Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, informazione

Descrizione generata automaticamente

* **Richieste TCP ripetute**: Ci sono molteplici richieste TCP con il flag SYN impostato inviate dall'indirizzo IP 192.168.200.100 verso l'indirizzo IP 192.168.200.150.

Basandoci su questi IOC, possiamo ipotizzare i seguenti potenziali vettori di attacco:

* **Scansione delle porte**: L'host con indirizzo IP 192.168.200.100 potrebbe essere coinvolto in una scansione delle porte dell'host di destinazione 192.168.200.150. Questo tipo di attività potrebbe essere finalizzato a identificare servizi e porte aperte su 192.168.200.150 per potenziali attacchi successivi.
* Sì, l'analisi della cattura di rete suggerisce fortemente che ci sia una scansione in corso da parte dell'host 192.168.200.100 verso l'host target 192.168.200.150. Questa ipotesi è supportata dalle risposte ricevute dal target:
* - Le risposte [SYN+ACK] indicano che alcune porte sono aperte e il target ha risposto positivamente alla richiesta di connessione SYN inviata dall'host 192.168.200.100. Questo suggerisce che il target sta accettando connessioni su quelle porte.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

* - Le risposte [RST+ACK] indicano che altre porte sono chiuse e il target ha risposto negativamente alla richiesta di connessione SYN inviata dall'host 192.168.200.100. Questo suggerisce che il target ha respinto la richiesta di connessione su quelle porte.
* Questa evidenza supporta l'ipotesi di una scansione in corso da parte dell'host 192.168.200.100 per determinare lo stato delle porte sull'host 192.168.200.150. La scansione potrebbe essere finalizzata all'identificazione di porte aperte che potrebbero essere vulnerabili ad attacchi successivi.
* In risposta a questa potenziale minaccia, è consigliabile configurare delle regole firewall per respingere le richieste in entrata dall'host 192.168.200.100 sull'host 192.168.200.150. Questo ridurrebbe l'esposizione del target alle scansioni e agli attacchi provenienti dall'host sospetto e proteggerebbe le risorse di rete da potenziali violazioni della sicurezza.

Per ridurre gli impatti di tale attacco, possiamo adottare le seguenti azioni:

* **Configurazione delle politiche firewall**: Si potrebbe configurare il firewall sull'host 192.168.200.150 per bloccare l'accesso a tutte le porte provenienti dall'host 192.168.200.100. Questo impedirebbe all'attaccante di continuare la scansione delle porte e proteggerebbe le informazioni sulle porte e sui servizi in ascolto dall'essere acquisite dall'attaccante.

La configurazione delle politiche firewall per bloccare l'accesso dall'indirizzo IP sospetto è una pratica comune per proteggere un sistema da tentativi di scansione delle porte e altri attacchi. Questo può essere implementato attraverso l'utilizzo di regole di firewall che specificano quali indirizzi IP sono autorizzati a comunicare con il sistema e quali devono essere bloccati. In questo caso specifico, bloccare l'accesso dall'host 192.168.200.100 impedirebbe all'attaccante di continuare la scansione delle porte sull'host 192.168.200.150, proteggendo così il sistema da potenziali attacchi basati su queste informazioni di scansione.

Per ridurre l'impatto di scansioni e potenziali attacchi futuri, è consigliabile adottare le seguenti misure di sicurezza:

1. \*\*Aggiornare e patchare regolarmente i sistemi\*\*: Mantenere tutti i sistemi e le applicazioni aggiornate con le patch di sicurezza più recenti può ridurre le vulnerabilità e prevenire l'esposizione a potenziali attacchi.

2. \*\*Configurare correttamente i firewall\*\*: Utilizzare firewall per limitare l'accesso alle porte e ai servizi solo a quelle necessarie per il funzionamento del sistema. Configurare regole firewall per bloccare l'accesso da indirizzi IP sospetti o noti per attività malevole.

3. \*\*Monitorare il traffico di rete\*\*: Utilizzare strumenti di monitoraggio del traffico di rete per individuare e analizzare comportamenti anomali, come scansioni delle porte o attività sospette.

4. \*\*Implementare la protezione avanzata contro minacce\*\*: Utilizzare soluzioni di sicurezza avanzate, come sistemi di rilevamento delle intrusioni (IDS) e sistemi di prevenzione delle intrusioni (IPS), per rilevare e mitigare attacchi in tempo reale.

5. \*\*Educare gli utenti\*\*: Sensibilizzare gli utenti sulle pratiche di sicurezza informatica, come l'utilizzo di password robuste, l'evitare di cliccare su link sospetti o di aprire allegati di posta elettronica da mittenti non attendibili.

6. \*\*Implementare autenticazione a più fattori (MFA)\*\*: Utilizzare l'autenticazione a più fattori per proteggere l'accesso alle risorse critiche, riducendo così il rischio di compromissione delle credenziali.

7. \*\*Monitoraggio e risposta agli incidenti\*\*: Avere procedure ben definite per la gestione degli incidenti di sicurezza, inclusa la capacità di rispondere prontamente e mitigare gli attacchi quando si verificano.

Implementando queste misure di sicurezza, è possibile ridurre l'impatto di scansioni e potenziali attacchi futuri, proteggendo così l'infrastruttura di rete e le risorse critiche dall'accesso non autorizzato e dalle violazioni della sicurezza.