Definieren von Strategien zum Schutz vor DoS-Angriffen (Denial of Service) auf TCP SYN

Inhalt

Zusammenfassung

Bei Internetdienstanbietern (ISPs), die auf Netzwerkgeräte abzielen, besteht ein potenzieller Denial-of-Service-Angriff.

- **TCP SYN-Angriff**: Ein Absender überträgt ein Volumen von Verbindungen, die nicht abgeschlossen werden können. Dadurch werden die Verbindungswarteschlangen gefüllt, wodurch legitimen TCP-Benutzern der Dienst verweigert wird.

Dieses Whitepaper enthält eine technische Beschreibung des möglichen TCP-SYN-Angriffs und Vorschläge für Methoden zur Abwehr dieser Angriffe mit der Cisco IOS-Software.

Hinweis: Die Cisco IOS 11.3-Software verfügt über eine Funktion, mit der TCP-Denial-of-Service-Angriffe aktiv verhindert werden können. Diese Funktion wird im Dokument Konfigurieren des TCP-Intercept (Verhinderung von Denial-of-Service-Angriffen) beschrieben.

Voraussetzungen

Anforderungen

Es sind keine besonderen Voraussetzungen erforderlich, um den Inhalt dieses Dokuments nachzuvollziehen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn sich Ihr Netzwerk in der Produktionsumgebung befindet, müssen Sie sich bei jedem Befehl zunächst dessen potenzielle Auswirkungen vor Augen führen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Problembeschreibung

TCP-SYN-Angriff

Wenn eine normale TCP-Verbindung gestartet wird, empfängt ein Ziel-Host ein SYN-Paket (synchronisieren/starten) von einem Quellhost und sendet eine SYN ACK zurück (Bestätigung synchronisieren). Der Ziel-Host muss dann eine ACK (Bestätigung) der SYN ACK hören, bevor die Verbindung hergestellt wird. Dies wird als "Drei-Wege-TCP-Handshake" bezeichnet.

Während Sie auf die ACK für die SYN-ACK warten, verfolgt eine Verbindungswarteschlange mit begrenzter Größe auf dem Ziel-Host alle Verbindungen, die auf ihre Fertigstellung warten. Diese Warteschlange wird in der Regel schnell geleert, da erwartet wird, dass das ACK einige Millisekunden nach der SYN ACK-Nachricht eintrifft.

Der TCP SYN-Angriff nutzt dieses Design aus, indem ein angreifender Quellhost TCP-SYN-Pakete mit zufälligen Quelladressen für einen angegriffenen Host generiert. Der Ziel-Host des Opfers sendet eine SYN-ACK zurück an die zufällige Quelladresse und fügt einen Eintrag in die Verbindungswarteschlange hinzu. Da die SYN ACK für einen falschen oder nicht vorhandenen Host bestimmt ist, wird der letzte Teil des "Drei-Wege-Handshake" nie abgeschlossen, und der Eintrag bleibt in der Verbindungswarteschlange, bis ein Timer abläuft, normalerweise für etwa eine Minute. Durch das schnelle Generieren von gefälschten TCP-SYN-Paketen von zufälligen IP-Adressen ist es möglich, die Verbindungswarteschlange zu füllen und TCP-Dienste (z. B. E-Mail, Dateiübertragung oder WWW) legitimen Benutzern zu verweigern.

Es gibt keine einfache Möglichkeit, den Urheber des Angriffs zu verfolgen, da die IP-Adresse der Quelle gefälscht ist.

Zu den externen Manifestationen des Problems gehören die Unfähigkeit, E-Mails zu erhalten, die Unfähigkeit, Verbindungen zu WWW- oder FTP-Diensten zu akzeptieren, oder eine große Anzahl von TCP-Verbindungen auf Ihrem Host im Zustand SYN_RCVD.

Schutz vor Angriffen auf Netzwerkgeräte

Geräte hinter Firewalls

Der TCP-SYN-Angriff zeichnet sich durch einen Zustrom von SYN-Paketen aus zufälligen Quell-IP-Adressen aus. Jedes Gerät hinter einer Firewall, das eingehende SYN-Pakete stoppt, ist bereits vor diesem Angriffsmodus geschützt, und es sind keine weiteren Maßnahmen erforderlich. Beispiele für Firewalls sind eine Cisco Private Internet Exchange (PIX)-Firewall oder ein Cisco Router, der mit Zugriffslisten konfiguriert ist. Beispiele zum Einrichten von Zugriffslisten auf einem Cisco Router finden Sie im Dokument Erhöhte Sicherheit in IP-Netzwerken.

Geräte, die öffentlich verfügbare Dienste anbieten (Mail-Server, öffentliche Webserver)

Es ist relativ einfach, SYN-Angriffe auf Geräte hinter Firewalls mithilfe von zufälligen IP-Adressen zu verhindern, da Sie mit Zugriffslisten den eingehenden Zugriff auf einige ausgewählte IP-Adressen explizit einschränken können. Im Falle eines öffentlichen Webservers oder Mailservers, der auf das Internet zeigt, kann jedoch nicht festgestellt werden, welche eingehenden IP-Quelladressen freundlich und unfreundlich sind. Aus diesem Grund gibt es keine eindeutige Abwehr gegen Angriffe von einer zufälligen IP-Adresse. Hosts stehen mehrere Optionen zur Verfügung:

- Vergrößern Sie die Verbindungswarteschlange (SYN ACK-Warteschlange).
- Verkürzung der Wartezeit auf den Drei-Wege-Handshake
- Verwenden Sie Software-Patches von Anbietern, um das Problem zu erkennen und zu umgehen (falls verfügbar).

Sie sollten sich an den Anbieter Ihres Hosts wenden, um zu sehen, ob dieser spezielle Patches erstellt hat, um den TCP SYN ACK-Angriff zu beheben.

Hinweis: Die Filterung von IP-Adressen auf dem Server ist ineffektiv, da ein Angreifer seine IP-Adresse ändern kann und die Adresse möglicherweise mit der eines legitimen Hosts übereinstimmt.

Verhindern, dass ein Netzwerk unbeabsichtigt einen Angriff hostet

Da der Hauptmechanismus dieses Denial-of-Service-Angriffs die Generierung von Datenverkehr ist, der von zufälligen IP-Adressen stammt, empfehlen wir, den für das Internet bestimmten Datenverkehr zu filtern. Das Grundkonzept besteht darin, Pakete mit ungültigen Quell-IP-Adressen wegzuwerfen, wenn diese das Internet betreten. Dies verhindert nicht einen Denial-of-Service-Angriff auf Ihr Netzwerk, sondern hilft Angreifern, Ihren Standort als Quelle des Angreifers auszuschließen. Darüber hinaus wird Ihr Netzwerk als Basis für diese Angriffsklasse weniger attraktiv.

Verhindern der Übertragung ungültiger IP-Adressen

Wenn Sie Pakete auf Ihren Routern filtern, die Ihr Netzwerk mit dem Internet verbinden, können Sie nur Paketen mit gültigen Quell-IP-Adressen erlauben, das Netzwerk zu verlassen und in das Internet zu gelangen.

Wenn Ihr Netzwerk beispielsweise aus dem Netzwerk 172.16.0.0 besteht und Ihr Router über eine serielle 0/1-Schnittstelle eine Verbindung zu Ihrem ISP herstellt, können Sie die Zugriffsliste wie folgt anwenden:

```
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
```

Hinweis: Die letzte Zeile der Zugriffsliste bestimmt, ob ein Datenverkehr mit einer ungültigen Quelladresse im Internet vorhanden ist. Diese Linie ist zwar nicht von entscheidender Bedeutung, trägt aber dazu bei, die Quelle möglicher Angriffe zu ermitteln.

Verhindern des Empfangs ungültiger IP-Adressen

Für ISPs, die Dienste für Endnetzwerke bereitstellen, empfehlen wir die Validierung eingehender Pakete von Ihren Clients. Dies kann durch die Verwendung von eingehenden Paketfiltern auf Ihren Grenzroutern erreicht werden.

Wenn Ihre Clients beispielsweise über eine serielle Schnittstelle mit dem Namen "serial 1/0" über die folgenden Netzwerknummern mit Ihrem Router verbunden sind, können Sie die folgende Zugriffsliste erstellen:

```
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
```

Hinweis: Die letzte Zeile der Zugriffsliste bestimmt, ob Datenverkehr mit ungültigen Quelladressen im Internet vorhanden ist. Diese Linie ist nicht entscheidend, aber sie hilft bei der Ermittlung der Quelle des möglichen Angriffs.

Dieses Thema wurde in der Mailingliste NANOG [North American Network Operator1s Group] ausführlich behandelt. Die Listenarchive finden Sie unter: http://www.merit.edu/mail.archives/nanog/index.html

Eine ausführliche Beschreibung des TCP SYN-Denial-of-Service-Angriffs und des IP-Spoofing finden Sie unter: http://www.cert.org/advisories/CA-1996-21.html

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

Zugehörige Informationen

- Technischer Support – Cisco Systems