S9L3

Dagli screen di Wiresharke molto probabilmente è in corso una scansione sul target (192.168.200.150) dall’attaccante (192.168.200.100)

Consigliami di configurare delle policy firewall per bloccare l’accesso a tutte le porta da parte di quel determinato attaccante, in modo tale da evitare che le informazioni circa porta e servizi in ascolto finiscano nelle mani dell’attaccante.

Dalla cattura notiamo che ci sono un numero elevato di richieste TCP (SYN) su porte sempre diverse in destinazione questo ci fa pensare ad una potenziale SCANSIONE in corso da parte dell’host 192.168.200.100 verso l’host target 192.168.200.150.

Questa ipotesi è supportata dal fatto che per alcune righe della cattura vediamo risposte positive del target [SYN+ACK] ad indicare che la porta è aperta. Per altre, invece, notiamo la risposta [RST+ACK] sta ad indicare che la porta è chiusa (evidenziate in rosso).

