Esito Analisi dell 11/10/2024 Per azienda Theta

Nel file Cattura_U3_W1_L3.pcapng fornitomi oggi ho notato la comunicazione tra due ip (192.168.200.100 e 192.168.200.150) attraverso il protocollo TCP.

Ho notato che vengono fatte piu' richieste di seguito dall' ip 100 verso la 150 ma dopo ogni SYN, ACK di risposta da parte non avviene piu' la chiusura del three-way handshake su diverse porte e questo ha generato subito in me la possibilita' di un attacco DOS attraverso SYN flood :

SYN FLOOD : Immagina di voler attaccare una macchina (come un server o un computer connesso a una rete) usando un **SYN flood**. Questo attacco cerca di bloccare il sistema impedendo agli altri di usarlo normalmente.

Ecco come funziona in pratica:

1. **Invio delle richieste false:** L'attaccante invia tantissime richieste di connessione alla macchina bersaglio. Queste richieste si chiamano **SYN**, e sono il primo passo per stabilire una connessione.
2. **La macchina risponde:** La macchina attaccata, pensando che queste richieste siano legittime, risponde con un messaggio che dice "Ok, sono pronta a connettermi", aspettandosi una conferma finale da chi ha fatto la richiesta.
3. **Nessuna risposta:** L'attaccante però non risponde mai. Lascia la macchina attaccata in attesa, come se fosse in sospeso.
4. **Risultato:** La macchina continua a ricevere nuove richieste SYN, ma tutte restano incomplete. Questo riempie la sua capacità di gestire le connessioni, rendendola sempre più lenta o completamente bloccata. Così, le persone che cercano di connettersi alla macchina non riescono a farlo, perché il sistema è sovraccarico e non può accettare nuove connessioni.

In breve, l'attaccante bombarda la macchina con richieste false per farla esaurire e impedire che risponda a utenti legittimi, bloccando l'accesso ai suoi servizi.

Visto la tipologia di vettore propongo di intervenire con le seguenti pratiche:

1. Aumentare la capacità del server

- **Ridurre il rischio di saturazione:** Configura i server per gestire un numero maggiore di connessioni, così possono sopportare un carico più elevato senza rallentare o bloccarsi.
- **Limitare il tempo di attesa delle connessioni:** Riduci il tempo che il server aspetta per completare una connessione sospetta, in modo da liberare più velocemente le risorse.

2. Usare firewall e sistemi di prevenzione

- **Firewall e filtri anti-DDoS:** Installa un firewall che riconosce e blocca automaticamente il traffico anomalo, come troppe richieste SYN provenienti da un solo indirizzo IP o da IP sospetti.
- **Filtro del traffico SYN:** Configura il firewall per limitare il numero di richieste SYN che possono provenire da una singola fonte o da un intervallo ristretto di indirizzi IP.

3. Abilitare SYN cookies

- **Cos'è:** I SYN cookies sono una tecnica che permette al server di non conservare le connessioni SYN incomplete nella memoria. Invece, la risposta del server include informazioni che permettono di ricostruire la connessione senza occupare risorse.
- **Vantaggio:** Questo protegge il server dall'esaurimento delle risorse, mantenendo aperte solo le connessioni legittime.

4. Usare un servizio di protezione contro DDoS

- **Protezione esterna:** Aziende che offrono servizi di protezione contro attacchi DDoS (come Cloudflare, Akamai, ecc.) possono filtrare e

bloccare il traffico malevolo prima che raggiunga i server dell'azienda. Questo è particolarmente utile per aziende con risorse limitate o senza un team di sicurezza dedicato.

5. Monitorare il traffico di rete

- **Rilevamento tempestivo:** Implementa strumenti di monitoraggio che controllano costantemente il traffico di rete e possono allertare se si notano picchi anomali di richieste, così da poter reagire rapidamente.
- **Semplicità d'uso:** Molti strumenti di monitoraggio (come Zabbix, Nagios, o servizi cloud) sono relativamente semplici da configurare e usare, anche per chi ha poca esperienza.

6. Aggiornamenti e manutenzione

- **Tenere il software aggiornato:** Assicurarsi che i server, i firewall e il software di rete siano sempre aggiornati con le ultime patch di sicurezza per proteggersi da vulnerabilità note che possono essere sfruttate in attacchi come il SYN flood.

7. Formazione del personale

- **Consapevolezza:** Anche se l'azienda ha poca esperienza, è importante educare il personale sui rischi e sui segnali di un attacco, per essere preparati a reagire prontamente in caso di sospetto.

Con queste best practices potrete sicuramente scongiurare attacchi di questo tipo ora e nel prossimo futuro.

11/10/2024

Nicolo` Biasio

Wolf ethical hacker member