Definizione delle strategie di protezione dagli attacchi Denial of Service TCP SYN

Sommario

Riassunto

Esiste un potenziale attacco Denial of Service presso i provider di servizi Internet (ISP) che interessa i dispositivi di rete.

- **Attacco SYN TCP**: Un mittente trasmette un volume di connessioni che non possono essere completate. In questo modo le code di connessione si riempiono, negando in tal modo il servizio agli utenti TCP legittimi.

Questo documento contiene una descrizione tecnica di come si verifica il potenziale attacco TCP SYN e suggerisce i metodi per utilizzare il software Cisco IOS per difendersi da esso.

Nota: il software Cisco IOS 11.3 è dotato di una funzione per prevenire attivamente gli attacchi TCP Denial of Service. Questa funzione è descritta nel documento sulla configurazione di TCP Intercept (Prevenzione di attacchi Denial of Service).

Prerequisiti

Requisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Descrizione del problema

L'attacco TCP SYN

Quando si avvia una normale connessione TCP, un host di destinazione riceve un pacchetto SYN (sincronizzazione/avvio) da un host di origine e restituisce un pacchetto SYN ACK (sincronizzazione conferma). L'host di destinazione deve quindi ascoltare un ACK (conferma) del SYN ACK prima di stabilire la connessione. Questo processo è noto come "handshake TCP a tre vie".

In attesa che il ACK venga inviato al SYN ACK, una coda di connessione di dimensioni finite sull'host di destinazione tiene traccia delle connessioni in attesa di completamento. In genere questa coda si svuota rapidamente poiché si prevede che l'ACK arrivi alcuni millisecondi dopo l'ACK SYN.

L'attacco TCP SYN sfrutta questo progetto facendo in modo che un host di origine di attacco generi pacchetti TCP SYN con indirizzi di origine casuali verso un host vittima. L'host di destinazione della vittima invia un SYN ACK all'indirizzo di origine casuale e aggiunge una voce alla coda di connessione. Poiché l'ACK SYN è destinato a un host errato o inesistente, l'ultima parte dell'handshake a tre vie non viene mai completata e la voce rimane nella coda di connessione fino alla scadenza di un timer, in genere per circa un minuto. Generando rapidamente pacchetti TCP SYN falsi da indirizzi IP casuali, è possibile riempire la coda di connessione e negare i servizi TCP (come e-mail, trasferimento file o WWW) agli utenti legittimi.

Non c'è un modo semplice per rintracciare l'autore dell'attacco perché l'indirizzo IP della fonte è falsificato.

Le manifestazioni esterne del problema includono l'impossibilità di ricevere posta elettronica, di accettare connessioni ai servizi WWW o FTP o a un numero elevato di connessioni TCP sull'host nello stato SYN_RCVD.

Difesa dagli attacchi ai dispositivi di rete

Dispositivi dietro i firewall

L'attacco TCP SYN è caratterizzato da un afflusso di pacchetti SYN da indirizzi IP di origine casuali. Tutti i dispositivi dietro un firewall che arrestano i pacchetti SYN in entrata sono già protetti da questa modalità di attacco e non sono necessarie ulteriori azioni. Esempi di firewall includono un firewall Cisco Private Internet Exchange (PIX) o un router Cisco configurato con elenchi degli accessi. Per esempi su come configurare gli elenchi degli accessi su un router Cisco, consultare il documento sul miglioramento della sicurezza sulle reti IP.

Dispositivi che offrono servizi disponibili al pubblico (server di posta, server Web pubblici)

Impedire gli attacchi SYN sui dispositivi dietro i firewall da indirizzi IP casuali è relativamente semplice, poiché è possibile utilizzare gli elenchi degli accessi per limitare esplicitamente l'accesso in entrata a pochi indirizzi IP selezionati. Tuttavia, nel caso di un server Web pubblico o di un server di posta con connessione Internet, non è possibile determinare quali indirizzi di origine IP in ingresso siano descrittivi e quali sconsigliati. Pertanto, non esiste una difesa netta contro un attacco da un indirizzo IP casuale. Per gli host sono disponibili diverse opzioni:

- Aumentare le dimensioni della coda di connessione (coda SYN ACK).
- Ridurre il timeout in attesa della stretta di mano a tre vie.
- Utilizzare le patch del software del fornitore per rilevare e aggirare il problema (se disponibile).

Contattare il fornitore dell'host per verificare se sono state create patch specifiche per risolvere l'attacco TCP SYN ACK.

Nota: il filtro degli indirizzi IP sul server non è efficace in quanto un utente non autorizzato può variare il proprio indirizzo IP e l'indirizzo può essere o non essere lo stesso di un host legittimo.

Come impedire a una rete di ospitare involontariamente un attacco

Poiché un meccanismo primario di questo attacco di negazione del servizio è la generazione di traffico proveniente da indirizzi IP casuali, si consiglia di filtrare il traffico destinato a Internet. Il concetto di base è quello di eliminare i pacchetti con indirizzi IP di origine non validi quando entrano in Internet. Ciò non impedisce un attacco Denial of Service sulla rete, ma aiuterà le parti attaccate a escludere la tua posizione come origine dell'aggressore. Inoltre, rende la rete meno attraente come base per questa classe di attacco.

Impedire la trasmissione di indirizzi IP non validi

Filtrando i pacchetti sui router che connettono la rete a Internet, è possibile consentire solo ai pacchetti con indirizzi IP di origine validi di uscire dalla rete e accedere a Internet.

Ad esempio, se la rete è costituita dalla rete 172.16.0.0 e il router si connette all'ISP utilizzando un'interfaccia 0/1 seriale, è possibile applicare l'elenco degli accessi come segue:

```
access-list 111 permit ip 172.16.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 0/1
ip access-group 111 out
```

Nota: l'ultima riga dell'elenco degli accessi determina se è presente traffico con un indirizzo di origine non valido che entra in Internet. Non è cruciale avere questa linea, ma aiuterà a individuare la fonte dei possibili attacchi.

Impedire la ricezione di indirizzi IP non validi

Per gli ISP che forniscono servizi per terminare le reti, è consigliabile convalidare i pacchetti in ingresso provenienti dai client. A tale scopo, è possibile utilizzare i filtri pacchetti in ingresso sui router di confine.

Ad esempio, se i client hanno i seguenti numeri di rete collegati al router tramite un'interfaccia seriale denominata "serial 1/0", è possibile creare il seguente elenco degli accessi:

```
The network numbers are 192.168.0.0 to 192.168.15.0, and 172.18.0.0.

access-list 111 permit ip 192.168.0.0 0.0.15.255 any
access-list 111 permit ip 172.18.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 1/0
ip access-group 111 in
```

Nota: l'ultima riga dell'elenco degli accessi determina se è presente traffico con indirizzi di origine non validi che entra in Internet. Non è cruciale avere questa linea, ma aiuterà a individuare la fonte del possibile attacco.

Questo argomento è stato trattato in dettaglio nella mailing list NANOG [North American Network Operator1s Group]. Gli archivi dell'elenco si trovano all'indirizzo: http://www.merit.edu/mail.archives/nanog/index.html

Per una descrizione dettagliata dell'attacco Denial of Service TCP SYN e dello spoofing IP, vedere: http://www.cert.org/advisories/CA-1996-21.html

http://www.cert.org/advisories/CA-1995-01.html

Informazioni correlate

- Supporto tecnico – Cisco Systems