HTTP)	*	none			

Add

Add

Delete

Save

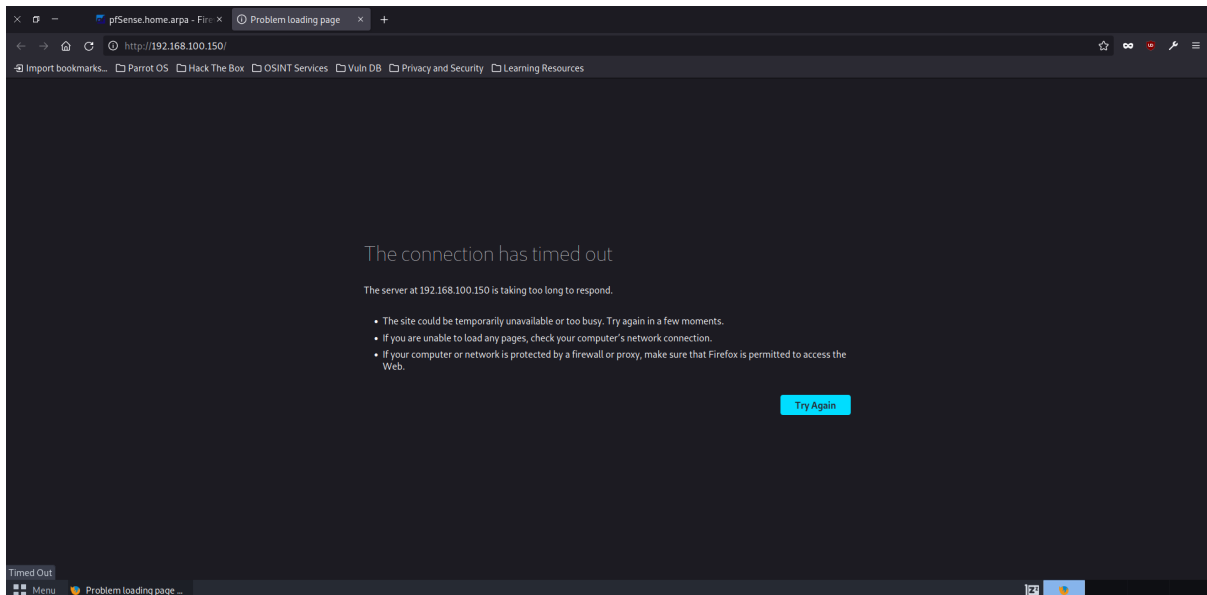
Separator

Queste due immagini mostrano invece le regole settate per entrambe le reti. Nel caso della **LAN** non è necessario disattivarle, ma l'importante è mettere la regola di blocco prima di qualsiasi regola "permissiva" perchè l'ordine con il quale vengono eseguite va dall'alto verso il basso.

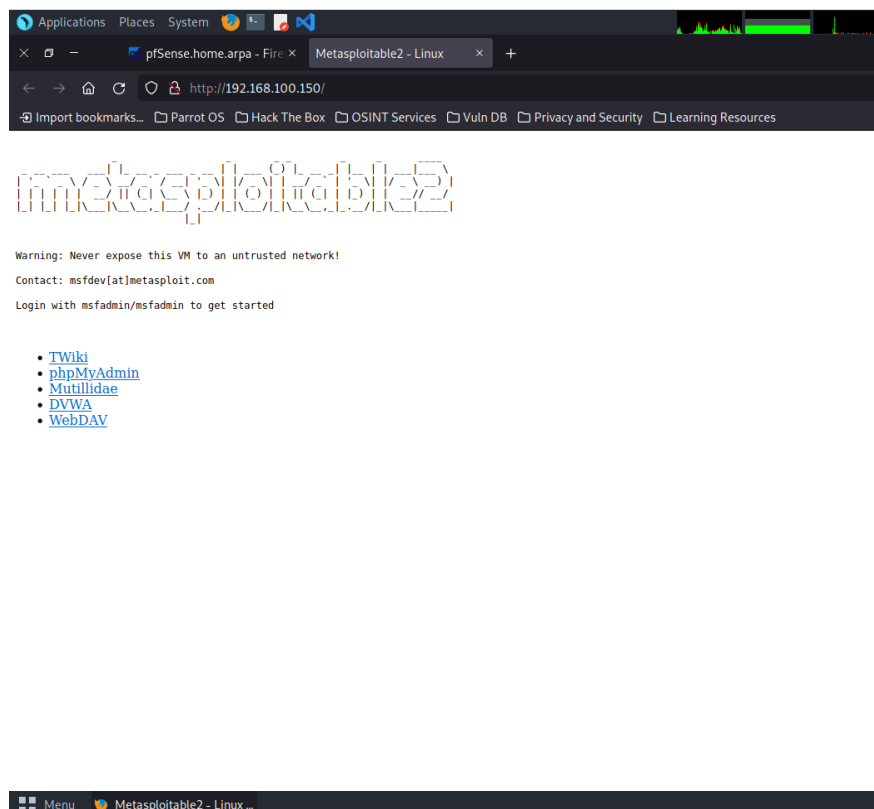
3) Prova da Browser

Ho effettuato due prove:

- *Prima prova:* con **policy firewall** attivate; il risultato è stato un lungo periodo di caricamento che ha portato il browser a lasciare un messaggio dove diceva che il tempo di risposta era troppo lungo, quindi la **Metasploitable** era irraggiungibile



- *Seconda prova:* con **policy firewall** disattivate; in questo caso il browser si è immediatamente connesso alla **Metasploitable** ed è stato possibile entrare nella **DVWA**.





Username

Password

Login