Esercizio S9 L3

Nella cattura di rete fornita possiamo notare multiple richieste TCP su ampi intervalli di porte. Da ciò possiamo supporre sia stato effettuato un port scanning con un tool che potrebbe essere Nmap o qualcosa di similare.

Identificazione IOC:

1. Indirizzi IP sospetti: 192.168.200.100
2. Porte coinvolte: 1-1024

Ipotesi sui Vettori di Attacco:

1. Scanning per la ricerca di vulnerabilità:
    - L'attaccante potrebbe eseguire il port scanning per individuare porte aperte e identificare vulnerabilità potenziali nei servizi in esecuzione su tali porte.
2. Preparazione per un attacco futuro:
    - Il port scanning può essere un passo preliminare per preparare un attacco più mirato. L'attaccante potrebbe cercare di mappare la topologia della rete per identificare obiettivi potenziali.

Azioni Consigliate:

1. Isolamento delle Porte:
    - Isolare le porte coinvolte nell'attacco. Ciò può impedire che l'attaccante prosegua con ulteriori fasi dell'attacco.
2. Regolamenti Firewall:
    - Aggiornare le regole del firewall per limitare l'accesso non autorizzato e per rilevare attività di scanning ricorrente.
3. Monitoraggio Attivo:
    - Implementare un monitoraggio attivo per rilevare e rispondere tempestivamente a ulteriori attività di scanning o tentativi di intrusione.
4. Aggiornamento dei Sistemi:
    - Assicurarsi che tutti i sistemi siano aggiornati con le ultime patch di sicurezza per ridurre il rischio di sfruttamento di eventuali vulnerabilità scoperte.
5. Formazione e Sensibilizzazione:
    - Fornire formazione al personale su pratiche di sicurezza informatica per ridurre la probabilità di cadere vittima di attacchi futuri.