Strategieën definiëren om te beschermen tegen TCP-blokkering van serviceaanvallen

Inhoud

Abstract

Er is een mogelijke ontkenning van een serviceaanval bij internetserviceproviders (ISP's) die netwerkapparaten herstelt.

- **TCP SYN-aanval**: Een zender geeft een volume verbindingen door dat niet kan worden voltooid. Dit veroorzaakt dat de verbindingsrijen worden vuld, waarbij de dienst aan legitieme TCP gebruikers wordt ontkend.

Dit document bevat een technische beschrijving van hoe de mogelijke TCP SYN-aanval optreedt en voorgestelde methoden voor het gebruik van Cisco IOS-software om deze te verdedigen.

Opmerking: Cisco IOS 11.3-software heeft een functie om TCP-ontkenning van serviceaanvallen actief te voorkomen. Deze optie wordt beschreven in het document waarin TCP-onderschepping wordt configureren (voorkoming van aanvallen van servicedetectie).

Voorwaarden

Vereisten

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens het te gebruiken.

Conventies

Zie de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Beschrijving van probleem

De TCP SYN-aanval

Wanneer een normale TCP verbinding begint, ontvangt een doelhost een SYN (synchroon/start)-pakket van een bronhost en stuurt een SYN ACK (synchrone erkennen) terug. De doelhost moet dan een ACK (Recognition) van de SYN ACK horen voordat de verbinding wordt gelegd. Dit wordt de "TCP-drievoudige handdruk" genoemd.

Terwijl het wachten op ACK aan SYN ACK, houdt een verbindingsrij van eindige grootte op de bestemmingshost bij het wachten op voltooiing van de verbindingen. Deze rij leegt gewoonlijk snel aangezien de ACK een paar milliseconden na de SYN ACK verwacht wordt.

De TCP SYN-aanval buit dit ontwerp door een aanvallende bronhost te hebben die TCP SYN-pakketten met willekeurige bronadressen naar een slachtoffer-host genereren. De gastheer van de slachtoffer bestemming stuurt een SYN ACK terug naar het willekeurige bronadres en voegt een ingang aan de verbindingsrij toe. Aangezien de SYN ACK voor een onjuiste of niet bestaande gastheer bestemd is, wordt het laatste deel van de "drierichtingshanddruk" nooit voltooid en blijft de ingang in de verbindingsrij tot een timer afloopt, gewoonlijk ongeveer een minuut. Door enige TCP SYN-pakketten te genereren uit willekeurige IP-adressen met een hoge snelheid, is het mogelijk de verbindingswachtrij te vullen en de TCP-services (zoals e-mail, bestandsoverdracht of WWW) aan legitieme gebruikers te ontkennen.

Er is geen makkelijke manier om de originator van de aanval te vinden omdat het IP-adres van de bron vervalst is.

De externe manifestaties van het probleem omvatten het onvermogen om e-mail te krijgen, het onvermogen om verbindingen met WW of FTP services te accepteren of een groot aantal TCP verbindingen op uw host in de staat SYN_RCVD.

Verdediging tegen aanvallen op netwerkapparaten

Apparaten achter firewalls

De TCP SYN-aanval wordt gekarakteriseerd door een toevloed van SYN-pakketten uit willekeurige bron-IP-adressen. Elk apparaat achter een firewall die de binnenkomende SYN-

pakketten stopt, is al beschermd tegen deze wijze van aanval en er is geen verdere actie nodig. Voorbeelden van firewalls omvatten een Cisco Private Internet Exchange (PIX)-firewall of een Cisco-router die met toegangslijsten is geconfigureerd. Voor voorbeelden van hoe u toegangslijsten op een router van Cisco kunt instellen, raadpleegt u het document Verhoogde beveiliging op IP-netwerken.

Apparaten die openbare diensten aanbieden (mailservers, openbare webservers)

Het verhinderen van SYN-aanvallen op apparaten achter firewalls van willekeurige IP-adressen is relatief simpel omdat u toegangslijsten kunt gebruiken om de inkomende toegang tot een paar IP-adressen expliciet te beperken. In het geval van een openbare webserver of mailserver die op het internet is gericht, is het echter onmogelijk te bepalen welke inkomende IP-bronadressen vriendelijk zijn en welke onvriendelijk zijn. Daarom is er geen duidelijke cut verdediging tegen een aanval van een willekeurig IP-adres. Er zijn verschillende opties beschikbaar voor hosts:

- Vergroot de grootte van de verbindingswachtrij (SYN ACK-wachtrij).
- Verminder de time-out die wacht op de handdruk.
- Gebruik softwarepatches van leveranciers om het probleem te detecteren en te omzeilen (indien beschikbaar).

U dient contact op te nemen met uw host-verkoper om te zien of zij specifieke patches hebben gemaakt voor de TCP SYN ACK-aanval.

Opmerking: Het filteren van IP adressen op de server is ineffectief aangezien een aanvaller zijn IP-adres kan variëren en het adres kan al dan niet hetzelfde zijn als dat van een legitieme host.

Een netwerk beletten dat je een aanval op onbedoelde wijze organiseert

Aangezien een primair mechanisme van deze ontkenning van de dienstaanval de generatie van verkeer is die uit willekeurige IP adressen komt, adviseren wij het filtreren verkeer dat voor het Internet bestemd is. Het basisconcept is om pakketten met ongeldige bron-IP adressen weg te gooien wanneer zij het internet betreden. Dit voorkomt geen ontkenning van de dienstaanval op uw netwerk, maar zal helpen aangevallen partijen uw plaats als bron van de aanvaller uit te sluiten. Bovendien maakt het uw netwerk minder aantrekkelijk als basis voor deze klasse van aanvallen.

Vermijding van verzending van ongeldige IP-adressen

Door pakketten te filteren op uw routers die uw netwerk met het internet verbinden, kunt u alleen pakketten met geldige bron-IP-adressen toestaan om uw netwerk te verlaten en op het internet te komen.

Als uw netwerk bijvoorbeeld bestaat uit netwerk 172.16.0.0 en uw router met uw ISP verbindt met behulp van een seriële 10/1 interface, kunt u de volgende toegangslijst toepassen:

```
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
```

Opmerking: de laatste regel van de toegangslijst bepaalt of er verkeer is met een ongeldig bronadres dat het internet invoert. Het is niet cruciaal om deze lijn te hebben, maar het zal de bron van de mogelijke aanvallen helpen vinden.

Het voorkomen van ontvangst van ongeldige IP-adressen

Voor ISP's die service bieden aan eindgebruikers, raden we de validatie van inkomende pakketten van uw klanten sterk aan. Dit kan worden bereikt door het gebruik van inkomende pakketfilters in uw grensrouters.

Als uw klanten bijvoorbeeld de volgende netwerknummers hebben die met uw router via een seriële interface met de naam "seriële 1/0" zijn verbonden, kunt u de volgende toegangslijst maken:

```
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
```

Opmerking: de laatste regel van de toegangslijst bepaalt of er verkeer is met ongeldige bronadressen die het internet invoeren. Het is niet van cruciaal belang om deze lijn te hebben, maar het zal de bron van de mogelijke aanval helpen vinden.

Dit onderwerp is in detail besproken op de mailinglijst van NANOG [North American Network Operators1s Group]. De lijsten zijn te vinden op:
http://www.merit.edu/mail.archives/nanog/index.html

Voor een gedetailleerde beschrijving van de TCP SYN-ontkenning van de dienstaanval en IP-spoofing, zie: http://www.cert.org/advisories/CA-1996-21.html

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

Gerelateerde informatie

- Technische ondersteuning - Cisco-systemen