Lezione S9/L3

Rosario Giaimo

Analizzando questo file “Cattura_U3_W1_L3” sembra che qualcuno sta cercando di entrare Ecco il succo:

- Abbiamo notato un sacco di richieste di connessione ripetute (richieste TCP) provenienti da un dispositivo specifico (192.168.200.100) che punta a un altro dispositivo sulla tua rete (192.168.200.150).
- Queste richieste stanno colpendo diverse porte sul dispositivo di destinazione, un po' come bussare a ogni porta per vedere se c'è qualcuno in casa.
- A volte il dispositivo di destinazione risponde positivamente (dicendo "Sì, questa porta è aperta!"), altre volte dice "No, questa porta è chiusa!" (a seconda che la porta sia aperta o chiusa).

Questo comportamento significa che qualcuno sta scansionando la rete per trovare punti deboli.

Ecco cosa possiamo fare per fermarli:

- **Mettere un cartello digitale "Vietato l'ingresso":** Possiamo impostare delle regole del firewall per bloccare tutto il traffico proveniente dal dispositivo sospetto. In questo modo, non potrà nemmeno provare a bussare nessuna porta.
- **Rinforzare il dispositivo di destinazione:** Possiamo configurare il firewall del dispositivo di destinazione per rifiutare specificamente le richieste di connessione dal dispositivo sospetto. Come un proprietario di casa che rinforza le serrature dopo un tentativo di scasso.
- **Tenere d'occhio le cose:** Dobbiamo continuare a monitorare l'attività della tua rete per qualsiasi altro comportamento sospetto. È come avere una telecamera di sicurezza per catturare chiunque cerchi di sgattaiolare in giro.
- **Tappare i buchi:** Assicurarsi che tutto il software sul dispositivo di destinazione sia aggiornato. Questi aggiornamenti spesso correggono le vulnerabilità di sicurezza che gli aggressori potrebbero tentare di sfruttare. È come tappare eventuali crepe nei muri per rendere più difficile l'ingresso a un ladro.

Adottando queste misure, possiamo rendere molto più difficile per l'attaccante accedere alla rete e rubare i dati.