

EPICODE-CS0124

S5/L1 - Pratica

Flaviano Sedici

Pratica

- Installazione VM pfsense
- Configurare la rete tra Kali Linux, pfsense e Metasploitable 2 in modo che Kali linux e Metasploitable 2 siano su due VLAN separata e pfsense agisca da Firewall/Router/Gateway
- Creare una regola per il firewall in modo che Kali Linux non possa raggiungere la webapp DVWA su Metasploitable 2

1. Configurazione rete

Su UTM le due VM (Kali e Metasploitable) sono state configurate con una sola interfaccia di rete ciascuna entrambe impostate su **host only**.

Pfsense è stato installato e configurato come VM con 3 schede di rete, due **host only** e una **bridge (advanced)**.

La prima scheda di rete **host only** è stata configurata con l'indirizzo statico **192.168.50.10** e soprannominata **LAN**.

La seconda scheda di rete **host only** è stata configurata con l'indirizzo statico **192.168.60.10** e soprannominata **LANMETA**.

La scheda con **bridge (advanced)** è stata impostata su **dhcp** e alla rete **WAN** consentendo l'accesso ad internet.

Current date/time	Mon Feb 19 14:48:40 CET 2024
DNS server(s)	<ul style="list-style-type: none">• 127.0.0.1• 192.168.1.1• 8.8.8.8• 8.8.4.4
Last config change	Mon Feb 19 14:36:28 CET 2024

Interfaces			
WAN	↑	1000baseT <full-duplex>	192.168.1.17
LAN	↑	1000baseT <full-duplex>	192.168.50.10
LANMETA	↑	1000baseT <full-duplex>	192.168.60.10

L'indirizzo IP statico di **Metasploitable** è stato impostato in modalità statica con **192.168.60.101**.

L'indirizzo IP statico di **Kali Linux** è stato impostato in modalità statica con **192.168.50.100**.

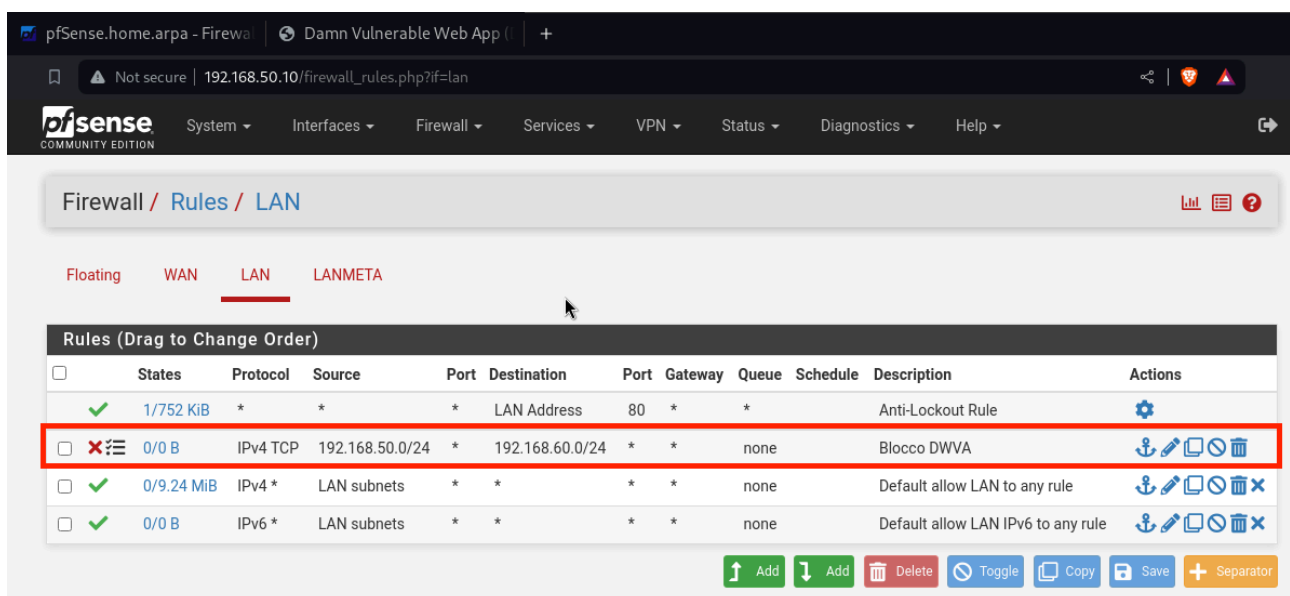


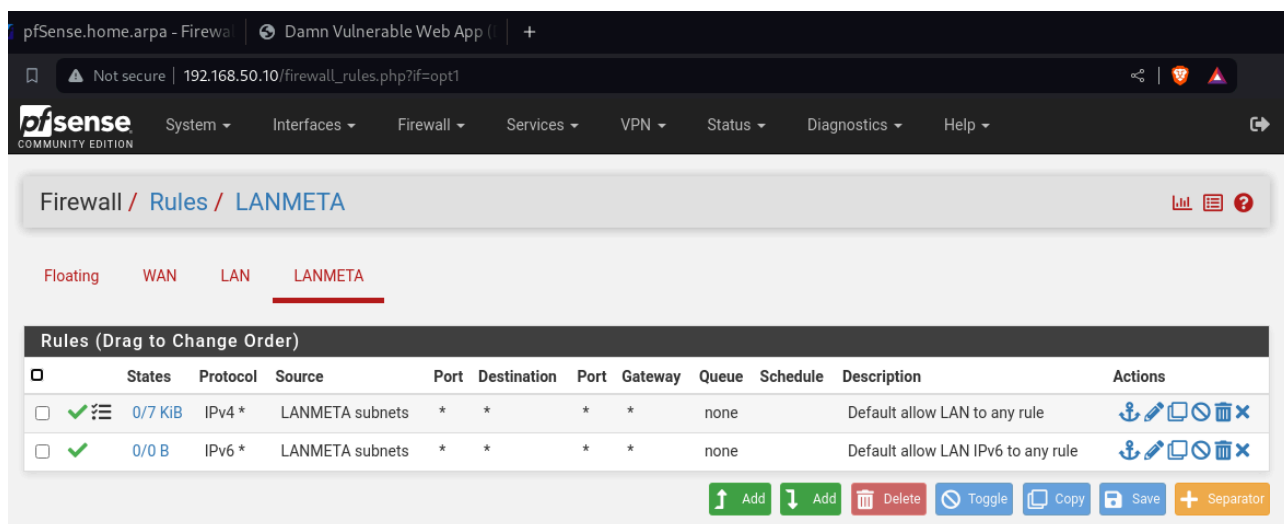
2. Configurazione Pfsense Firewall

Tramite l'interfaccia web di pfsense è stata configurata una regole per il traffico in uscita dalla LAN 192.168.50.0/24 in modo che non possa comunicare tramite protocollo TCP con la LAN 192.168.60.0/24.

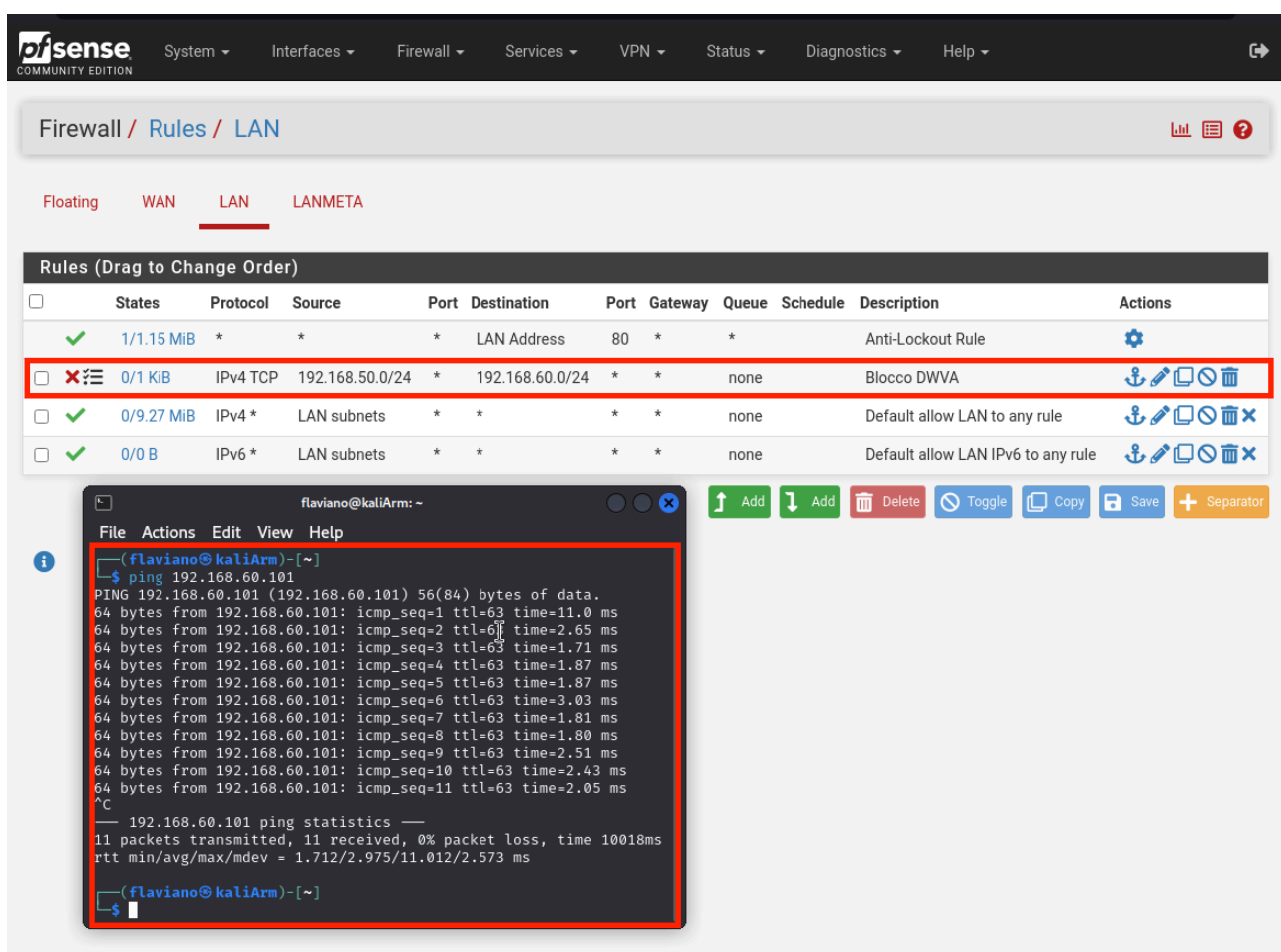
La macchina Metasploitable non è esposta su internet, infatti non è stata configurata alcuna regola per il traffico in entrata dalla WAN sulla LANMETA e di conseguenza il firewall blocca le comunicazioni in ingresso sulla LAN META.

Per questo motivo si è scelto di bloccare semplicemente il traffico dalla LAN (dove risiede Kali Linux) alla LANMETA per evitare che le macchine presenti sulla LAN possano interagire con DVWA, non avendo altre vie di accesso.



































































Come si evince dalle immagini precedenti e dalla successiva, avendo impostato il blocco solo sul protocollo TCP, la funzione ping ad esempio non ha problemi a raggiungere Metasploitable da Kali Linux.



Contrariamente, osservando i log del firewall è possibile notare come la connessione sulla porta 80 della VM Metasploitable in uscita dalla LAN di Kali Linux.

✗	Feb 19 14:38:29	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39714	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:30	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39724	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:31	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39714	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:31	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39724	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:32	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39714	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:32	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39724	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:33	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39714	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:33	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39724	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:34	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39714	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:34	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39724	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:35	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39714	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:35	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39724	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:37	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39714	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:37	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39724	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:41	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39724	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:41	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39714	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:43	WAN	Default deny rule IPv4 (1000000103)	 192.168.1.1	 224.0.0.1	IGMP
✗	Feb 19 14:38:49	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39724	 192.168.60.101:80	TCP:S
✗	Feb 19 14:38:49	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39714	 192.168.60.101:80	TCP:S
✗	Feb 19 14:39:05	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39724	 192.168.60.101:80	TCP:S
✗	Feb 19 14:39:05	LAN	 Blocco DWVA (1708341549)	 192.168.50.100:39714	 192.168.60.101:80	TCP:S