REPORT 21/11/2022

FACCILONGO DOMENICO

PENETRATION TESTING

TASK

- Dopo aver configurato Kali, Metaspoitable e Pfsense, tra cui, le prime due in rete Interna e l'ultima abilitando altre due reti aggiuntive, dobbiamo permettere che le tre macchina possano pingarsi tra di loro (dimostrazione successivamente). Pertanto è necessario che le macchine Kali e Metaspoitable siano su reti diverse.
- Creare una regola Firewall che non consenta l'accesso alla DVWA da Kali e ne impedisca lo scan.

ANALISI E VALUTAZIONI:

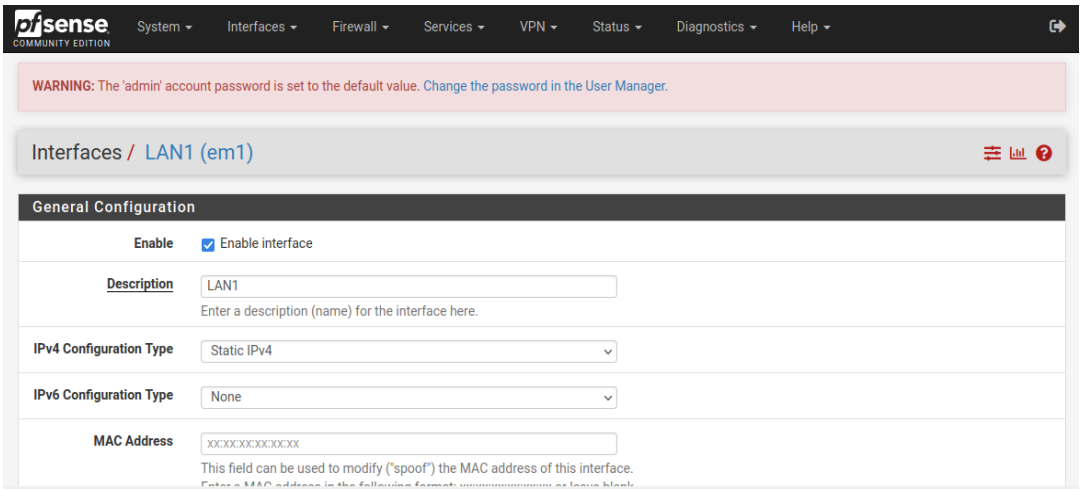
Per prima cosa andiamo a configurare kali e metaspoitable con due reti differenti, rispettivamente con questi indirizzi:

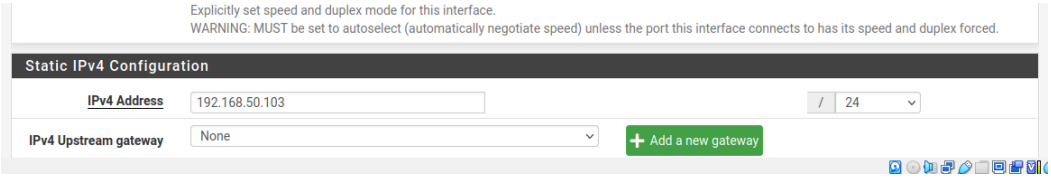
MACCHINA	INDIRIZZO IP ADDRESS	RETE
Kali	192.168.50.100	Rete 1 (LAN1)
Metaspoitable	192.168.90.101	Rete 2 (LAN2)
Pfsense	192.168.50.103	NAT, Rete 1 (LAN1), Rete 2 (LAN2)

Per entrare nel sito di pfsense da kali dobbiamo inserire l'indirizzo ipv4 per la macchina e per farlo basta inserire nel terminale di pfsense il tasto "1" per la modifica dell'indirizzo e inseriamo rispettivamente solo per l'indirizzo Ipv4 192.168.50.103.

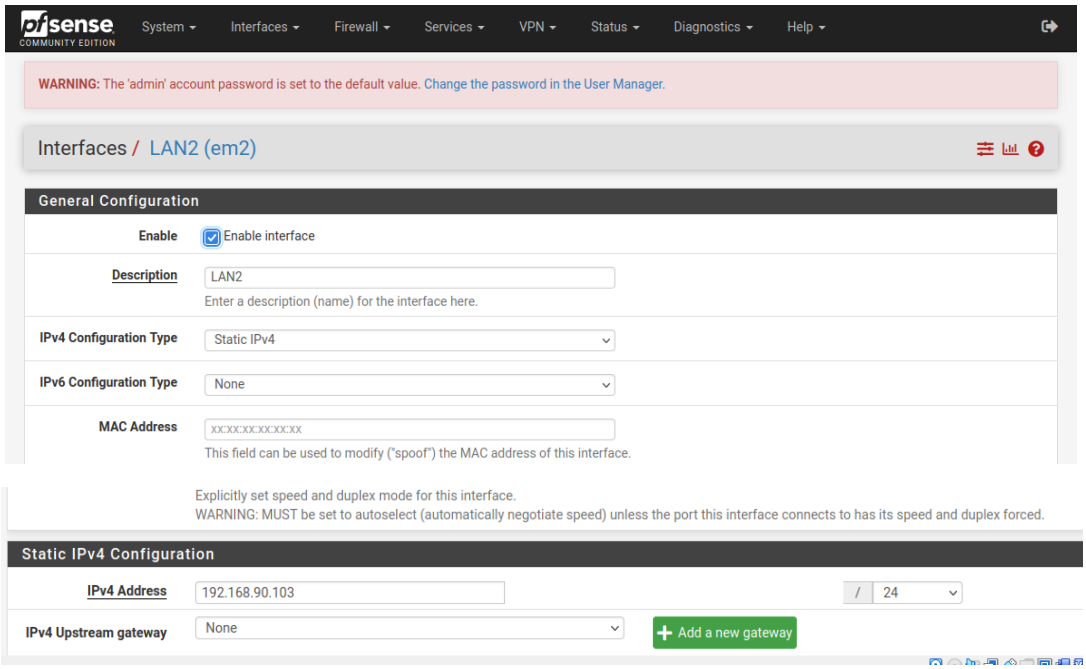
Successivamente possiamo andare ad impostare una nuova rete per pfsense e per farlo entriamo nel sito da Kali utilizzando il suo indirizzo IP impostato. La nuova rete servirà per poter collegare rispettivamente le due macchine Kali e Metaspoitable, di fatti la configurazione per la LAN1 e la LAN2 (rete che creeremo clicclando su ADD da "Interfacess → Assignment") sarà rispettivamente questa:

- LAN1

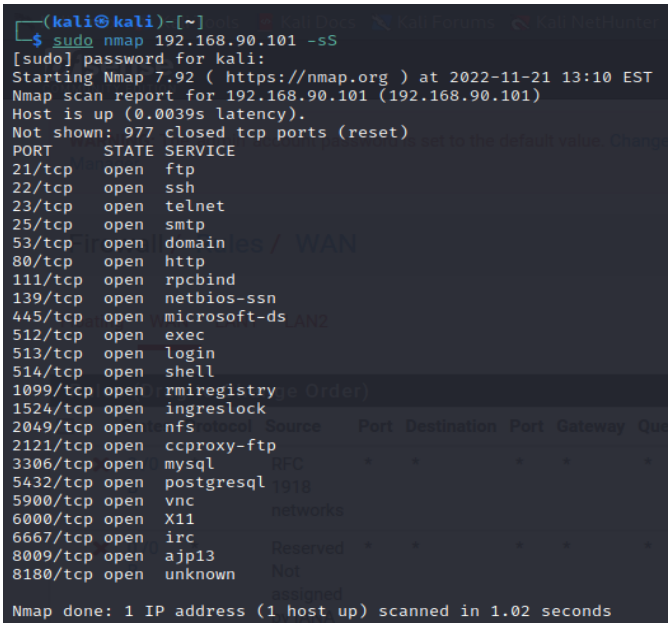




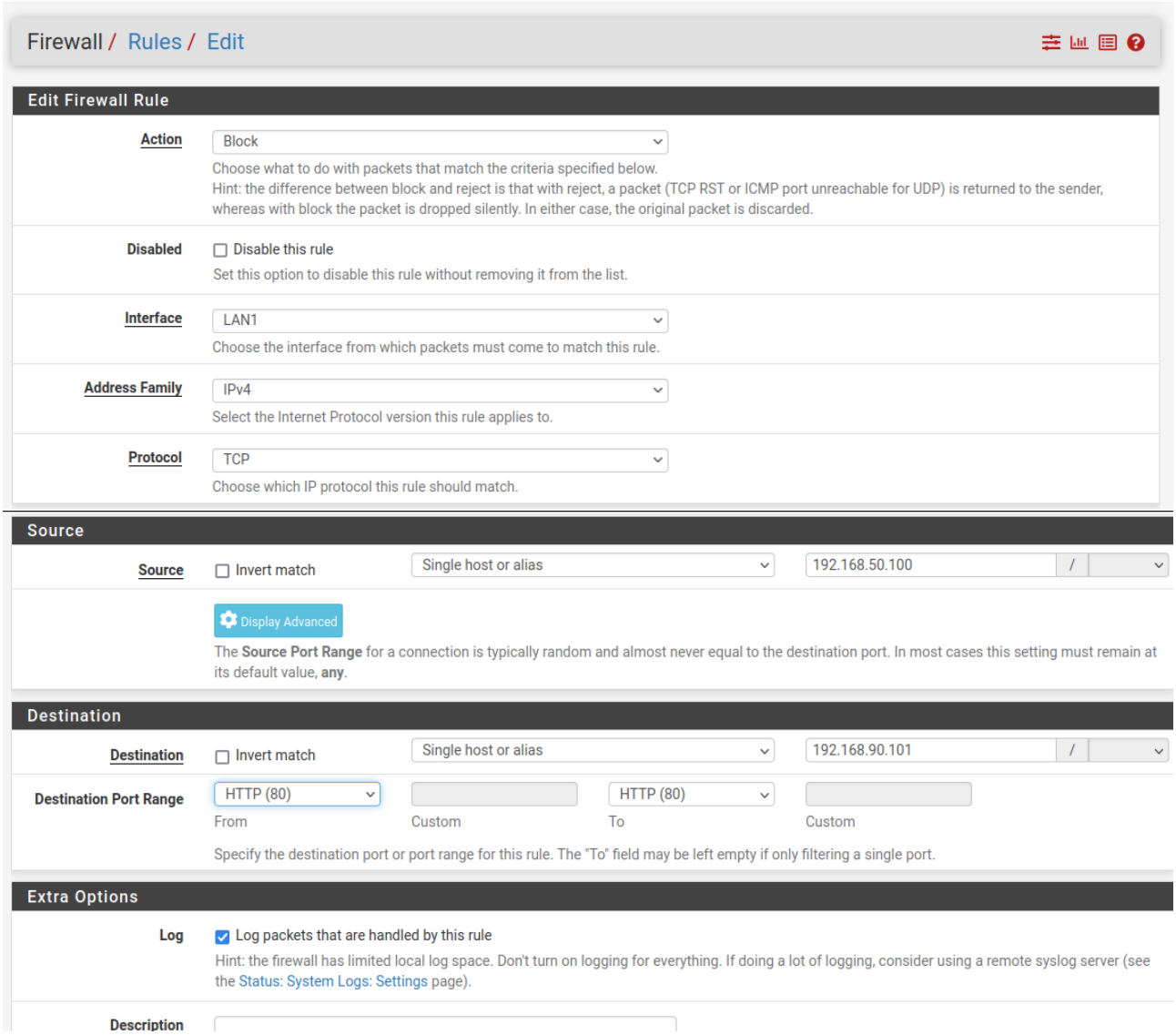
- LAN2



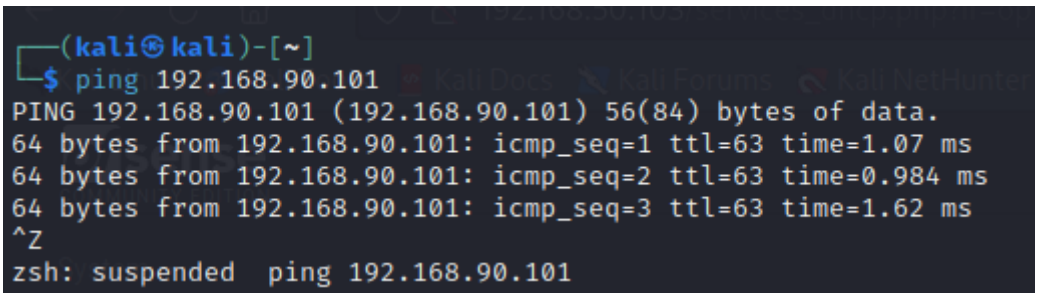
Dopo di che facciamo un scansione di DVWA con nmap -sS e andiamo a vedere le porte aperte sull'indirizzo IP target. Il risultato sarà pressocchè questo:



Il risultato che dovremmo ottenere dal firewall che andremo a creare sarà il filtraggio sulla porta 80. Per la creazione del firewall basterà entrare sempre su pfsense e andare su “Firewall”:



Così facendo andiamo a fare nuovamente un test per vedere se le macchine Kali e Metaspoitable continuano a pingarsi tra loro:



Il ping funziona e di conseguenza il firewall però blocca l'accesso al sito dvwa e ora andando a testare la scansione, il firewall và a filtrare i pacchetti della porta 80 di cui abbiamo inserito: