Cyber Security

**THREAT INTELLIGENCE E IOC**

Analisi Scansione di rete con WireShark

linea orizzontale

# 

# Identificazione IOC di un probabile attacco

Come vediamo nello screenshot riportato sopra, possiamo visualizzare che l’Attaccante sonda diverse porte su un host per identificare vulnerabilità.

**Segnale**: Numerose richieste SYN verso porte diverse in rapida successione.

#### **Dati Rilevanti**

* **Host Sospetto:** 192.168.200.100
* **Destinazione:** 192.168.200.150
* **Tipi di Traffico:** TCP, ARP
* **Porte Analizzate:**
  + 23 (Telnet)
  + 80 (HTTP)
  + 443 (HTTPS)
  + 111 (RPC)
  + 135 (RPC)
  + E molte altre
* **Flag TCP Rilevati:**
  + **SYN:** Numerosi tentativi di connessione
  + **RST:** Connessioni interrotte rapidamente

#### **Indicatori di Compromissione (IOC)**

1. **Tentativi di scansione delle porte:**
   * Numerose richieste SYN verso porte comuni e non comuni, analizzando le prime 1024 porte per identificare vulnerabilità.
   * Tabelle mostrano una grande quantità di traffico TCP generato dall'host 192.168.200.100 verso la destinazione 192.168.200.150, con porte specifiche e ripetuti tentativi di connessione (flag SYN).

#### **Ipotesi sui Vettori di Attacco**

1. **Port Scanning:**
   * L'host 192.168.200.100 sembra utilizzare strumenti per eseguire una scansione delle porte (ad esempio, Nmap).
2. **Preparazione per Exploit:**
   * Gli attaccanti potrebbero essere alla ricerca di porte aperte per sfruttare vulnerabilità nei servizi esposti.

#### **Azioni Consigliate**

##### **Mitigazione Immediata**

1. **Bloccare l'IP Sospetto:**
   * Configurare regole firewall per bloccare tutto il traffico proveniente da 192.168.200.100.
2. **Monitoraggio in Tempo Reale:**
   * Utilizzare strumenti IDS/IPS come Suricata o Snort per rilevare e bloccare comportamenti sospetti.

##### **Prevenzione**

1. **Hardening della Rete:**
   * Chiudere tutte le porte non necessarie su 192.168.200.150.
   * Limitare l'accesso ai servizi esposti.
2. **Aggiornamento dei Servizi:**
   * Assicurarsi che tutti i servizi in esecuzione siano aggiornati per ridurre vulnerabilità note.
3. **Analisi del Traffico:**
   * Isolare i pacchetti sospetti con strumenti come Wireshark e analizzare i payload per individuare eventuali dati malevoli.
4. **Implementazione di Autenticazione e Crittografia:**
   * Abilitare TLS per tutti i servizi esposti (HTTPS, email, ecc.).
   * Configurare l'autenticazione basata su certificati ove possibile.

#### **Conclusione**

L'analisi dei pacchetti ha evidenziato un comportamento sospetto dell'host 192.168.200.100, suggerendo una scansione delle porte e tentativi di identificare vulnerabilità. È fondamentale implementare misure di mitigazione immediate e rafforzare la sicurezza della rete per prevenire futuri attacchi.

#### **Dettagli Tecnici**

1. **Contesto del traffico:**
   * L'indirizzo IP sorgente principale, 192.168.200.100, invia numerosi pacchetti verso l'indirizzo IP di destinazione, 192.168.200.150.
   * Si osservano numerosi pacchetti TCP con flag SYN inviati senza una risposta completa dal destinatario, accompagnati da un significativo numero di pacchetti RST (reset delle connessioni).
2. **Implicazioni:**
   * Elevato numero di pacchetti SYN: Questo pattern è tipico di un attacco SYN flood, in cui l'attaccante tenta di esaurire le risorse del sistema bersaglio.
   * Presenza di pacchetti RST: L'invio di numerosi pacchetti RST da parte del bersaglio indica che il sistema sta rigettando connessioni non valide o non desiderate.
   * Traffico verso porte multiple: L'attività verso diverse porte suggerisce una scansione delle porte, probabilmente volta a identificare servizi attivi o vulnerabili sul bersaglio.
3. **Azioni consigliate:**
   * Configurare regole di firewall per prevenire traffico non autorizzato.
   * Implementare un sistema IDS/IPS per monitorare le attività di rete in tempo reale.
   * Rafforzare la configurazione di sicurezza della rete, assicurandosi che i servizi esposti siano limitati e aggiornati.