Relazione progetto S5-L1

Studente: Simone Mininni

Configurazione firewall pfsense

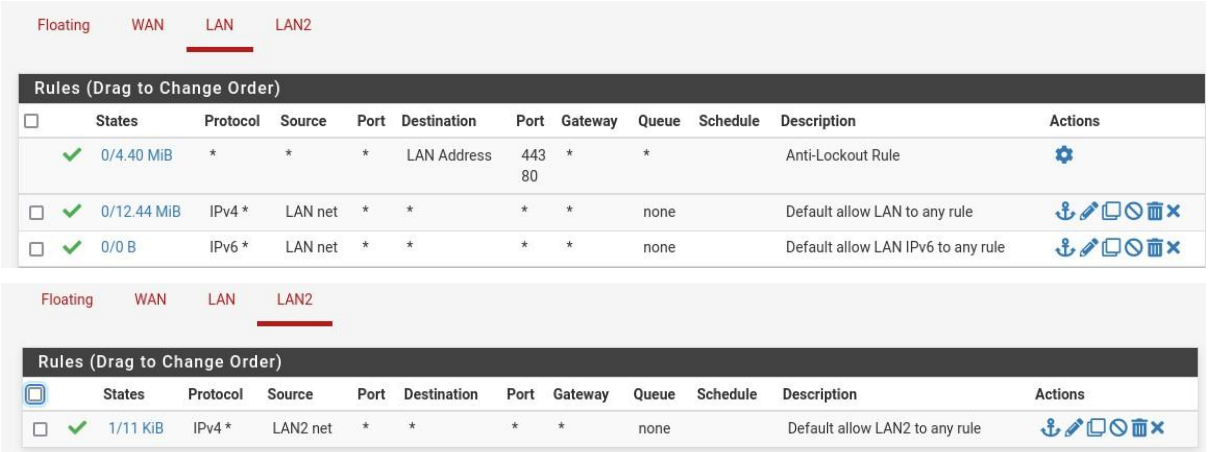
Obiettivo:

Date due macchine appartenenti a reti diverse creare una situazione iniziale dove queste riescono a comunicare secondo il modello client-server.Successivamente impedire al client(Linux) di raggiungera la DVWA sul server(metasploitable) impostando le rules sul firewall pfsense.

Procedimento:

Quindi dopo aver configurato tre schede di rete sul firewall(Nat, Lan1, Lan2) ho impostato la macchina Linux sulla rete della Lan1 (ip network: 192.168.50.0) e la metasploitable sulla Lan2(ip network:192.168.32.0).

Successivamente ho configurato le rules nel firewall per la LAN1 e LAN2 in modo che potessero comunicare come di seguito:



Floating WAN LAN LAN2

Rules (Drag to Change Order)

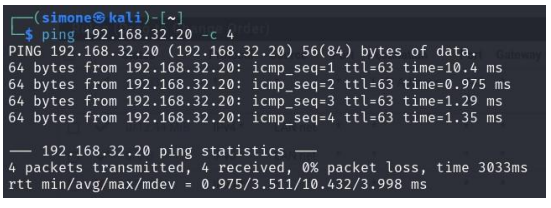
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0/4.40 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✓	0/12.44 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓	0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Floating WAN LAN LAN2

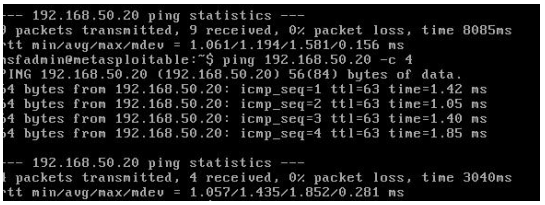
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	1/11 KiB	IPv4 *	LAN2 net	*	*	*	*	none		Default allow LAN2 to any rule	

Test ping delle due macchine Linux(ip:192.168.50.20) e Metasploitable(ip:192.168.32.20)

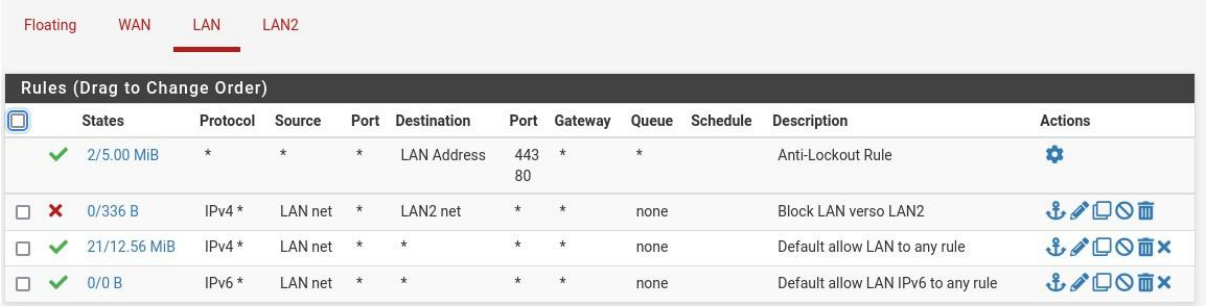


```
┌──(simone㉿kali)-[~]
└─$ ping 192.168.32.20 -c 4
PING 192.168.32.20 (192.168.32.20) 56(84) bytes of data.
64 bytes from 192.168.32.20: icmp_seq=1 ttl=63 time=10.4 ms
64 bytes from 192.168.32.20: icmp_seq=2 ttl=63 time=0.975 ms
64 bytes from 192.168.32.20: icmp_seq=3 ttl=63 time=1.29 ms
64 bytes from 192.168.32.20: icmp_seq=4 ttl=63 time=1.35 ms

── 192.168.32.20 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3033ms
rtt min/avg/max/mdev = 0.975/3.511/10.432/3.998 ms
```



```
-- 192.168.50.20 ping statistics ---
packets transmitted, 9 received, 0% packet loss, time 8085ms
tt min/avg/max/mdev = 1.061/1.194/1.581/0.156 ms
sfadmin@metasploitable:~$ ping 192.168.50.20 -c 4
ING 192.168.50.20 (192.168.50.20) 56(84) bytes of data.
4 bytes from 192.168.50.20: icmp_seq=1 ttl=63 time=1.42 ms
4 bytes from 192.168.50.20: icmp_seq=2 ttl=63 time=1.05 ms
4 bytes from 192.168.50.20: icmp_seq=3 ttl=63 time=1.40 ms
4 bytes from 192.168.50.20: icmp_seq=4 ttl=63 time=1.85 ms

-- 192.168.50.20 ping statistics ---
packets transmitted, 4 received, 0% packet loss, time 3040ms
tt min/avg/max/mdev = 1.057/1.435/1.852/0.281 ms
```

Infine ho impostato una rule per impedire ai dispositivi della LAN1 di raggiungere i servizi della Metasploitable della LAN2.



Fine.