

# 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 separate e pfsense agisca da Firewall/Router
- 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.

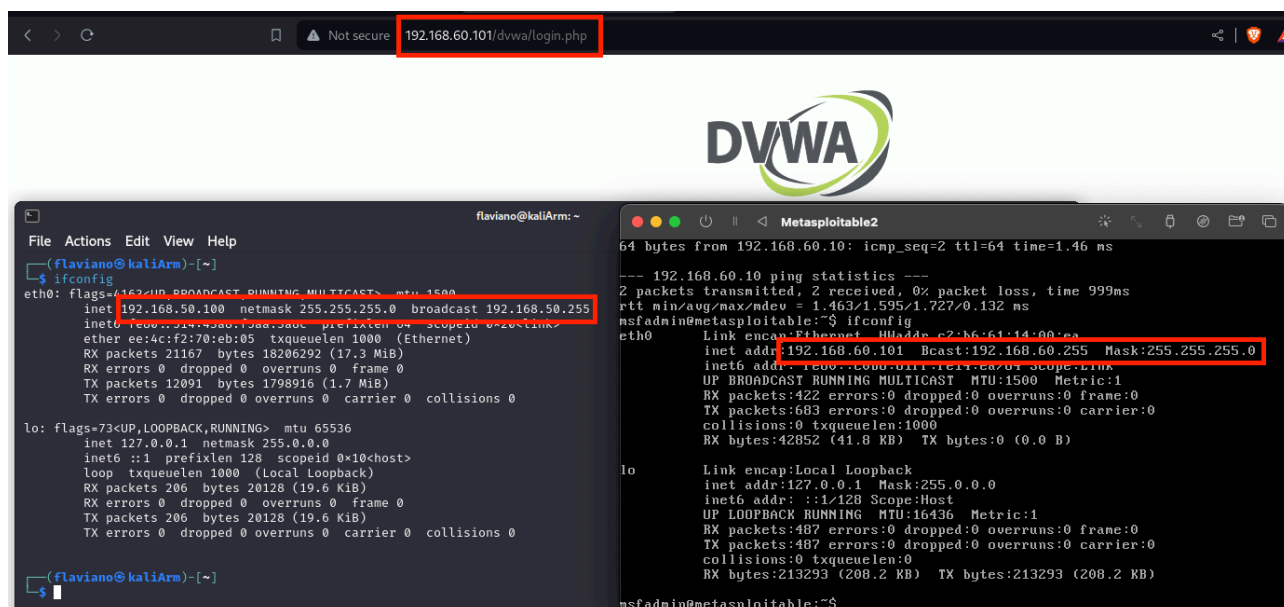
Current date/time	Mon Feb 19 14:48:40 CET 2024
DNS server(s)	<ul style="list-style-type: none"><li>• 127.0.0.1</li><li>• 192.168.1.1</li><li>• 8.8.8.8</li><li>• 8.8.4.4</li></ul>
Last config change	Mon Feb 19 14:36:28 CET 2024

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 regola per il traffico in uscita dalla VM di Kali (192.168.50.100) in modo che non possa comunicare tramite protocollo TCP con la VM di DVWA (192.168.60.101) sulla porta 80.

Floating WAN LAN LANMETA

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1/402 KIB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	192.168.50.100	*	192.168.60.101	80 (HTTP)	*	none		Blocco DVWA	
<input type="checkbox"/>	✓ 1/673 KIB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

↑ Add ↓ Add Delete Toggle Copy Save Separator

Floating WAN LAN LANMETA

Rules (Drag to Change Order)

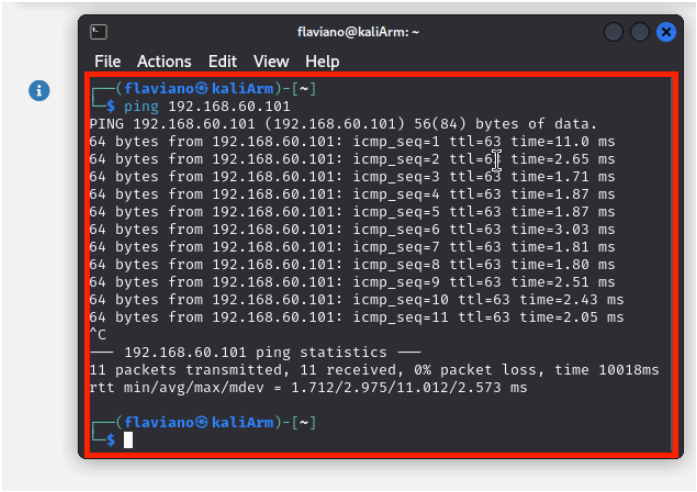
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/7 KIB	IPv4 *	LANMETA subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LANMETA subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

↑ Add ↓ Add Delete Toggle Copy Save Separator

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 LANMETA.

Per questo motivo si è scelto di bloccare semplicemente il traffico diretto tra le due VM.

Come si evince dalle immagini precedenti e dalla successiva, avendo impostato il blocco solo sul protocollo TCP e la porta 80, 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 14:38:32	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