Obiettivo dell'esercizio

L'esercizio si concentra sull'analisi di una **cattura di rete** ottenuta con **Wireshark**, con l'obiettivo di identificare **Indicatori di Compromissione (IOC).**

In particolare, l'attività si concentra su una possibile scansione delle porte mediante **Nmap** di tipo **TCP connect (`-sT`)**, che completa l'handshake TCP e risulta particolarmente visibile nel traffico di rete.

Cosa è una scansione `-sT` di Nmap?

Una scansione di tipo `-sT` è una scansione TCP completa, anche conosciuta come **"full connect scan"**. Ecco come funziona:

1. **Invio di un pacchetto SYN** alla porta target.
2. Se la porta è **aperta**, il target risponde con un pacchetto **SYN-ACK**.
3. L'attaccante, completando l'handshake TCP, invia un pacchetto **ACK**.
4. La connessione viene stabilita e il sistema risponde con un pacchetto **ACK** di conferma.

Questa scansione è facilmente rilevabile poiché il traffico TCP mostra connessioni complete, e quindi l'handshake è visibile a chi monitora il traffico di rete.

Indicatori di Compromissione (IOC)

Nel caso specifico, i possibili IOC da cercare nella cattura di traffico di Wireshark sono:

1. **Tipo di pacchetti TCP**:
    - **SYN** (tentativi di connessione);
    - **SYN-ACK** (risposte alle richieste di connessione);
    - **ACK** (completamento dell'handshake).
2. **Comportamento delle connessioni**:
    - La presenza di **scansioni multiple** verso una serie di porte aperte, suggerendo un tentativo di enumerazione delle porte.
    - La sequenza di **SYN-SYN-ACK-ACK** ripetuta potrebbe indicare una scansione delle porte, un comportamento tipico di un attacco di tipo **port scanning**.
3. **Numero di connessioni**: Se una serie di **connessioni brevi** o ripetute verso molte porte diverse è visibile, potrebbe essere un segno di una scansione delle porte.
4. **Flag RST**:
    - La presenza di pacchetti **RST (Reset)** indica che l'attaccante ha ricevuto un "reset" per le connessioni che ha provato a stabilire, segno che le porte potrebbero essere chiuse.
    - Il flag RST viene inviato quando una connessione viene rifiutata o una porta non è aperta.

Possibili Vettori di Attacco

In base agli IOC identificati, si possono fare le seguenti ipotesi sui possibili vettori di attacco:

1. **Scansione delle porte (Port Scanning)**:
    - L'attaccante sta cercando di identificare quali porte sono aperte sulla macchina target. La scansione delle porte è una delle fasi preliminari in un attacco, perché consente di raccogliere informazioni cruciali sui servizi attivi sulla macchina.
    - In particolare, il tipo di scansione `-sT` (TCP connect) implica che l'attaccante sta cercando di stabilire connessioni complete con le porte target per verificare se sono aperte e per identificare i servizi che vi sono in esecuzione.
2. **Esplorazione di vulnerabilità**:
    - Una volta identificati i servizi attivi, l'attaccante potrebbe proseguire tentando di sfruttare vulnerabilità note o effettuare attacchi mirati su questi servizi (ad esempio, sfruttando una vulnerabilità specifica in una versione di un servizio trovato).

Strategie per Mitigare l'Attacco e Ridurre l'Impatto

1. **Monitoraggio e rilevamento delle scansioni di porte**:
    - **IDS/IPS**: Utilizzare sistemi di rilevamento/prevenzione delle intrusioni per monitorare attività sospette, come scansioni di porte, tentativi di connessione ripetuti o pacchetti SYN-RST.
    - **Firewall**: Configurare regole firewall più rigorose per bloccare i pacchetti provenienti da fonti sospette o per limitare la velocità delle connessioni in ingresso.
    - **Rate Limiting**: Implementare **limiti di velocità** per le connessioni, in modo da impedire tentativi di scansioni di porte su larga scala.
2. **Limitare l'accesso alle porte non necessarie**:
    - **Chiusura delle porte non utilizzate**: È buona pratica **chiudere o disabilitare le porte non utilizzate** sul server per ridurre il numero di porte che l'attaccante può targetizzare.
    - **Rete privata virtuale (VPN)**: Se possibile, rendere accessibile solo tramite **VPN** l'accesso a determinate porte o servizi.
3. **Implementazione di tecniche di hardening**:
    - **Hardening del sistema**: Assicurarsi che il sistema sia aggiornato con le patch di sicurezza, e limitare l'accesso ai servizi solo a utenti e indirizzi IP di fiducia.
    - **Gestione dei privilegi**: Ridurre al minimo i privilegi degli utenti e dei servizi, per impedire l'escalation dei privilegi in caso di compromissione.

Conclusioni

La scansione Nmap di tipo `-sT` è una modalità di port scanning piuttosto visibile che completa l'handshake TCP. Analizzando la cattura con Wireshark, abbiamo identificato i possibili IOC relativi a connessioni SYN, risposte SYN-ACK e pacchetti RST, che

suggeriscono un tentativo di enumerazione delle porte. L'attaccante, probabilmente, sta cercando di identificare vulnerabilità sui servizi esposti.

Le misure di mitigazione includono l'uso di IDS/IPS, limitazione dell'accesso alle porte e una configurazione corretta del firewall, per proteggere la macchina target e ridurre i rischi di un attacco riuscito.