# Threat Intelligence & IoC

Gli indicatori di compromissione (IoC) sono segnali specifici, come determinati IP noti per essere utilizzati in attività dannose, che suggeriscono che un sistema o una rete sono stati compromessi o stanno per essere compromessi da un attacco informatico.

## Caso studio: analisi report di Wireshark

La cattura di rete fornita ritorna un'analisi tramite Wireshark di quello che sembra essere un penetration test su una macchina Metasploitable 192.168.200.150, come dichiarato dall'annuncio di broadcast sulla rete alla riga 1.

Analizzando i dati forniti, possiamo subito notare un elemento che potrebbe indicare un potenziale attacco, ossia i moltissimi tentativi di connessione attraverso svariate porte da parte dell'IP 192.168.200.100 all'IP 192.168.200.150. Numerosi tentativi di connessione su diverse porte in poco tempo possono indicare un tentativo di scansione delle porte, elemento tipico di una fase di ricognizione in cui un attaccante ricerca sulla macchina vittima servizi vulnerabili ad un attacco.

Per ridurre l'impatto di questo tipo di attacchi e prevenire future intrusioni, possono essere adottate alcune contromisure:

- Blocco dell'IP sospetto: una misura immediata potrebbe essere bloccare l'indirizzo IP sospetto per interrompere i tentativi di connessione e impedire ulteriori scanning o attacchi.

- Limitare il numero di tentativi di connessione per ogni IP: è possibile configurare il sistema in modo che dopo un dato numero di tentativi falliti l'IP sospetto venga bloccato.

- Utilizzare un sistema di rilevamento delle intrusioni come IDS/IPS: sistemi di rilevamento e prevenzione possono essere configurati per rilevare attività sospette, come scanning delle porte, e generare alert in tempo reale.

## Note

Possiamo notare dalle numerose risposte RST da 192.168.200.150 a molte delle richieste SYN di 192.168.200.100 che quest'ultimo rifiuta veri tentativi di connessione, comportamento comune in caso di porte chiuse o di presenza di firewall attivi che bloccano il traffico non autorizzato.

## Conclusioni

Dall'analisi della cattura di rete si evidenzia un possibile attacco in fase di ricognizione, con numerosi tentativi di scanning delle porte sull'indirizzo target. Bloccare l'IP dell'attaccante è una soluzione immediata per mitigare l'attacco, mentre adottare soluzioni come IDS e IPS può aiutare a prevenire simili attacchi in futuro.