Report di Analisi degli Indicatori di Compromissione (IOC)

Obiettivo: Identificare, analizzare e mitigare un attacco in corso basato sul traffico di rete fornito.

1. Identificazione degli Indicatori di Compromissione (IOC)

Gli IOC sono le "impronte digitali" di un attacco. La nostra analisi si è basata sulla scansione dei pacchetti di rete per individuare attività anomale.

- **IOC 1: Riconoscimento del Sistema Vulnerabile.** Il primo pacchetto della nostra analisi mostra una chiara identificazione del sistema di destinazione. Un host si è annunciato come "METASPLOITABLE". Questo è un nome comunemente usato per sistemi volutamente vulnerabili, suggerendo che l'attaccante ha trovato un bersaglio facile.
- **IOC 2: Scansione di Porte Aggressiva.** Abbiamo osservato un'alta frequenza di pacchetti TCP con il flag `SYN` (richiesta di connessione) che non hanno avuto successo e sono stati immediatamente seguiti da pacchetti `RST` (connessione interrotta). Questa sequenza, che si ripete su una vasta gamma di porte, è il segnale di una **scansione delle porte** in corso. L'attaccante sta cercando di identificare quali servizi sono attivi e accessibili.
- **IOC 3: Identificazione degli Indirizzi IP.** Dall'analisi dei pacchetti, abbiamo identificato chiaramente gli indirizzi IP:
    - **Indirizzo di Origine:** `192.168.200.150` (la macchina dell'attaccante).
    - **Indirizzo di Destinazione:** `192.168.200.100` (il sistema vittima).

2. Spiegazione dei Termini Chiave e delle Analisi

Come abbiamo capito che l'host è Metasploitable?

L'identificazione di un host come "Metasploitable" è avvenuta grazie all'analisi del **banner di servizio** nel primo pacchetto. Un banner è come un biglietto da visita che un server invia a chi si connette. Nel nostro caso, il banner conteneva esplicitamente la stringa "METASPLOITABLE", un nome che non viene mai utilizzato in ambienti di produzione. Questo ha immediatamente rivelato che si trattava di una macchina vulnerabile, spesso usata per esercitazioni di sicurezza.

Cosa indicano i flag SYN e RST?

Nel traffico di rete, i flag TCP come `SYN`, `ACK` e `RST` sono fondamentali per capire lo stato di una connessione.

- Il flag **SYN** (Synchronize) indica che un client sta tentando di avviare una connessione.
- Il flag **RST** (Reset) indica che un server sta immediatamente terminando una connessione.

Quando vediamo un'alta concentrazione di pacchetti `SYN` che ricevono una risposta `RST`, come nel nostro caso, significa che l'attaccante sta inviando richieste di connessione a porte che non sono

aperte. Questo comportamento è la firma di una scansione di porte. A volte, si vede `RST` insieme a `ACK`, che suggerisce un tentativo di scansione più subdolo, in cui la connessione non viene mai completata del tutto per non lasciare tracce evidenti.

Come abbiamo capito che si tratta di una scansione con Nmap?

Sebbene non si identifichi in modo esplicito, il traffico ha la firma di uno strumento come Nmap. Nmap invia una serie di pacchetti per mappare i servizi attivi su un host. La combinazione di un alto volume di pacchetti `SYN` e le risposte `RST` è la tipica "conversazione" di una scansione Nmap. Quando questo accade su una macchina nota per essere vulnerabile come Metasploitable, l'ipotesi è quasi certa.

3. Ipotesi sui Potenziali Vettori di Attacco

Sulla base delle prove raccolte, è possibile formulare un'ipotesi chiara sul tipo di attacco e gli strumenti utilizzati.

- **Vettore di Attacco Primario: Scanning e Enumerazione.** L'attacco è iniziato con una fase di **riconoscimento**. L'attaccante ha utilizzato strumenti come **Nmap** o un modulo di scansione integrato in un framework di hacking per identificare la natura del sistema vittima e le sue potenziali vulnerabilità. L'obiettivo era creare una mappa dei servizi aperti per pianificare l'attacco.
- **Vettore di Attacco Secondario: Framework di Sfruttamento.** La presenza del banner "METASPLOITABLE" e il traffico di scansione indicano che l'attaccante sta utilizzando un framework per l'hacking etico, probabilmente **Metasploit**. Questi framework automatizzano la fase di attacco, permettendo all'hacker di scegliere un exploit mirato per la vulnerabilità identificata.

4. Azioni Consigliate per Ridurre gli Impatti

Per rispondere efficacemente a questo incidente e rafforzare la sicurezza a lungo termine, raccomandiamo le seguenti azioni.

- **Azione Immediata:**
    1. **Isolamento del Sistema:** Disconnettere immediatamente il sistema con IP `192.168.200.100` dalla rete. Questo previene qualsiasi ulteriore tentativo di intrusione e l'eventuale diffusione dell'attacco.
    2. **Backup e Analisi Forense:** Eseguire un backup completo del sistema e condurre un'analisi forense per determinare l'entità dell'attacco.
- **Azioni di Mitigazione a Lungo Termine:**
    1. **Rafforzamento del Firewall:** Implementare un firewall per filtrare e bloccare il traffico in entrata da indirizzi IP sospetti e su porte non necessarie.
    2. **Patch Management:** Eseguire un aggiornamento completo di tutti i sistemi operativi e i software per correggere le vulnerabilità note.

3. **Monitoraggio Proattivo:** Installare e configurare un sistema di monitoraggio del traffico di rete in grado di rilevare e avvisare in tempo reale su attività anomale, come le scansioni di porte.

4. **Formazione del Personale:** Fornire una formazione continua al personale sui rischi e sulle migliori pratiche di sicurezza per prevenire attacchi futuri.

Info Extra

Wireshark è uno strumento di analisi di rete potentissimo che permette di scavare molto più a fondo. Si possono ricavare:

- **Contenuto dei pacchetti:** Possiamo ispezionare il payload per trovare password in chiaro, dati sensibili, comandi eseguiti, o file trasferiti.
- **Conversazioni complete:** Possiamo ricostruire l'intera "storia" di una connessione, analizzando la sequenza di pacchetti per capire esattamente cosa è successo tra l'attaccante e il bersaglio.
- **Analisi delle performance:** Possiamo identificare la latenza e la perdita di pacchetti, che possono essere segnali di attacchi di tipo DoS (Denial of Service).

Conclusioni

L'analisi del traffico di rete ha fornito prove chiare di un attacco in corso, con indicatori di compromissione che puntano a una scansione di rete e all'uso di un framework di hacking. La rapida identificazione di questi segnali è cruciale per la risposta all'incidente. Le azioni immediate di isolamento e le misure a lungo termine, come il rafforzamento del firewall e il monitoraggio, sono fondamentali per mitigare l'impatto attuale e prevenire futuri attacchi. Questo esercizio sottolinea l'importanza di una vigilanza costante e di un approccio proattivo alla sicurezza, essenziali per proteggere le risorse aziendali dalle minacce informatiche in evoluzione.