Traccia

Creare una regola firewall che blocchi l'accesso alla DVWA (su Metasploitable) dalla macchina Kali Linux. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse.

Svolgimento

Per poter svolgere questo esercizio, è necessario che le tre macchine virtuali (Kali, Meta e PfSense) siano configurate nel modo corretto.

Kali Linux:

- Da VirtualBox, impostare la scheda di rete su 'Rete interna', nome della rete 'intnet';
- Impostare come indirizzo IP della macchina '192.168.50.100' e gateway '192.168.50.1'.

Metasploitable:

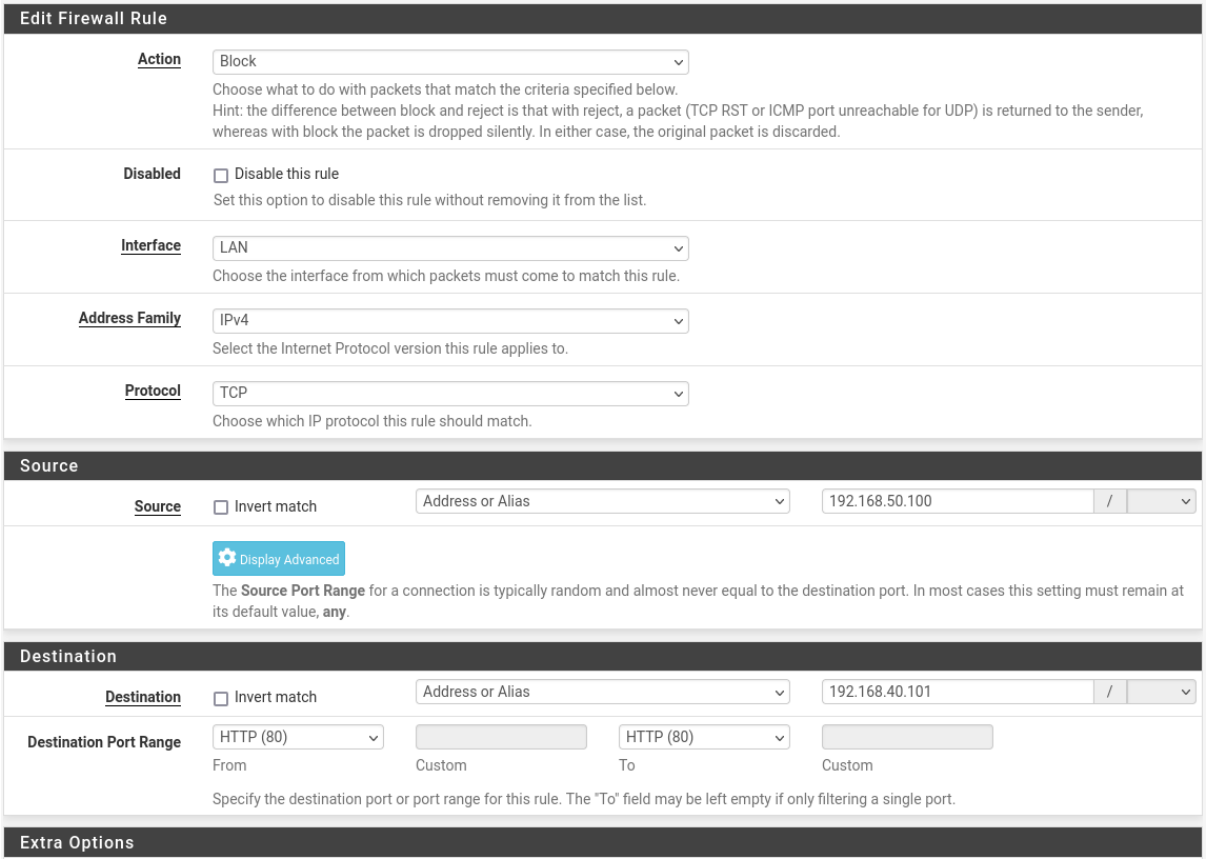
- Da VirtualBox, impostare la scheda di rete su 'Rete interna', nome della rete 'intnet2';
- Impostare come indirizzo IP della macchina '192.168.40.101' e gateway '192.168.40.1'.

PfSense:

- Da VirtualBox, impostare 3 schede di rete. La prima su 'NAT', interfaccia che serve a collegarsi su Internet. La seconda su 'Rete interna', con nome della rete 'intnet', che serve per comunicare con la rete di Kali. La terza su 'Rete interna', con nome della rete 'intnet2', che serve a comunicare con la rete di Meta;
- La prima interfaccia di rete, è configurata di default in DHCP, lasciare questa impostazione;
- La seconda, è configurata di default con l'indirizzo '192.168.1.1', impostare l'indirizzo con '192.168.50.1', per poter accedere all'interfaccia web di PfSense da Kali.
- Una volta aver fatto l'accesso alla WUI con le credenziali 'admin-pfsense', abilitare la terza interfaccia di rete, accenderla ed assegnarle l'indirizzo '192.168.40.1'.

Dopo aver seguito i passaggi sopraindicati, da Kali, è possibile eseguire il ping verso Meta. Inoltre, è possibile accedere alla pagina web di DVWA.

Ora non resta che creare la regola che ci permetta di bloccare tutte le richieste HTTP, provenienti dalla macchina di Kali, verso la macchina di Meta. Questa regola, deve essere creata per l'interfaccia 'LAN' , perchè, per come è configurato il firewall, esso esegue prima le regole di questa interfaccia, poi quelle dell'interfaccia 'OPT1'. La regola deve essere configurata come nella figura sottostante.



Come si può vedere nella figura sottostante, dopo aver configurato questa regola, dalla macchina di Kali, si potrà ancora eseguire il ping verso Meta, ma non sarà più possibile accedere alla pagina web di DVWA.