Relazione PROGETTO FIREWALL

Ho analizzato e implementato due casi di studio.

PRIMO CASO: kali e metasploitable sulla stessa rete.

Ho configurato la macchina virtuale kali con ip 192.168.50.100 netmask 255.255.255.0 e default gateway 192.168.50.1.

Ho configurato la macchina virtuale metasploitable tramite comando sudo nano /etc/network/interfaces con ip 192.168.50.101,netmask 255.255.255.0 e default gateway 192.168.50.1.

Per impedire l'accesso alla DVWA della metasploitable da parte di kali bisogna impedire il traffico http da una macchina all'altra quindi ho impostato Action in Reject, come sorgente l'indirizzo ip della kali e destinazione quello della metasploitable sulla porta 80 per bloccare il servizio http.

SECONDO CASO : kali e metasploitable su reti diverse

Ho lasciato invariata la configurazione di kali mentre ho configurato manualmente la metasploitable
con ip 192.168.60.100 , netmask 255.255.255.0 e default gateway 192.168.60.1.
Nel pannello di virtualbox ho abilitato una terza scheda di rete per la macchina Pfsense, ho cambiato il nome in metasploitable.
Lo stesso ho fatto per la scheda di rete della metasploitable impostata su Rete interna.

Ho eseguito poi l'accesso a pfsense dalla kali e ho configurato una nuova interfaccia per il router (OPT1) con indirizzo ip 192.168.60.1 tramite web gui.

A questo punto ho aggiunto una regola al firewall impostando l'action in reject , ip sorgente 192.168.50.100 e ip destinazione 192.168.60.100 bloccando il traffico http sulla porta 80 della metasploitable.