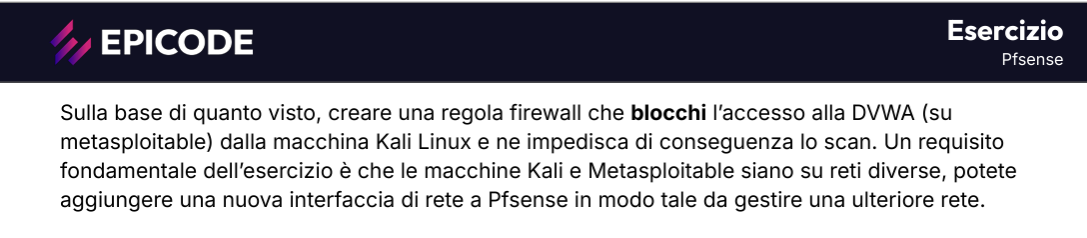
**Esame S3L5**

**Marco Falchi**

**Consegna:**



**Considerazioni pre esercizio:**

La consegna dell’esercizio si presenta per me di difficile comprensione inizialmente ma con un po' di logica capisco cosa devo fare e mi accorgo subito che ho bisogno di informarmi usando le slide per ricordare alcuni comandi passati all’interno della metaspoitable e che sarà una prova abbastanza complessa a livello logico.

**Report tecnico**

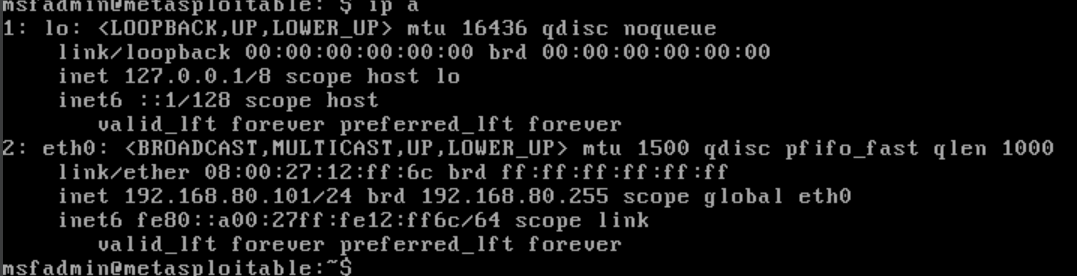
L'obiettivo primario di questa attività era la configurazione di una regola firewall su un sistema pfSense per gestire e filtrare il traffico di rete in un ambiente controllato. Nello specifico, si intendeva bloccare l'accesso da una macchina Kali Linux al servizio web DVWA (Damn Vulnerable Web Application), ospitato su una macchina virtuale Metasploitable2.

**Prerequisiti**

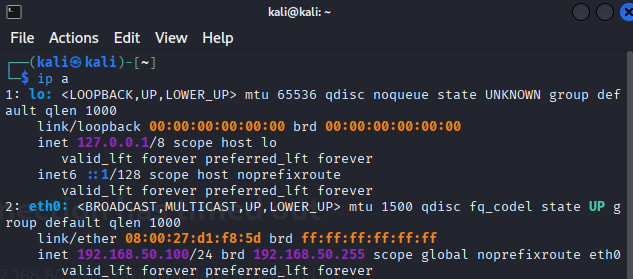
Per soddisfare i requisiti, le due macchine virtuali sono state configurate su due sottoreti separate:

* Macchina Kali Linux: configurata con l'indirizzo IP statico 192.168.50.100/24.

Macchina Metasploitable2: configurata con indirizzo IP statico 192.168.80.101/24 e gateway 192.168.80.1





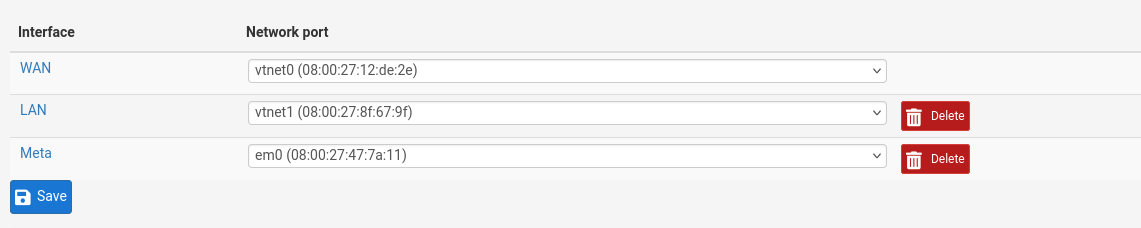
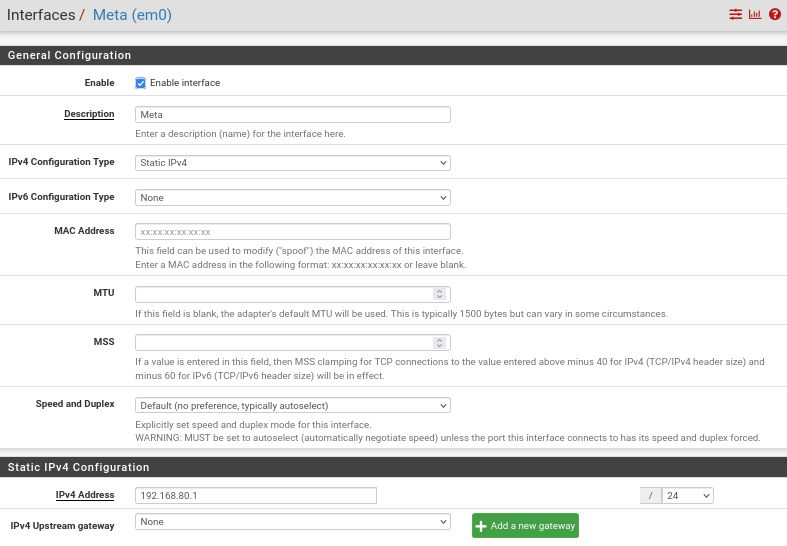


**Configurazione interfaccia**

È stata creata una nuova interfaccia su pfSense, denominata "Meta", per gestire il traffico della rete dedicata alla macchina Metasploitable2.

L'interfaccia è stata poi abilitata e configurata con i seguenti parametri:

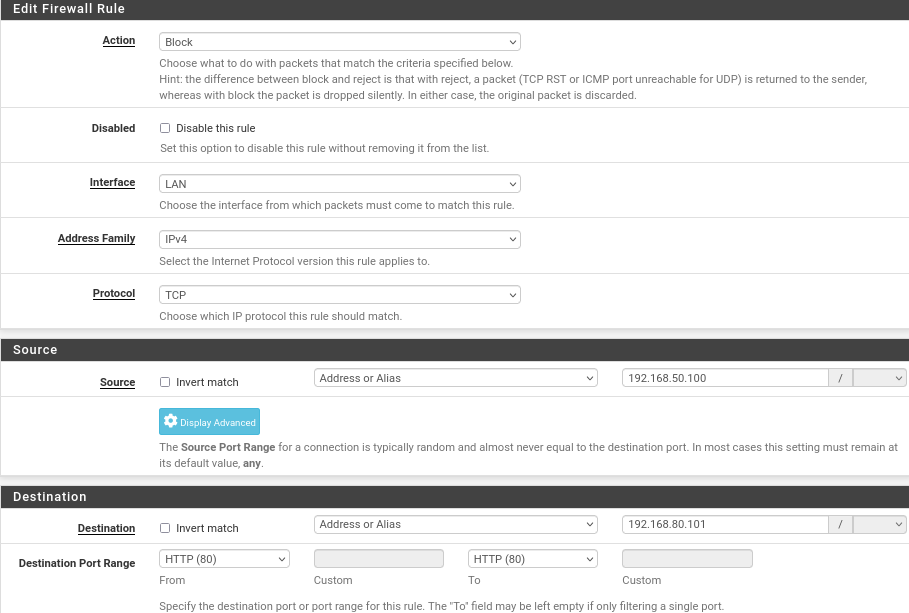
* Descrizione: Meta
* Tipo di Configurazione IPv4: Static IPv4
* Indirizzo IPv4: 192.168.80.1 con una subnet mask di /24



**Creazione della Regola Firewall**

Successivamente, è stata definita una regola sul firewall per implementare il blocco del traffico desiderato. La regola è stata configurata come segue:

* **Action:** Block. Questa azione scarta i pacchetti in modo silente, senza inviare una risposta al mittente.
* **Interface:** LAN. La regola si applica al traffico in ingresso dall'interfaccia LAN, dove è connessa la macchina Kali Linux.
* **Address Family:** IPv4
* **Protocol:** TCP
* **Source:** 192.168.50.100 (Indirizzo IP della macchina Kali Linux)
* **Destination:** 192.168.80.101 (Indirizzo IP della macchina Metasploitable)
* **Destination Port Range:** HTTP (porta 80)

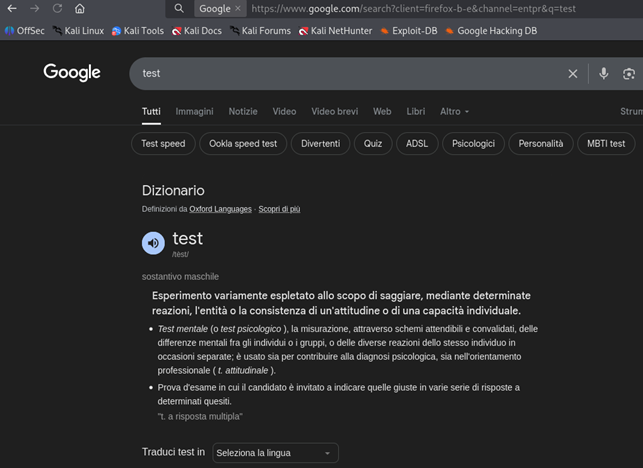


**Test e Verifica dei Risultati**

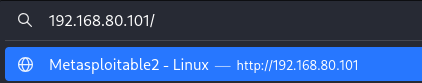
Per validare l'efficacia della configurazione, sono stati eseguiti dei test di connettività dalla macchina Kali Linux.

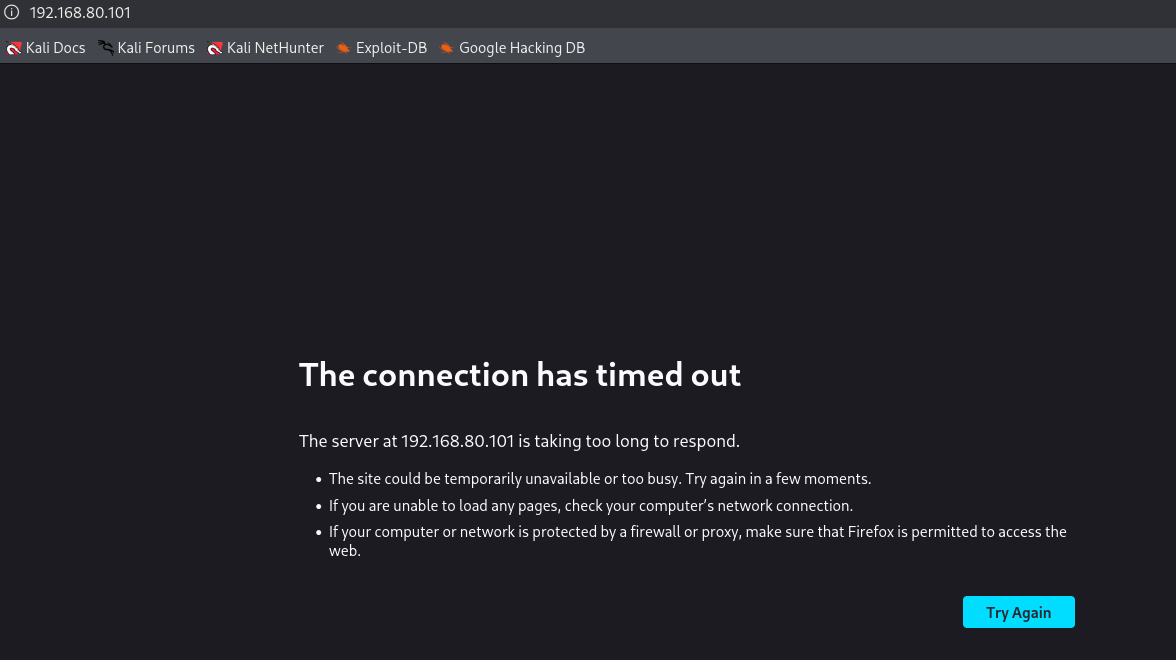
**Navigazione su siti web con porta non controllata dal firewall:** La navigazione verso siti esterni che utilizzano il protocollo HTTPS (porta 443), come Google, ha funzionato correttamente.

Questo dimostra che la regola non ha interrotto la connettività generale della macchina ai siti con porte https 443.

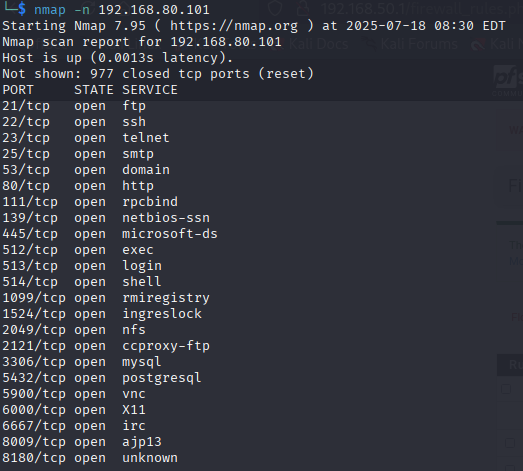


**Navigazione su siti web con porta controllata dal firewall:** Il tentativo di accesso via browser all'indirizzo http://192.168.80.101 è fallito, generando un errore di "The connection has timed out". Questo risultato è coerente con l'azione "Block" della regola firewall, che scarta i pacchetti senza notificare il client, causando un timeout della richiesta



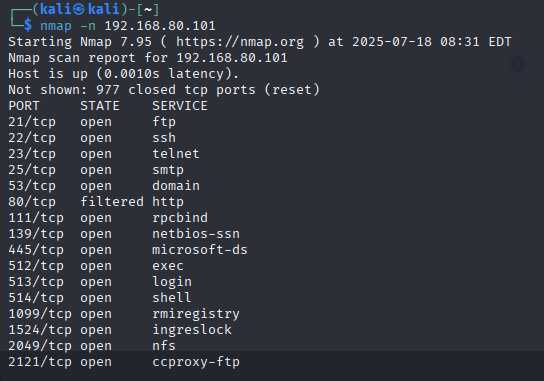


**Test scansione porte senza firewall**

**e**

Al fine di verificare lo stato di connettività iniziale, ho proceduto con una scansione delle porte da Kali Linux verso metaspoitable2. Questa operazione è stata eseguita con la regola di filtraggio del firewall temporaneamente disattivata, ha confermato quindi che le porte di servizio erano tutte aperte.

**Test scansione con firewall**



Ho successivamente proceduto con una scansione delle porte da Kali Linux verso metaspoitable2 ma questa volta con le regole di filtraggio firewall attive, ha confermato quindi che le porte di servizio erano tutte aperte tranne quella bloccata dal nostro firewall che è quindi filtrata.

**Conclusione**

I test effettuati confermano il successo della configurazione. La regola firewall implementata su pfSense blocca efficacemente il traffico sulla porta 80 (HTTP) proveniente dalla macchina Kali Linux e diretto alla macchina Metasploitable2, come richiesto dall'obiettivo. L'accesso al servizio DVWA è stato quindi inibito, mantenendo al contempo la connettività per altri servizi di rete. L'obiettivo dell'esercizio è stato pienamente raggiunto.

**Considerazioni post esercizio:**

Alla fine dell’esercitazione sono totalmente conscio di ciò che ho fatto e sicuro del mio esercizio, è stata una sfida nella parte iniziale capire come configurare tutto, ho invece trovato facile e logico configurare il firewall, ho avuto diversi problemi durante l’esercitazione ma si trattava sempre di piccoli problemi che ho poi risolto dopo poco con la logica.