Soluzione Esercizio

Identificare eventuali IOC (Indicators of Compromise)

Evidenze di attacchi in corso:

- Richieste TCP ripetute

Ipotesi sui potenziali vettori di attacco utilizzati

In base agli IOC trovati, è possibile formulare la seguente ipotesi:

- Molto probabilmente è in corso una scansione sul target 192.168.200.150 dall'attaccante 192.168.200.100.

Consigli per ridurre gli impatti dell'attacco

Per mitigare l'attacco, si consiglia di:

- Configurare delle policy firewall per bloccare l'accesso a tutte le porte da parte dell'attaccante specifico (192.168.200.100), in modo da impedire che informazioni sulle porte e servizi in ascolto finiscano nelle mani dell'attaccante.

Analisi della cattura

Dalla cattura dei dati si osserva un numero elevato di richieste TCP (SYN) su porte sempre diverse in destinazione. Questo indica una potenziale scansione in corso da parte dell'host 192.168.200.100 verso l'host target 192.168.200.150.

L'ipotesi è supportata dai seguenti elementi:

- Alcune righe della cattura mostrano risposte positive del target ([SYN+ACK]), indicando che la porta è aperta.
- Altre righe mostrano la risposta ([RST+ACK]), indicando che la porta è chiusa.

Azioni consigliate lato target

Per proteggere il target, si potrebbe:

- Configurare delle regole firewall per respingere le richieste in entrata dall'host 192.168.200.100.