Report Threat Intelligence & IOC

Obiettivo

L'obiettivo principale di questa attività è l'esame analitico del traffico di rete per rispondere ai seguenti requisiti di sicurezza:

1. **Detection:** Isolare e documentare gli IOC (indirizzi IP, pattern di traffico, anomalie nei protocolli) che confermano un'attività malevola.
2. **Threat Modeling:** Formulare ipotesi realistiche sui vettori di attacco utilizzati dall'attore malevolo, basandosi sulle evidenze raccolte.
3. **Incident Response:** Definire un piano d'azione immediato per la mitigazione del rischio (Containment) e proporre strategie a lungo termine per il rafforzamento della sicurezza (Hardening) della rete.

1. Identificazione e Analisi degli IOC

Dall'analisi del file di cattura, emergono chiari indicatori che un attacco (nello specifico la fase di *Reconnaissance*) è in corso.

A. IOC di Rete (Indirizzi IP e Ruoli)

Il primo passo è definire gli attori coinvolti analizzando le "Conversations" di Wireshark:

- **IP Attaccante:** `192.168.200.100` (è il mittente della raffica di pacchetti).
- **IP Vittima:** `192.168.200.150` (corrisponde all'host denominato "Metasploitable").

B. IOC Comportamentale: Scansione delle Porte (Port Scanning)

L'evidenza principale è l'altissima frequenza di pacchetti inviati in un brevissimo lasso di tempo.

- **Dettaglio Tecnico:** Si nota una sequenza di pacchetti **TCP [SYN]** inviati dall'attaccante verso porte diverse (80, 21, 22, 23, 443, 445, ecc.).
- **Analisi dei Flag:** L'invio massivo di flag SYN senza completare l'handshake TCP (spesso seguito da un RST da parte della vittima se la porta è chiusa) è un IOC tipico di un **SYN Stealth Scan** (eseguito solitamente con il comando `nmap -sS`).

C. IOC di Servizio: Tentativi di Connessione a Porte Critiche

Osservando la colonna "Info" e la colonna "Destination Port" notiamo le porte "sotto attacco":

- **Porta 21 (FTP):** Possibile tentativo di individuare versioni vulnerabili di ProFTPD o vsftpd.
- **Porta 23 (Telnet):** Tentativo di trovare un accesso remoto non cifrato.
- **Porta 80 (HTTP):** Ricerca di server web per successivi attacchi di tipo SQL Injection o Cross-Site Scripting (XSS).

D. Analisi dei Tempi (Timestamp)

Un altro IOC fondamentale è il **tempo di occorrenza**. Nota come tra un pacchetto e l'altro passino solo pochi millisecondi. Un comportamento umano non può generare richieste così rapide verso porte sequenziali o casuali; questo indica l'uso di un **tool automatizzato**.

2. Ipotesi sui Potenziali Vettori di Attacco

Dato che l'attaccante ha preso di mira una macchina **Metasploitable** (famosa per avere servizi vulnerabili "out-of-the-box"), i vettori più probabili sono:

A. Sfruttamento di Servizi di Rete Vulnerabili (Exploitation)

È l'ipotesi più immediata. L'attaccante ha scansionato porte specifiche che spesso ospitano software datato:

- **Porta 21 (FTP):** Potrebbe tentare di sfruttare backdoor note (come quella famosa di *vsftpd 2.3.4*) per ottenere una shell immediata.
- **Porta 445 (SMB):** Un classico. L'attaccante potrebbe testare vulnerabilità come **EternalBlue (MS17-010)** per eseguire codice da remoto senza credenziali.

B. Attacchi ai Servizi Web (Web-based Attacks)

C’è traffico sulla **Porta 80**. Questo apre la strada a una miriade di vettori a livello applicativo:

- **SQL Injection (SQLi):** Se il server ospita un database, l'attaccante potrebbe provare a esfiltrare dati tramite i form di login o parametri URL.

- **Remote Code Execution (RCE):** Tentare di caricare script malevoli (web shell) tramite vulnerabilità di upload o plugin non aggiornati.

C. Accesso tramite Credenziali Deboli (Brute Force / Guessing)

La presenza di porte come la **22 (SSH)** e la **23 (Telnet)** suggerisce un altro vettore molto comune:

- **Brute Force:** L'attaccante potrebbe usare tool come *Hydra* per tentare migliaia di combinazioni di username e password (es. `admin:admin`, `root:root`).
- **Credential Stuffing:** Utilizzo di password rubate in altri data breach nella speranza che siano state riutilizzate.

3. Azioni per ridurre gli impatti ed evitare attacchi futuri

A. Azioni Immediate (Contenimento)

Queste sono le operazioni da fare "mentre i pacchetti corrono" per limitare i danni:

1. **Interruzione della comunicazione:** Configurare immediatamente una regola sul Firewall perimetrale o sull'Host-based Firewall (come `iptables` o `ufw` su Linux) per bloccare tutto il traffico proveniente dall'IP sorgente identificato come malevolo: `192.168.200.100`.
2. **Isolamento dell'Host:** Se si sospetta che dopo la scansione l'attaccante sia riuscito a entrare (ad esempio se vedi traffico anomalo dopo la fase di scan), la macchina vittima (`192.168.200.150`) deve essere isolata dalla rete per evitare movimenti laterali verso altri server aziendali.
3. **Reset delle sessioni:** Terminare forzatamente tutte le connessioni TCP attive tra l'attaccante e la vittima.

B. Azioni Correttive e di Hardening (Prevenzione)

Per evitare che un simile attacco abbia successo in futuro, bisogna ridurre la "superficie di attacco":

1. **Chiusura dei servizi non necessari:** Abbiamo visto porte aperte come la 21 (FTP) e la 23 (Telnet). Questi protocolli sono obsoleti e insicuri. Vanno disabilitati se non strettamente necessari per il business.
2. **Patch Management:** Aggiornare tutti i servizi rimasti aperti (es. il server Web sulla porta 80 o SMB sulla 445) all'ultima versione disponibile per correggere le vulnerabilità che l'attaccante stava cercando di individuare.
3. **Configurazione di un IPS/IDS:** Implementare un sistema di rilevamento e prevenzione delle intrusioni (come **Snort** o **Suricata**). Questi strumenti avrebbero rilevato automaticamente il "SYN Scan" e avrebbero potuto bloccare l'IP dell'attaccante dopo i primi tentativi.
4. **Implementazione di Fail2Ban:** Configurare un tool che blocchi automaticamente per un certo periodo di tempo gli indirizzi IP che effettuano troppi tentativi di connessione falliti o scansioni rapide.
5. **Cifratura dei dati:** Sostituire protocolli in chiaro (Telnet, FTP) con versioni cifrate (SSH, SFTP) per evitare che l'attaccante possa "sniffare" le credenziali durante l'accesso.

SOMMA MASSIMO