Relazione sull'Analisi della Cattura di Rete in Wireshark

Relazione sull'Analisi della Cattura di Rete in Wireshark

Identificazione degli IOC

Dalla cattura di rete in Wireshark, sono stati individuati diversi Indicatori di Compromissione (IOC). I principali IOC osservati includono:

- **1. Tentativi di Connessione TCP con SYN Flooding:**
  - L'indirizzo IP `192.168.200.100` invia ripetutamente pacchetti TCP SYN su diverse porte di destinazione (es. **880**, **939**, **743**, **831**, ecc.) verso `192.168.200.150`, ma senza ottenere una risposta positiva. Questi pacchetti SYN indicano tentativi di stabilire connessioni, che potrebbero suggerire un tentativo di scansione o attacco.
- **2. Risposte di Reset (RST):**
  - Ogni tentativo di connessione da parte di `192.168.200.100` viene seguito da una risposta RST (Reset) inviata da `192.168.200.150`. Il flag RST indica che la connessione viene immediatamente rifiutata, un comportamento che può essere causato da un firewall o da un sistema di difesa attivo che blocca i tentativi di connessione non autorizzati.
- **3. Pattern di Pacchetti Ripetitivi:**
  - I tentativi di connessione e le risposte RST sono ripetuti in modo quasi identico per diverse porte di comunicazione, indicando una scansione delle porte o un attacco a più porte del server. Questo tipo di comportamento è tipico di attività di scansione da parte di un attaccante che cerca di identificare vulnerabilità nel sistema.

Ipotesi sui Potenziali Vettori di Attacco

In base agli IOC trovati, è possibile formulare le seguenti ipotesi sui potenziali vettori di attacco utilizzati:

- **1. Scansione delle Porte (Port Scanning):**
  - L'invio di pacchetti SYN a diverse porte suggerisce che `192.168.200.100` stia eseguendo una scansione delle porte per identificare eventuali porte aperte o vulnerabili su `192.168.200.150`. Questo comportamento è caratteristico di attacchi di tipo "Port Scanning", dove l'attaccante cerca di mappare la rete e individuare i punti deboli da sfruttare.
- **2. Attacco di Denial of Service (DoS):**

- Il ripetersi dei tentativi di connessione falliti seguiti da risposte RST potrebbe essere parte di un tentativo di DoS. L'attaccante potrebbe star cercando di saturare le risorse del server o del firewall, inondandolo di richieste SYN, un classico esempio di un attacco SYN Flood.

- **3. Tentativi di Intrusione e Ricognizione:**
  - La scansione delle porte potrebbe anche indicare un tentativo di ricognizione finalizzato a identificare vulnerabilità sfruttabili (ad esempio, attraverso exploit di software o servizi non sicuri).

Raccomandazioni per Ridurre gli Impatti dell'Attacco Attuale e Futuri

In risposta agli IOC identificati, si consiglia di adottare le seguenti azioni per mitigare gli impatti dell'attacco corrente e prevenire attacchi simili in futuro:

- **1. Implementazione di un Firewall Rigoroso:**
  - Impostare regole firewall che limitano le connessioni in ingresso da indirizzi IP sospetti o non riconosciuti. Le risposte RST potrebbero già essere una difesa attiva, ma l'adozione di un firewall più restrittivo potrebbe aiutare a bloccare ulteriori tentativi di scansione o attacchi.
- **2. Limiti di Connessione e Rate Limiting:**
  - Implementare un sistema di rate limiting che limiti il numero di connessioni simultanee per un singolo indirizzo IP o porta. Ciò ridurrebbe la capacità di un attaccante di eseguire attacchi SYN Flood.
- **3. Monitoraggio Attivo della Rete:**
  - Attivare il monitoraggio in tempo reale per rilevare anomalie nel traffico di rete, come un numero elevato di pacchetti SYN o tentativi di connessione da un singolo IP verso molteplici porte. L'analisi automatizzata dei flussi di rete può aiutare a identificare tempestivamente attacchi in corso.
- **4. Implementazione di IDS/IPS:**
  - Utilizzare sistemi di rilevamento (IDS) e prevenzione delle intrusioni (IPS) per identificare e bloccare i tentativi di scansione delle porte e gli attacchi DoS prima che possano danneggiare i sistemi.
- **5. Aggiornamenti e Patch di Sicurezza:**
  - Assicurarsi che tutti i dispositivi e le applicazioni siano aggiornati con le ultime patch di sicurezza, per ridurre la possibilità che un attaccante possa sfruttare vulnerabilità note.
- **6. Formazione del Personale e Procedure di Incident Response:**
  - Formare il personale IT a riconoscere i segnali di attacco e rispondere tempestivamente, nonché a implementare e testare regolarmente procedure di risposta agli incidenti per ridurre i tempi di recupero durante un attacco.