PROGETTO S9L5

Traccia:

Esercizio Threat Intelligence & IOC Durante la lezione teorica, abbiamo visto la Threat Intelligence e gli indicatori di compromissione. Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso

- n base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco attuale ed eventualmente un simile attacco futuro

Preparazione dell'Ambiente

Nel contesto dell'esercitazione pratica dedicata alla Threat Intelligence e all'identificazione degli Indicatori di Compromissione (IOC), è stata analizzata una cattura di rete effettuata tramite Wireshark. L'obiettivo dell'analisi è stato quello di individuare eventuali evidenze di attacchi informatici in corso o già avvenuti, formulare ipotesi sui vettori di attacco utilizzati e proporre misure di mitigazione.

Durante l'analisi, è emerso che l'indirizzo IP sorgente dell'attività sospetta è **192.168.200.100**, mentre l'indirizzo IP di destinazione, identificato come potenziale vittima dell'attacco, è **192.168.200.150**. Questo scenario ha permesso di focalizzare l'attenzione sul traffico generato tra i due host, al fine di rilevare comportamenti anomali e possibili compromissioni.

Indicatori di Compromissione Rilevati

Analisi Traffico TCP

È stato rilevato un elevato numero di pacchetti **TCP SYN** inviati da `192.168.200.100` verso `192.168.200.150`, diretti a diverse porte di servizio, tra cui:

- **80 (HTTP)** – traffico web
- **443 (HTTPS)** – comunicazioni cifrate
- **23 (Telnet)** – accesso remoto non sicuro
- **21 (FTP)** – trasferimento file
- **22 (SSH)** – accesso remoto sicuro
- **Altre porte meno comuni**

La sequenza sistematica di richieste SYN su molteplici porte è un chiaro segnale di **port scanning**, una tecnica utilizzata per identificare servizi attivi e potenzialmente vulnerabili su un host. Questo tipo di attività è tipico della fase di **ricognizione** che precede un attacco vero e proprio.

Risposte RST, ACK dal Server

in risposta alle richieste SYN, l'host `192.168.200.150` ha generato numerosi pacchetti **RST, ACK**, indicando che:

- Le porte interrogate non sono attive o non accettano connessioni
- Il server sta rigettando le richieste in modo esplicito, segno che non riconosce il traffico come legittimo
- Non sono presenti handshake TCP completi, quindi non si è instaurata alcuna comunicazione reale

La presenza esclusiva di pacchetti **RST, ACK** rafforza l'ipotesi di una scansione non autorizzata, e rappresenta un chiaro IOC che evidenzia un tentativo di accesso non consentito.

Ipotesi sui Vettori di Attacco (Port Scanning)

Sulla base degli IOC rilevati, è plausibile ipotizzare che l'attaccante stia utilizzando strumenti automatizzati (**Nmap**) per:

- Mappare i servizi esposti sulla macchina target
- Identificare eventuali porte aperte o vulnerabili
- Preparare un attacco mirato sfruttando vulnerabilità note

Il vettore di attacco è riconducibile a una **scansione TCP SYN**, una tecnica silenziosa ma efficace per la raccolta di informazioni preliminari.

Analisi del Traffico ARP

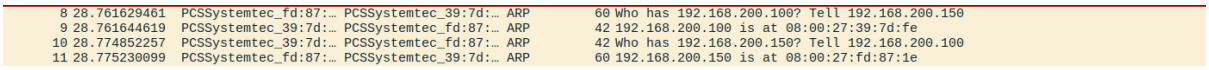
Durante l'analisi del traffico di rete, è stata rilevata una sequenza sospetta di pacchetti **ARP (Address Resolution Protocol)** provenienti dall'indirizzo IP **192.168.200.100** e diretti verso **192.168.200.150**, identificato come potenziale vittima. Sebbene il traffico ARP sia normalmente presente in una rete locale per la risoluzione degli indirizzi IP in MAC address, una frequenza elevata e ripetitiva di richieste **"Who has...?"** può indicare un comportamento malevolo.

Comportamento Osservato

- L'host **192.168.20.100** ha inviato più richieste ARP del tipo: **"Who has 192.168.200.150? Tell 192.168.20.100"**
- Il pattern è coerente con una **scansione ARP**, utilizzata per identificare dispositivi attivi nella rete.

Il fatto che ci sia stata una risposta legittima implica che:

- Il target è **attivo sulla rete** e raggiungibile
- La risoluzione ARP è andata a buon fine, quindi **192.168.20.100** ora conosce il MAC address della vittima
- Se l'intento era malevolo (es. scansione o spoofing), l'attaccante ha ottenuto un'informazione utile per proseguire con un attacco più avanzato, come:
    - **Man-in-the-Middle (MITM)**
    - **ARP poisoning**



8	28.761629461	PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	ARP	60 Who has 192.168.200.100? Tell 192.168.200.150
9	28.761644619	PCSSystemtec_39:7d:…	PCSSystemtec_fd:87:…	ARP	42 192.168.200.100 is at 08:00:27:39:7d:fe
10	28.774852257	PCSSystemtec_39:7d:…	PCSSystemtec_fd:87:…	ARP	42 Who has 192.168.200.150? Tell 192.168.200.100
11	28.775230099	PCSSystemtec_fd:87:…	PCSSystemtec_39:7d:…	ARP	60 192.168.200.150 is at 08:00:27:fd:87:1e

Azioni per mitigare l'impatto e prevenire attacchi futuri

Port Scanning – Contromisure

Il port scanning è una tecnica di ricognizione per identificare servizi attivi e vulnerabili. Per contrastarlo:

- **Configurare firewall per bloccare traffico non autorizzato** Impostare regole restrittive che consentano solo le connessioni necessarie, limitando l'esposizione delle porte.
- **Utilizzare sistemi IDS/IPS per rilevare scansioni** Strumenti come Snort, Suricata o soluzioni commerciali possono identificare pattern di scansione (es. TCP SYN flood) e bloccare l'attaccante.
- **Disabilitare servizi non necessari** Ridurre il numero di porte aperte e servizi attivi minimizza le possibilità di exploit.

- **Implementare rate limiting e blacklisting** Limitare il numero di richieste per IP e bloccare indirizzi che mostrano comportamenti aggressivi.
- **Effettuare vulnerability assessment periodici** Simulare scansioni interne controllate per identificare e correggere eventuali esposizioni prima che lo faccia un attaccante.

ARP Scanning – Contromisure

L'ARP scanning è spesso utilizzato dagli attaccanti per identificare dispositivi attivi nella rete locale. Per contrastarlo:

- **Abilitare la protezione ARP sui dispositivi di rete** Utilizzare switch gestiti con funzionalità di *Dynamic ARP Inspection (DAI)* per bloccare pacchetti ARP non validi o sospetti.
- **Configurare voci ARP statiche per host critici** Impedisce che le tabelle ARP vengano sovrascritte da richieste malevole, proteggendo server e dispositivi sensibili.
- **Segmentare la rete in VLAN** Isolare i dispositivi in sottoreti dedicate riduce la visibilità e la superficie d'attacco per chi tenta di mappare la rete.
- **Monitorare il traffico ARP con IDS/IPS** Rilevare pattern di richieste ripetitive e generare alert in caso di scansioni sospette.
- **Limitare l'accesso fisico e logico alla rete LAN** Autenticazione su porta, NAC (Network Access Control) e whitelist MAC address per impedire l'ingresso di dispositivi non autorizzati.

Difesa Integrata

Infine, è consigliabile adottare un approccio **difensivo proattivo e multilivello**, che includa:

- **Formazione del personale IT** per riconoscere segnali di ricognizione e reagire tempestivamente
- **Logging e analisi centralizzata** per correlare eventi e individuare pattern sospetti
- **Aggiornamento costante dei dispositivi di rete e sicurezza** per garantire la protezione contro tecniche di scansione sempre più sofisticate

Conclusione

L'analisi della cattura di rete ha permesso di identificare diversi **Indicatori di Compromissione (IOC)** che suggeriscono attività sospette e potenzialmente malevole all'interno della rete. In particolare, sono stati rilevati:

- **Scansioni ARP** ripetute da parte dell'host `192.168.20.100` verso `192.168.200.150`, indicative di una fase di ricognizione per mappare i dispositivi attivi
- **Port scanning TCP SYN** su porte comuni e critiche, finalizzato all'individuazione di servizi esposti e vulnerabili
- **Risposte RST, ACK** da parte del target, segno che le connessioni non sono autorizzate e che il sistema sta rigettando i tentativi di accesso

Questi comportamenti, seppur tecnicamente semplici, rappresentano le fasi iniziali di un attacco informatico e non devono essere sottovalutati. L'identificazione tempestiva degli IOC ha consentito di formulare ipotesi sui vettori di attacco utilizzati, come strumenti automatizzati di scansione e tecniche di spoofing, e di proporre misure concrete per contenere l'impatto e rafforzare la sicurezza della rete.

In conclusione, l'esercizio ha evidenziato l'importanza della **Threat Intelligence** come strumento proattivo per la difesa informatica, dimostrando come anche segnali apparentemente innocui possano nascondere tentativi di compromissione. Una rete ben monitorata, segmentata e protetta da sistemi IDS/IPS rappresenta la chiave per prevenire attacchi futuri e garantire la resilienza dell'infrastruttura.