Karakterisering en overtrekken van pakketoverstromingen met Cisco-routers

Inhoud

Inleiding

De aanvallen van Denial of Service (DoS) worden veel op het internet gebruikt. De eerste stap die je gebruikt om op zo'n aanval te reageren is om uit te vinden wat het soort aanval is. Veel van de meest gebruikte DoS-aanvallen zijn gebaseerd op grote bandbreedte-overstromingen of op andere repetitieve stromen van pakketten.

De pakketten in veel DoS aanvalstreams kunnen worden geïsoleerd wanneer u ze vergelijkt met de items van Cisco IOS® de software toegangslijst. Dit is waardevol voor het filteren van aanvallen. Het is ook handig voor wanneer u onbekende aanvallen karakteriseert en voor wanneer u "gespoofde" pakketstromen terugvindt naar hun echte bronnen.

De routerfuncties van Cisco zoals debug loggen en IP accounting kunnen soms voor gelijkaardige doeleinden gebruikt worden, vooral met nieuwe of ongebruikelijke aanvallen. Maar met recente versies van Cisco IOS-software zijn toegangslijsten en vastlegging van een toegangslijst de functies in eerste instantie voor het kenmerken en overtrekken van gewone aanvallen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

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

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

De meest voorkomende DOS-aanvallen

Er is een grote verscheidenheid aan DOS-aanvallen mogelijk. Zelfs als u aanvallen negeert die softwarebugs gebruiken om systemen met relatief weinig verkeer te sluiten, blijft het feit dat elk IP-pakket dat over het netwerk kan worden verzonden kan worden gebruikt om een overstroomde DoS-aanval uit te voeren. Wanneer u wordt aangevallen, moet u altijd rekening houden met de mogelijkheid dat wat u ziet iets is dat niet in de gebruikelijke categorieën valt.

Onder voorbehoud van dat voorbehoud is het echter ook goed te bedenken dat vele aanslagen op elkaar lijken. Aanvallers kiezen voor gemeenschappelijke explosies omdat ze bijzonder effectief zijn, vooral moeilijk te traceren, of omdat er gereedschappen beschikbaar zijn. Veel DoS-aanvallers hebben niet de vaardigheid of de motivatie om hun eigen gereedschap te maken en gebruiken programma's die op het internet gevonden worden. Deze tools vallen meestal in en buiten de mode.

Ten tijde van dit schrijven, in juli 1999, hebben de meeste klantverzoeken om Cisco ondersteuning betrekking op de "smurf"-aanval. Deze aanslag heeft twee slachtoffers: een " uiteindelijk doel " en een " reflector " . De aanslagpleger stuurt een stimulusstroom van de verzoeken van de echo van ICMP ("pings") naar het uitzending adres van reflector Subnet. De bronadressen van deze pakketten worden vervalst om het adres van het uiteindelijke doel te zijn. Voor elk pakket dat door de aanslagpleger wordt verzonden, reageren vele gastheren op reflectornet. Hierdoor wordt het uiteindelijke doel overspoeld en wordt de bandbreedte van beide slachtoffers verspild.

Een soortgelijke aanval, die "fraggle" wordt genoemd, gebruikt op dezelfde manier gerichte uitzendingen, maar gebruikt UDP echo-verzoeken in plaats van CMP-echo-verzoeken (Internet Control Message Protocol). Fragle bereikt gewoonlijk een kleinere versterkingsfactor dan smurf, en is veel minder populair.

Smurf-aanvallen worden gewoonlijk opgemerkt omdat een netwerklink wordt overbelast. Een volledige beschrijving van deze aanvallen en van de maatregelen van de verdediging is te vinden op de pagina Informatie over de voorkoming van aanvallen op servicedetecten.

Een andere gemeenschappelijke aanval is de overstroming van SYN, waarin een doelmachine overstroomd wordt met TCP-verbindingsverzoeken. De bronadressen en de bron TCP poorten van het verbindingsverzoek worden gerandomiseerd. Het doel is om de doelhost te dwingen

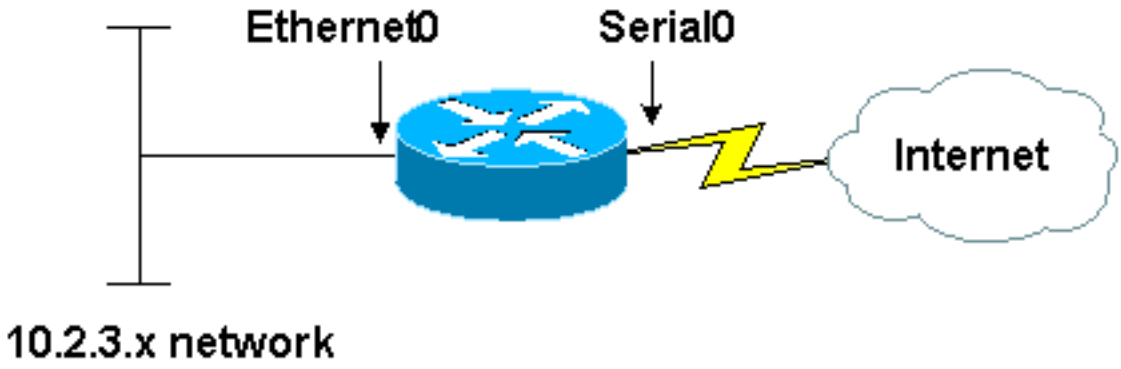
overheidsinformatie te bewaren voor veel verbindingen die nooit zijn voltooid.

De aanvallen van de SYN-overstroming worden gewoonlijk opgemerkt omdat de doelgastheer (vaak een HTTP of MTP-server) extreem langzaam wordt, crashes of hangs. Het is ook mogelijk voor het verkeer dat van de doelgastheer terugkeert om problemen op routers te veroorzaken. Dit is omdat dit terugkeerverkeer naar de gerandomiseerde bronadressen van de originele pakketten gaat, het de localiteitseigenschappen van "echt"IP verkeer niet heeft, en routekaarten kan overlopen. Op Cisco routers, manifesteert dit probleem zich vaak in de router die geen geheugen meer heeft.

Samen nemen de overstromingen van Ssmurf en SYN het grootste deel van de overstroomde DoS-aanvallen voor hun rekening die aan Cisco worden gemeld, en is het snel herkennen ervan zeer belangrijk. Beide aanvallen (zowel als sommige aanvallen van de "tweede kant", zoals pingende overstromingen) worden makkelijk herkend wanneer u Cisco toegangslijsten gebruikt.

Een DOS-toegangslijst voor tekens

Stel een router met twee interfaces in. Ethernet 0 wordt aangesloten op een intern LAN bij een bedrijf of kleine ISP. Seriële modus 0 biedt een internetverbinding via een upstream ISP. De invoerpakketsnelheid met serie 0 wordt "gekoppeld" aan de volledige bandbreedte en hosts op de LAN-run langzaam, crasht, opgehangen of toont andere tekenen van een DoS-aanval. De kleine plaats waar de router aansluit heeft geen netwerkanalyzer, en de mensen daar hebben weinig of geen ervaring in het lezen van de sporen van de analyzer zelfs als de sporen beschikbaar zijn.



Ga er nu van uit dat u een toegangslijst toepast zoals deze uitvoer aantoont:

```
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

Deze lijst filtert geen enkel verkeer uit; alle inzendingen zijn vergunningen . Omdat de lijst echter pakketten op een handige manier categoriseert, kan de lijst tegelijkertijd worden gebruikt om alle drie typen aanvallen te diagnosticeren: overstroming, SYN-overstroming en een strijd.

Smurf Ultiem doel

Als u de opdracht **toegang-lijst tonen** geeft, ziet u uitvoer gelijkend op dit:

```
Extended IP access list 169
    permit icmp any any echo (2 matches)
    permit icmp any any echo-reply (21374 matches)
    permit udp any any eq echo
    permit udp any eq echo any
    permit tcp any any established (150 matches)
    permit tcp any any (15 matches)
    permit ip any any (45 matches)
```

Het meeste verkeer dat op de seriële interface wordt ontvangen bestaat uit de antwoordpakketten van de echo van ICMP. Dit is waarschijnlijk de handtekening van een smurf-aanval, en onze site is het ultieme doelwit, in plaats van de reflector. U kunt meer informatie over de aanval verzamelen wanneer u de toegangslijst bekijkt, zoals deze output toont:

```
interface serial 0
no ip access-group 169 in

no access-list 169
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply log-input
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

De verandering hier is dat het **loginginput** sleutelwoord wordt toegevoegd aan de ingang van de toegangslijst die het verdachte verkeer aanpast. (Cisco IOS-softwarereleases eerder dan 11.2 heeft dit trefwoord niet. Gebruik in plaats daarvan het sleutelwoord "**log**".) Dit veroorzaakt de router om informatie over pakketten in te loggen die de lijstingang overeenkomen. Als u ervan uitgaat dat **gebufferde houtkap** is ingesteld, kunt u de berichten zien die resulteren met de opdracht Logboek (het kan een tijdje duren voordat de berichten zich ophopen vanwege snelheidsbeperking). De berichten lijken op deze uitvoer:

```
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.72
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.154
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.15
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
```

```
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.59
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.82
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.56
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.84
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.15
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.33
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
```

De bronadressen van de echo antwoordpakketten worden geclusterd in adresprefixes 192.168.212.0/24, 192.168.45.0/24, en 172.16.132.0/24 (privé adressen in de netwerken 192.168.x.x en 172.16.x.x zouden niet op internet zijn; dit is een voorbeeld uit een laboratorium .) Dit is heel typisch voor een smurf-aanval, en de bronadressen zijn de adressen van de smurf-reflectoren. Als je de eigenaars van deze adresblokken opzoekt in de juiste Internet "Whis"-databases, kun je de beheerders van deze netwerken vinden en om hun hulp vragen in het omgaan met de aanval.

Het is belangrijk om op dit moment in een klein incident te bedenken dat deze reflectoren medeschuldig zijn en geen aanvallers. Het is extreem zeldzaam voor aanvallers om hun eigen bronadressen op IP-pakketten te gebruiken in elke overstroming van DoS, en onmogelijk voor hen om dit te doen in een werkende aanslag op de smurf. Ieder adres in een overstromingspakketje moet verondersteld worden volledig vervalst te zijn, of het adres van een slachtoffer van een of ander soort. De meest productieve benadering van het uiteindelijke doel van een aanslag op een hinderpaal is om contact op te nemen met de reflectoren, of om hen te vragen hun netwerken aan te passen om de aanval te stoppen, of om hun hulp te vragen bij het traceren van de stimuleringsstroom.

Omdat de schade aan het uiteindelijke doel van een zelfmoordaanslag gewoonlijk wordt veroorzaakt door het overladen van de inkomende link van het internet, is er vaak geen andere reactie dan contact opnemen met de reflectoren. Tegen de tijd dat de pakketten in een machine onder controle van het doel aankomen, is het grootste deel van de schade reeds gedaan.

Een stoplap maatregel is de stroomopwaartse netwerkprovider te vragen alle antwoorden van de ICMP-echo te filteren, of alle antwoorden van de ICMP-echo van specifieke reflectoren. Het wordt niet aanbevolen dit soort filter permanent in te zetten. Zelfs voor een tijdelijk filter mogen alleen de echo-antwoorden worden gefilterd, niet alle ICMP-pakketten. Een andere mogelijkheid is om de upstream provider te hebben om Quality-of-Service- en snelheidsbeperkende functies te gebruiken om de bandbreedte die beschikbaar is voor echo-antwoorden te beperken. Een redelijke bandbreedte-beperking kan onbeperkt blijven. Beide benaderingen hangen af van de

uitrusting van de stroomopwaarts gelegen leverancier die over de nodige capaciteit beschikt, en soms is die capaciteit niet beschikbaar.

Smurf-reflector

Als het inkomende verkeer uit echo-verzoeken bestaat in plaats van echo-antwoorden (met andere woorden als het eerste toegangslijstje en niet het tweede, veel meer wedstrijden telde dan redelijkerwijs verwacht kon worden), zou u een smurf-aanval vermoeden waarin het netwerk als reflector werd gebruikt, of mogelijk een eenvoudige pingoverstroming. In beide gevallen, als de aanval een succes is, zou u verwachten dat de vertrekkende kant van de serielijn, evenals de inkomende kant, wordt opgeschoven. Sterker nog, door de versterkingsfactor zou je verwachten dat de vertrekkende kant nog meer overbelast is dan de inkomende kant.

Er zijn verschillende manieren om de zelfmoordaanslag te onderscheiden van de eenvoudige pingdij:

- Smurf-stimuluspakketten worden naar een gericht uitgezonden adres gestuurd in plaats van naar een éénmailadres, terwijl normale ping-overstromingen vrijwel altijd gebruikmaken van eensten. U kunt de adressen zien die het **logbestand-input** sleutelwoord gebruiken in de juiste toegangslijst ingang.
- Als u als een reflector van het klein wordt gebruikt, is er een disproportioneel aantal output uitzendingen in de **show** interface display op Ethernet aan de kant van het systeem, en meestal een disproportioneel aantal uitzendingen verzonden in de **show ip verkeer**. Een standaard ping flood verhoogt niet het achtergronduitzendingsverkeer.
- Als je gebruikt wordt als een reflector op een klein dak, gaat er meer verkeer naar het internet dan verkeer dat binnenkomt van het internet. In het algemeen is er meer uitvoerpakketten dan invoerpakketten op de seriële interface. Zelfs als de stimulusstroom de input interface volledig vult, is de responsstroom groter dan de stimulusstroom en worden pakketdruppels geteld.

Een kleine reflector heeft meer opties dan het uiteindelijke doel van een smurf aanval. Als een reflector kiest om de aanval te sluiten, volstaat het juiste gebruik van **geen ip geregisseerde uitzending** (of gelijkwaardige niet-IOS opdrachten) gewoonlijk. Deze opdrachten horen bij elke configuratie thuis, zelfs als er geen actieve aanval is. Raadpleeg voor meer informatie over de preventie van het gebruik van uw Cisco-apparatuur in een Cisco-aanval op Cisco-routers voor het verbeteren van de beveiliging. Raadpleeg voor meer algemene informatie over kleinere aanvallen in het algemeen en voor informatie over de beveiliging van niet-Cisco-apparatuur de informpagina Denial of Service Attacks.

Een kleine reflector is één stap dichter bij de aanvaller dan het uiteindelijke doelwit is, en verkeert daarom in een betere positie om de aanval te traceren. Als u ervoor kiest om de aanval te traceren, moet u met de betrokken ISP's werken. Als u actie wilt ondernemen wanneer u de sporen heeft voltooid, moet u samenwerken met de bevoegde rechtshandhavingsinstanties. Als u een aanval probeert op te sporen, wordt aanbevolen dat u zo snel mogelijk de politie erbij betrekt. Zie het gedeelte Tracing voor technische informatie over het traceren van overstromingen.

fragmenteren

De fraaie aanval is analoog aan de zelfmoordaanslag, behalve dat de UDP-echo-verzoeken worden gebruikt voor de stimulusstroom in plaats van de echo-verzoeken van het ICMP. De derde en vierde regels van de toegangslijst identificeren de aanvallen van de strijd. De juiste reactie voor de slachtoffers is hetzelfde, behalve dat de UDP-echo in de meeste netwerken een minder

belangrijke dienst is dan het ICMP-echo. Daarom kunt u deze volledig uitschakelen met minder negatieve gevolgen.

SYN-overstromingen

De vijfde en zesde regel van de toegangslijst zijn:

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
```

De eerste van deze lijnen past elk TCP-pakket aan met het ACK-bit dat is ingesteld. Voor onze doeleinden betekent dit dat het elk pakje aanpast dat geen TCP SYN is. De tweede lijn past slechts pakketten aan die TCP SYNs zijn. Een overstroming van SYN wordt gemakkelijk herkend vanuit de tellers in deze lijst. In normaal verkeer overtreffen niet-SYN TCP pakketten SYNs door minstens een factor van twee, en meestal meer zoals vier of vijf. Bij een SYN-overstroming overtreffen SYN's meestal meerdere niet-SYN TCP-pakketten.

De enige niet-aanvalsvoorwaarde die tot deze handtekening leidt is een enorme overvloed aan echte verbindingsverzoeken. Over het algemeen zal een dergelijke overbelasting niet onverwachts ontstaan en zal er niet zoveel SYN-pakketten bij betrokken zijn als een echte overstroming van SYN. Ook bevatten SYN-overstromingen vaak pakketten met volledig ongeldige bronadressen: met behulp van het sleutelwoord **loginvoer**, is het mogelijk om te zien of de verbindingsverzoeken van dergelijke adressen komen.

Er is een aanval, een ‘proces-tafelaanval' genoemd, die enigszins lijkt op de SYN-overstroming. Bij de aanval van de procestabel worden de TCP verbindingen voltooid, en toegestaan om uit te stappen zonder verder protocolverkeer, terwijl in de overstroming van SYN alleen de eerste verbindingsverzoeken worden verzonden. Omdat een aanval van de procestabel de voltooiing van de TCP eerste handdruk vereist, moet het over het algemeen gelanceerd worden met het gebruik van het IP adres van een echte machine waartoe de aanvaller toegang heeft (gewoonlijk gestolen toegang). De de tabelaanvallen van het proces zijn daarom gemakkelijk te onderscheiden van de SYN-overstromingen door het gebruik van pakketvastlegging. Alle SYN's in een procestabel aanval komen van één of een paar adressen, of hooguit van één of een paar subnetten.

De responsopties voor de slachtoffers van SYN-overstromingen zijn zeer beperkt. Het systeem dat wordt aangevallen is gewoonlijk een belangrijke dienst, en het blokkeren van de toegang tot het systeem bereikt gewoonlijk wat de aanvaller wil. Veel router- en firewallproducten, waaronder Cisco's, hebben functies die kunnen worden gebruikt om de impact van SYN-overstromingen te verminderen. Maar de effectiviteit van deze functies hangt af van het milieu. Raadpleeg voor meer informatie de documentatie voor de Cisco IOS Firewallfunctieset, de documentatie voor de Cisco IOS TCP-onderschepping en verbetering van beveiliging op Cisco-routers.

Het is mogelijk om SYN-overstromingen te traceren, maar het traceringsproces vereist de hulp van elke ISP langs het pad van de aanvaller naar het slachtoffer. Als u wilt proberen een SYN-overstroming op te sporen, neem dan vroeg contact op met de politie en werk met uw eigen serviceprovider. Zie het gedeelte overtrekken van dit document voor meer informatie over overtrekken met behulp van Cisco-apparatuur.

Overige aanvallen

Als u gelooft dat u onder een aanval staat en als u die aanval kunt karakteriseren met behulp van IP bron- en doeladressen, protocolnummers en poortnummers, kunt u toegangslijsten gebruiken

om uw hypothese te testen. Maak een ingang van de toegangslijst die het verdachte verkeer aanpast, pas het op een aangewezen interface toe, en bekijk de lucifers of log het verkeer.

Vastlegging en aftellen

De teller op een toegangslijst telt alle overeenkomsten tegen die ingang. Als u een toegangslijst op twee interfaces toepast, zijn de tellingen die u ziet geaggregeerd tellen.

De lijst met toegangslijsten geeft niet elk pakket weer dat overeenkomt met een ingang. Vastlegging is aan de snelheid gebonden om overbelasting door CPU te voorkomen. Wat de houtkap laat zien is een redelijk representatief monster, maar geen volledig pakketspoor. Vergeet niet dat er pakketten zijn die u niet ziet.

In sommige softwareversies werkt het loggen van de toegangslijst slechts in bepaalde switchmodi. Als een toegangslijst een hoop overeenkomsten telt, maar logt niets, probeer dan het routecache te wissen om pakketten te forceren om te worden verwerkt geschakeld. Wees voorzichtig als u dit doet op zwaar geladen routers met veel interfaces. Veel verkeer kan vallen terwijl het cache opnieuw wordt opgebouwd. Gebruik Cisco Express doorsturen wanneer dat mogelijk is.

Toegangslijsten en houtkap hebben een impact op de prestaties, maar niet een groot effect. Wees voorzichtig met routers die bij meer dan 80 procent CPU-belasting werken, of wanneer u toegangslijsten toepast op zeer snelle interfaces.

overtrekken

De bronadressen van de pakketten van Dos worden bijna altijd ingesteld op waarden die niets met de aanvallers zelf te maken hebben. Daarom zijn ze niet nuttig bij het identificeren van de aanvallers. De enige betrouwbare manier om de bron van een aanval te identificeren is het terug hop-voor-hop door het netwerk te vinden. Dit proces betreft de configuratie van routers en het onderzoek van loginformatie. Er is samenwerking nodig tussen alle netwerkoperatoren op het pad van de aanvaller naar het slachtoffer. Om ervoor te zorgen dat deze samenwerking gewoonlijk plaatsvindt, moeten de wetshandhavingsinstanties, die ook betrokken moeten worden bij de bestrijding van de aanvaller, worden betrokken.

Het traceringsproces voor Dos-overstromingen is relatief eenvoudig. Om te beginnen bij een router (genaamd "A") die overstromingsverkeer heeft, identificeert men de router (genaamd "B") waarvan A het verkeer ontvangt. Een logt dan in B en vindt de router (genaamd "C") waarvan B het verkeer ontvangt. Dit duurt voort totdat de uiteindelijke bron is gevonden.

Bij deze methode zijn verschillende complicaties opgetreden, die in deze lijst worden beschreven:

- De 'ultieme bron' kan een computer zijn die door de aanvaller gecompromitteerd is, maar die in werkelijkheid eigendom is van en bestuurd wordt door een ander slachtoffer. In dit geval is het overtrekken van de DoS-overstroming slechts de eerste stap.
- De aanvallers weten dat ze getraceerd kunnen worden en zetten hun aanvallen gewoonlijk slechts voor beperkte tijd voort. Er is misschien niet genoeg tijd om de overstroming echt op te sporen.
- Aanvallen kunnen uit meerdere bronnen komen, vooral als de aanvaller relatief geavanceerd is. Het is belangrijk te proberen zoveel mogelijk bronnen te identificeren.
- Communicatieproblemen vertragen het overtrekken. Vaak beschikken één of meer van de

betrokken netwerkexploitanten niet over voldoende gekwalificeerd personeel.
- Juridische en politieke bezwaren maken het wellicht moeilijk om tegen aanvallers op te treden, zelfs als die wel gevonden worden.

De meeste pogingen om DOS-aanvallen te traceren mislukken. Hierom proberen veel netwerkexploitanten niet eens een aanval te traceren, tenzij ze onder druk worden geplaatst. Veel anderen sporen alleen "ernstige" aanvallen aan, met verschillende definities van wat "ernstig" is. Sommigen helpen alleen met een spoor als het gaat om rechtshandhaving.

Overtrekken met "loginvoer"

Als u ervoor kiest om een aanval te overtrekken die door een router van Cisco passeert, is de meest effectieve manier om dit te doen een ingang van de toegangslijst te bouwen die het aanvalsverkeer aanpast, het **logbestand-input** sleutelwoord eraan toe te voegen, en de toegangslijst toe te passen die op de interface loopt waardoor de aanvalsstroom naar zijn ultieme doel wordt verzonden. De logitems die door de toegangslijst worden geproduceerd, identificeren de router-interface waardoor het verkeer aankomt, en, als de interface een multi-point verbinding is, geven Layer 2-adres van het apparaat waarvan het ontvangen is. Layer 2 adres kan dan worden gebruikt om de volgende router in de keten te identificeren, door bijvoorbeeld de **opdracht** *IP-mac-adres* te gebruiken.

SYN Flood

U kunt een gelijkaardige toegangslijst maken als u een SYN-overstroming wilt overtrekken:

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any host victim-host log-input
access-list 169 permit ip any any
```

Dit logt alle SYN-pakketten in die voor de doelhost bestemd zijn, inclusief legitieme SYNs. Om het meest waarschijnlijke pad naar de aanslagpleger te identificeren, onderzocht u de logingangen in detail. In het algemeen komt de bron van de overstroming overeen met het grootste aantal pakketten. De bron-IP-adressen betekenen niets. U zoekt broninterfaces en bron-MAC-adressen. Soms is het mogelijk om overstromingspakketten van legitieme pakketten te onderscheiden omdat pakketten van overstromingen ongeldige bronadressen kunnen hebben. Elk pakket waarvan het bronadres ongeldig is, zal waarschijnlijk deel uitmaken van de overstroming.

De overstroming kan uit meerdere bronnen komen, hoewel dit relatief ongebruikelijk is voor SYN-overstromingen.

Smurf Stimulus

Om een smurf stimulusstroom te traceren gebruikt u een toegangslijst zoals deze:

```
access-list 169 permit icmp any any echo log-input
access-list 169 permit ip any any
```

Merk op dat het eerste punt zich niet beperkt tot pakketten die bestemd zijn voor het reflectoradres. De reden hiervoor is dat de meeste smurf-aanvallen meerdere reflectornetwerken gebruiken. Als u niet in contact bent met het uiteindelijke doel, kent u mogelijk niet alle reflectoradressen. Als je spoor dichter bij de bron van de aanval komt, kun je beginnen met het zien van verzoeken van echo om naar meer en meer bestemmingen te gaan. dat is een goed teken .

Als u echter met veel ICMP-verkeer te maken hebt, kan dit te veel loginformatie genereren om gemakkelijk te lezen. Als dit gebeurt, kunt u het doeladres beperken tot een van de reflectoren die bekend is om te worden gebruikt. Een andere nuttige tactiek is het gebruik van een artikel dat gebruik maakt van het feit dat netwerkmaskers van 255.255.255.0 heel gewoon zijn op het internet. En door de manier waarop aanvallers kleine reflectoren vinden, zullen de reflectoradressen die gebruikt worden voor smurf-aanvallen nog waarschijnlijker op dat masker passen. Host adressen die eindigen op 0 of 0,255 zijn zeer ongewoon in het internet. Daarom kunt u een relatief specifieke herkenner voor smurf-stimulusstromen bouwen zoals deze uitvoer laat zien:

```
access-list 169 permit icmp any host known-reflector echo log-input access-list 169 permit icmp
any 0.0.0.255 255.255.255.0 echo log-input access-list 169 permit icmp any 0.0.0.0 255.255.255.0
echo log-input access-list 169 permit ip any any
```

Met deze lijst kunt u veel van de "lawaai"-pakketten uit uw logbestand verwijderen, terwijl u nog steeds een goede kans hebt om extra stimulusstromen te zien terwijl u dichter bij de aanvaller komt.

Overtrekken zonder "loginvoer"

Het sleutelwoord **log-input** bestaat in Cisco IOS-softwarereleases 11.2 en later, en in bepaalde op 11.1 gebaseerde software die specifiek voor de serviceprovider-markt is gemaakt. In oudere softwarereleases wordt dit trefwoord niet ondersteund. Als u een router met oudere software gebruikt, hebt u drie opties:

- Maak een toegangslijst zonder loggen, maar met ingangen die overeenkomen met het verdachte verkeer. Pas de lijst op de *ingangszijde* van elke interface toe en kijk naar de tellers. Zoek naar interfaces met hoge matrijzen. Deze methode heeft een zeer kleine prestatiekloof en is goed voor de identificatie van broninterfaces. Zijn grootste nadeel is dat het geen link-layer bronadressen geeft en daarom vooral nuttig is voor point-to-point lijnen.
- Maak toegangslijsten met het **logtrefwoord** (in plaats van **loginvoer**). Pas de lijst opnieuw toe aan de inkomende kant van elke interface. Deze methode geeft nog steeds geen bron-MAC-adressen, maar kan handig zijn om IP-gegevens te zien. Bijvoorbeeld, om te verifiëren dat een pakketstroom echt deel van een aanval uitmaakt. De impact op prestaties kan matig tot hoog zijn en nieuwere software presteert beter dan oudere software.
- Gebruik de opdracht **ip-pakketdetails** debug om informatie over pakketten te verzamelen. Deze methode geeft MAC-adressen, maar kan een ernstige impact hebben op de prestaties. Het is makkelijk om een fout te maken met deze methode en een router onbruikbaar te maken. Als u deze methode gebruikt, zorg ervoor dat de router het aanvalverkeer in snelle, autonome of optimale modus switches. Gebruik een toegangslijst om het debuggen te beperken tot alleen de informatie die u echt nodig hebt. Eerst informatie over het foutoptreden aan de lokale logbuffer, maar zet de houtkap van debug informatie aan de sessies van het telnet en aan de console uit. Indien mogelijk, schik voor iemand om fysiek in de buurt van de router te zijn, zodat het op stroom kan worden aangesloten zoals nodig.Onthoud dat de **debug IP-pakketopdracht** geen informatie over snel geschakelde pakketten toont. U moet de **heldere ip cache** opdracht uitgeven om informatie op te nemen. Elke duidelijke opdracht geeft u een of twee pakketten debug-uitvoer.

Gerelateerde informatie

- Kerberos
- Technische ondersteuning en documentatie – Cisco Systems