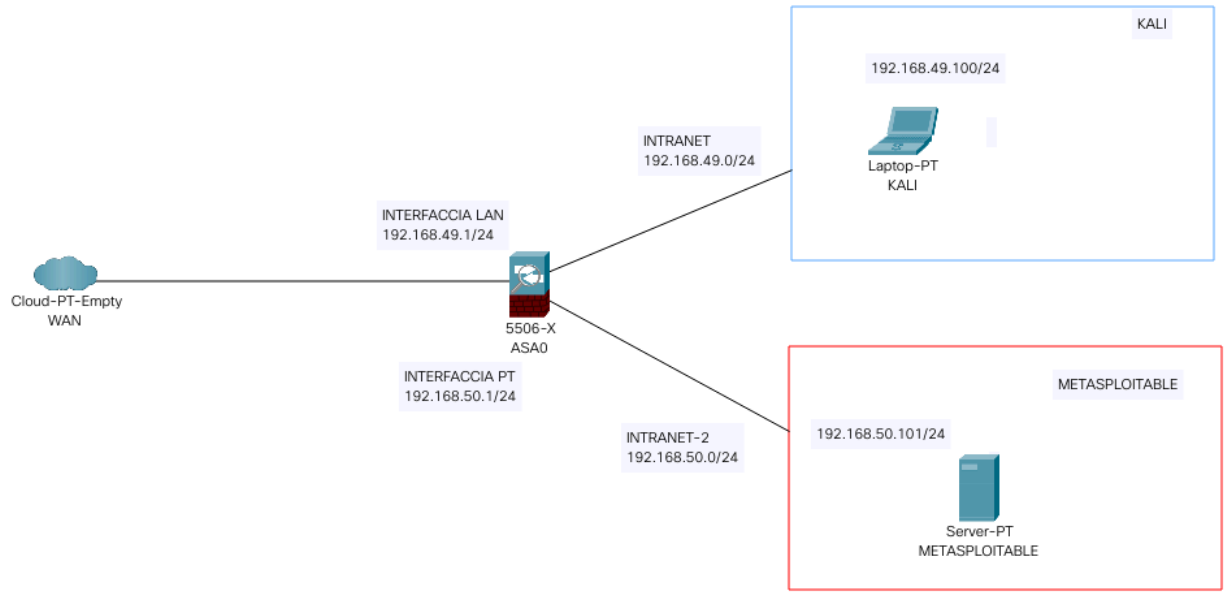
ESERCIZIO S5L1

Traccia: Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete.
Pfsense è una distribuzione basata su FreeBSD ottimizzata per essere utilizzata come firewall.

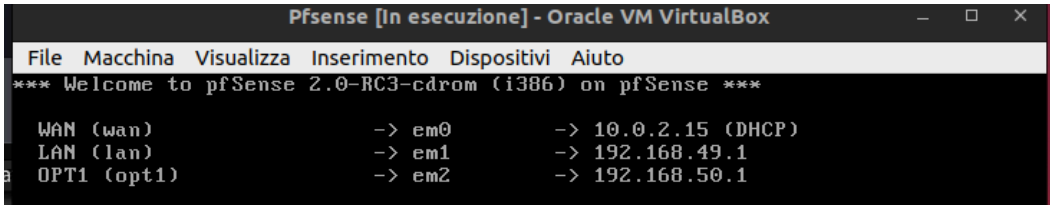
IMPOSTAZIONI AMBIENTE



Inizialmente Pfsense è stata creata sulla macchina virtuale settando 3 schede di rete diverse:

- NAT (interfaccia WAN)
- Rete interna (intnet) (interfaccia LAN)
- Rete interna (pfsense)

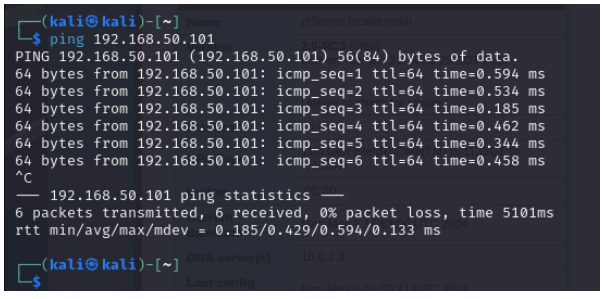
La terza scheda di rete è stata creata per aggiungere una nuova interfaccia di rete a Pfsense in modo tale da avere pfsense e metasploitable su una stessa sottorete che chiamiamo "pfsense".
OBJ

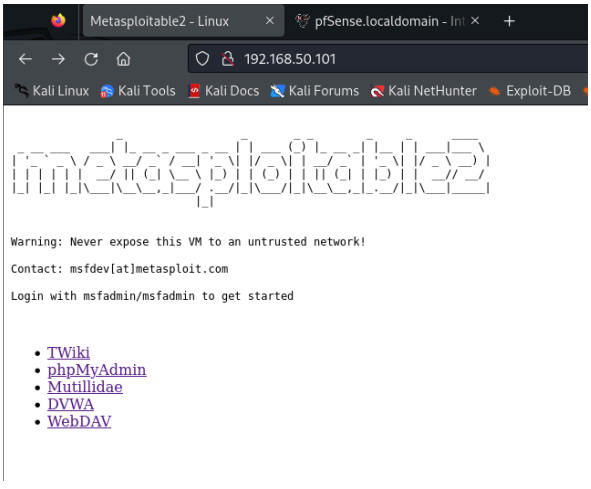


Successivamente si è abilitato il servizio dhcp sull'interfaccia appena creata e sono state modificate le impostazioni di rete di Metasploitable in modo da non utilizzare la configurazione di rete statica, ma quella "dhcp".

TEST FUNZIONAMENTO

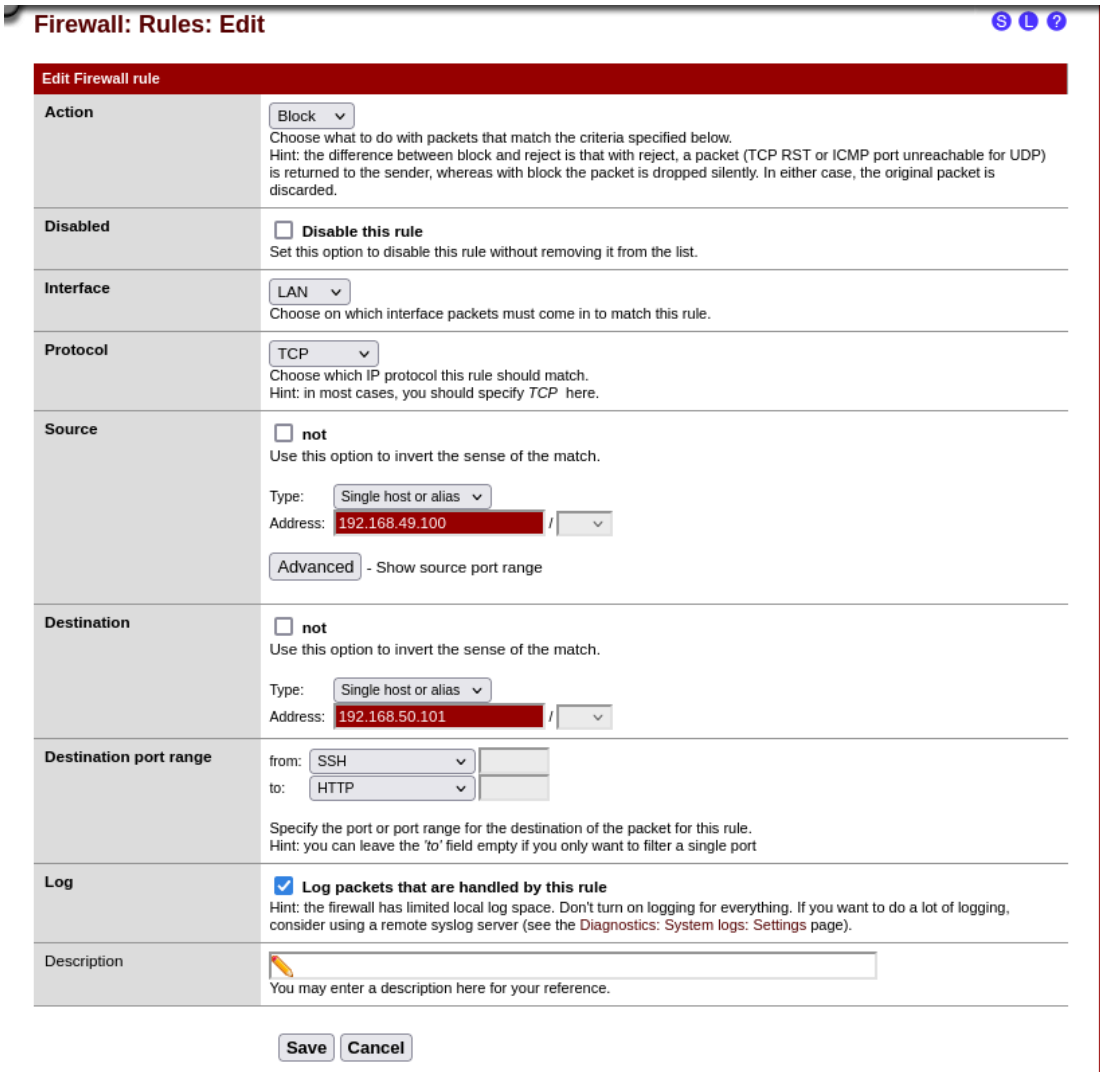
Dopo aver settato l'ambiente, si verifica che ci sia connettività tra Kali e Meta, attraverso sia un ping verso Meta (figura a sinistra), che attraverso la DVWA (immagine a destra).





CREAZIONE FIREWALL RULE

Ora, attraverso il sito di Pfsense, si va a creare la regola per bloccare il traffico tra Kali e Meta, in particolare si è bloccato il traffico dalla porta 22 (SSH) alla porta 80 (HTTP). In questo modo si rende inaccessibile la DVWA da Kali.



Qui di seguito è mostrato uno screen che mostra la regola appena creata, attiva.

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	*	*	LAN Address	22 80	*	*		Anti-Lockout Rule
		*	LAN net	*	*	*	*	none		Default allow LAN to any rule
		TCP	192.168.49.100	*	192.168.50.101	22 - 80	*	none		

pass
pass (disabled)
block
block (disabled)
reject
reject (disabled)
log
log (disabled)

Ora se si prova a raggiungere nuovamente la DVWA, si nota che questa è inaccessibile. In particolare si noti come la risposta del server non sia legata ad un errore 404, ma proprio ad una mancata risposta. Questo comportamento di mancata risposta indica che il firewall Pfsense sia riuscito a bloccare le richieste.