# Analisi di sicurezza della rete

## 1. Indicatori di Compromissione (IOC)

Sono stati individuati diversi indicatori di compromissione, tra cui:  
- Traffico TCP con flag SYN senza completamento (ACK), indicativo di scansioni di porta o attacchi DoS.  
- Comunicazioni non crittografate su Telnet (porta 23), che espongono le credenziali in chiaro.  
- Presenza di un host denominato 'METASPLOITABLE', associato a vulnerabilità intenzionali.  
- Richieste ARP sospette, potenzialmente indicanti ARP spoofing o attacchi man-in-the-middle (MITM).  
- Utilizzo di SMB (porta 445) con configurazioni potenzialmente insicure, che espongono a ransomware e furto di credenziali.  
- Pacchetti RST e ACK non correlati a flussi di traffico validi, indicativi di attività sospette o manipolazione del traffico.

## 2. Ipotesi sui vettori di attacco

Sulla base degli IOC identificati, i potenziali vettori di attacco includono:  
- Attacchi SMB o NetBIOS, sfruttando vulnerabilità per eseguire codice remoto o accedere a condivisioni di rete.  
- Spoofing ARP o attacchi MITM, mirati a intercettare o manipolare il traffico di rete.  
- Scansioni di porte per mappare i servizi attivi e individuare vulnerabilità sfruttabili.  
- Attacchi brute-force su Telnet, sfruttando credenziali deboli o predefinite.  
- Attacchi DoS tramite SYN flood, con l'obiettivo di sovraccaricare i dispositivi.

## 3. Azioni per mitigazione immediata

Le seguenti azioni sono raccomandate per mitigare gli attacchi attuali:  
- Isolare i dispositivi sospetti, in particolare 192.168.200.150 e 192.168.200.100.  
- Bloccare traffico sulle porte critiche (23, 445, 138, 443) non necessario.  
- Monitorare attivamente il traffico di rete utilizzando strumenti IDS/IPS.  
- Rimuovere o isolare l'host Metasploitable, configurandolo in una VLAN separata.  
- Disabilitare Telnet a favore di SSH e applicare patch di sicurezza ai sistemi.

## 4. Prevenzione di attacchi futuri

Per prevenire attacchi futuri, si consiglia di:  
- Disattivare servizi inutilizzati come NetBIOS e SMB non configurati in modo sicuro.  
- Implementare autenticazione avanzata e crittografia per SMB e altri servizi.  
- Segmentare la rete con VLAN per limitare la propagazione degli attacchi.  
- Eseguire controlli periodici sui log di sistema e traffico DNS per individuare anomalie.  
- Configurare firewall per filtrare il traffico broadcast e ridurre i rischi di attacchi ARP.