**Consegna 11 Ottobre**

Analizzando con wireshark ho notato che l’IP sorgente effettua connessioni verso porte TCP su una macchina presente sulla stessa rete. Tutta via l’IP sorgente tronca la connessione appena riceve una risposta dal server il che fa pensare ad un SYN Scan (Half-Open Scan).

Il SYN Scan (Half-Open Scan) è una tecnica di scansione delle porte che sfrutta il meccanismo di handshake del protocollo TCP. Invece di stabilire una connessione completa (completando il three-way handshake), l'attaquer invia un pacchetto SYN per avviare la connessione e attende la risposta del server. Se il server risponde con un pacchetto SYN-ACK, l'attaccante non completa l handshake inviando un pacchetto RST, mantenendo così la connessione "mezza aperta". Questo metodo è utile per identificare le porte aperte senza rivelare l'indirizzo IP dell'attaccante.

**Azioni Immediate**

1. **Monitoraggio dei Log**: Controlla i log del firewall e del sistema per identificare ulteriori attività sospette o tentativi di scansione.
2. **Regole del Firewall**: Aggiorna le regole del firewall per bloccare il traffico proveniente da indirizzi IP sospetti. Considera di implementare il rate limiting per ridurre il rischio di scansioni massicce.
3. **Intrusion Detection Systems (IDS)**: Implementa o aggiorna un sistema di rilevamento delle intrusioni per identificare e allertare su comportamenti anomali nel traffico di rete.
4. **Aggiornamento delle Patch**: Assicurati che tutti i sistemi siano aggiornati con le ultime patch di sicurezza per ridurre le vulnerabilità.

**Azioni Future**

1. **Formazione del Personale**: Educa il personale IT sulla sicurezza della rete e sulle tecniche di scansione comuni per aumentare la consapevolezza e la reattività.
2. **Analisi del Rischio**: Conduci un’analisi del rischio per identificare e valutare le vulnerabilità esistenti nella tua rete e nei tuoi sistemi.
3. **Penetration Testing**: Effettua regolarmente test di penetrazione per identificare potenziali vulnerabilità e migliorare la resilienza della rete.
4. **Implementazione di Honeypot**: Considera di utilizzare honeypot per rilevare e analizzare attacchi in tempo reale, ottenendo informazioni utili per migliorare la sicurezza.
5. **Rete di Difesa in Profondità**: Adotta una strategia di difesa in profondità, combinando diversi livelli di sicurezza (firewall, IDS/IPS, segmentazione della rete) per migliorare la protezione complessiva.