Charakterisierung und Verfolgung von Paketfluten mit Cisco Routern

Inhalt

Einführung

Denial of Service (DoS)-Angriffe sind im Internet üblich. Der erste Schritt, mit dem Sie auf einen solchen Angriff reagieren, besteht darin, herauszufinden, welche Art von Angriff er ist. Viele der häufig verwendeten DoS-Angriffe basieren auf Paketfluten mit hoher Bandbreite oder auf anderen sich wiederholenden Paketströmen.

Die Pakete in vielen DoS-Angriffs-Streams können isoliert werden, wenn Sie sie mit den Zugriffslisteneinträgen in der Cisco IOS®-Software abgleichen. Dies ist für das Herausfiltern von Angriffen nützlich. Sie ist auch nützlich, wenn Sie unbekannte Angriffe charakterisieren und wenn Sie "gefälschte" Paket-Streams auf ihre eigentlichen Quellen zurückverfolgen.

Cisco Router-Funktionen wie Debug-Protokollierung und IP-Accounting können manchmal für ähnliche Zwecke verwendet werden, insbesondere bei neuen oder ungewöhnlichen Angriffen. Bei den aktuellen Versionen der Cisco IOS-Software sind Zugriffslisten und die Protokollierung von Zugriffslisten jedoch die wichtigsten Funktionen, wenn Sie häufige Angriffe charakterisieren und verfolgen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Die häufigsten DoS-Angriffe

Eine Vielzahl von DoS-Angriffen ist möglich. Selbst wenn Sie Angriffe ignorieren, bei denen Software-Bugs zum Herunterfahren von Systemen mit relativ geringem Datenverkehr verwendet werden, bleibt die Tatsache bestehen, dass jedes IP-Paket, das über das Netzwerk gesendet werden kann, zum Ausführen eines Flooding-DoS-Angriffs verwendet werden kann. Wenn Sie angegriffen werden, müssen Sie immer die Möglichkeit in Betracht ziehen, dass das, was Sie sehen, etwas ist, das nicht in die üblichen Kategorien fällt.

Vorbehaltlich dieser Vorbehalte ist es jedoch auch gut daran zu denken, dass viele Angriffe ähnlich sind. Angreifer entscheiden sich für häufige Exploits, da sie besonders effektiv sind, besonders schwer nachzuvollziehen sind oder Tools zur Verfügung stehen. Viele DoS-Angreifer verfügen nicht über die Fähigkeiten oder die Motivation, eigene Tools zu erstellen und im Internet gefundene Programme zu verwenden. Diese Tools neigen dazu, in die Mode zu fallen und aus der Mode zu gehen.

Zum Zeitpunkt der Veröffentlichung dieses Dokuments im Juli 1999 waren die meisten Kundenanfragen bei Cisco mit dem "smurf"-Angriff verbunden. Dieser Angriff hat zwei Opfer: ein "ultimatives Ziel" und ein "Reflektor". Der Angreifer sendet einen Stimulusstrom von ICMP-Echoanfragen ("Pings") an die Broadcast-Adresse des Reflektor-Subnetzes. Die Quelladressen dieser Pakete werden als Adresse des endgültigen Ziels gefälscht. Für jedes vom Angreifer gesendete Paket reagieren viele Hosts im Reflektor-Subnetz. Dadurch wird das ultimative Ziel überflutet und Bandbreite für beide Opfer verschwendet.

Bei einem ähnlichen Angriff, der als "Fraggle" bezeichnet wird, werden auf die gleiche Weise gezielte Broadcasts verwendet, aber anstelle von ICMP-Echoanfragen (Internet Control Message Protocol) werden UDP-Echoanfragen verwendet. Fraggle erzielt in der Regel einen kleineren Verstärkungsfaktor als smurf und ist viel weniger beliebt.

Smurf-Angriffe werden in der Regel bemerkt, weil eine Netzwerkverbindung überlastet wird. Eine vollständige Beschreibung dieser Angriffe und der Abwehrmaßnahmen finden Sie auf der Seite "Informationen zu Denial of Service Attacks" (Informationen zu DoS-Angriffen).

Ein weiterer häufiger Angriff ist die SYN-Flood, bei der ein Zielcomputer mit TCP-Verbindungsanforderungen überflutet wird. Die Quell- und Quell-TCP-Ports der

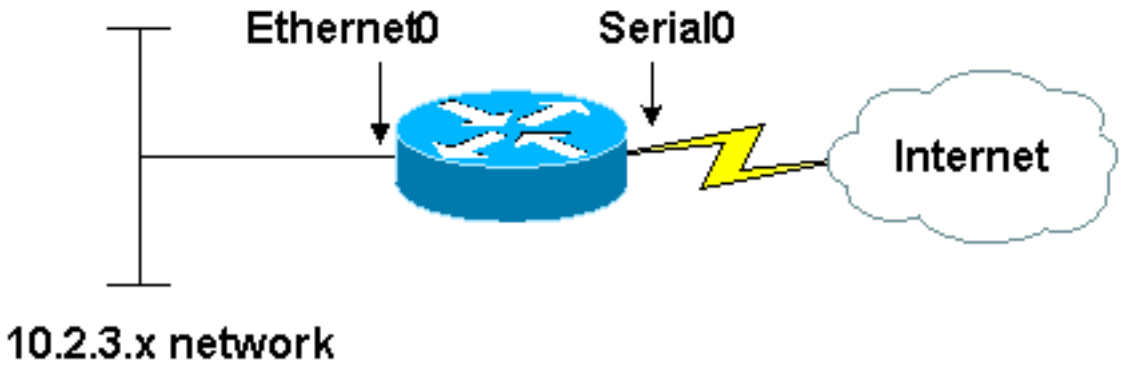
Verbindungsanforderungspakete werden randomisiert. Der Zweck besteht darin, den Ziel-Host zu zwingen, Zustandsinformationen für viele Verbindungen beizubehalten, die nie abgeschlossen wurden.

SYN-Flood-Angriffe werden in der Regel bemerkt, weil der Ziel-Host (häufig ein HTTP- oder SMTP-Server) extrem langsam, abstürzt oder stürzt. Es ist auch möglich, dass der vom Zielhost zurückgegebene Datenverkehr Probleme bei Routern verursacht. Der Grund hierfür ist, dass dieser Rückverkehr an die randomisierten Quelladressen der ursprünglichen Pakete geleitet wird, dass ihm die Lokalisierungseigenschaften des "echten" IP-Datenverkehrs fehlen und dass er Routen-Caches überfluten kann. Bei Cisco Routern tritt dieses Problem häufig auf, wenn der Speicher des Routers knapp ist.

Gemeinsam bilden SMURF- und SYN-Flood-Angriffe den Großteil der Flooding-DoS-Angriffe, die Cisco gemeldet wurden. Eine schnelle Erkennung ist daher sehr wichtig. Beide Angriffe (wie auch einige "Second-Tier"-Angriffe, wie Ping-Floods) können problemlos erkannt werden, wenn Sie Cisco Zugriffslisten verwenden.

Zugriffsliste für DoS-Zeichen

Stellen Sie sich einen Router mit zwei Schnittstellen vor. Ethernet 0 ist mit einem internen LAN in einem Unternehmen oder einem kleinen ISP verbunden. Serial 0 stellt eine Internetverbindung über einen Upstream-ISP bereit. Die Eingangspaketrate für serielle 0 wird an der vollen Verbindungsbandbreite "gekoppelt", und Hosts im LAN laufen langsam, stürzen ab, hängen oder zeigen andere Anzeichen für einen DoS-Angriff. Der kleine Standort, an dem der Router eine Verbindung herstellt, verfügt über keinen Netzwerkanalysegerät, und die dort befindlichen Personen haben kaum oder keine Erfahrung im Lesen von Analyzerfolgen, selbst wenn die Traces verfügbar sind.



Gehen Sie jetzt davon aus, dass Sie eine Zugriffsliste anwenden, wie diese Ausgabe zeigt:

```
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
```

Diese Liste filtert keinen Datenverkehr heraus. alle Einträge sind zulässig. Da die Liste Pakete jedoch sinnvoll kategorisiert, kann sie zur vorläufigen Diagnose aller drei Angriffstypen verwendet werden: smurf, SYN-Floods und Fraggle.

SMURF Ultimate-Ziel

Wenn Sie den Befehl **show access-list** ausgeben, wird die Ausgabe ähnlich wie folgt angezeigt:

```
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)
```

Der Großteil des an der seriellen Schnittstelle ankommenden Datenverkehrs besteht aus ICMP-Echo-Antwortpaketen. Dies ist wahrscheinlich die Signatur eines intelligenten Angriffs, und unsere Website ist das ultimative Ziel, nicht der Reflektor. Wenn Sie die Zugriffsliste überarbeiten, können Sie weitere Informationen zu dem Angriff sammeln, wie die folgende Ausgabe zeigt:

```
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
```

Die Änderung besteht darin, dass das **log-input**-Schlüsselwort dem Zugriffslisteneintrag hinzugefügt wird, der dem verdächtigen Datenverkehr entspricht. (In Cisco IOS Software Releases vor 11.2 fehlt dieses Schlüsselwort. Verwenden Sie stattdessen das "**log**"-Schlüsselwort.) Dies veranlasst den Router, Informationen über Pakete zu protokollieren, die mit dem Listeneintrag übereinstimmen. Wenn Sie davon ausgehen, dass die **gepufferte Protokollierung** konfiguriert ist, können Sie die Meldungen sehen, die mit dem Befehl **show log** erzeugt werden (es kann wegen der Ratenbegrenzung eine Weile dauern, bis die Meldungen akkumuliert werden). Die Meldungen erscheinen ähnlich der folgenden Ausgabe:

```
%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
```

Die Quelladressen der Echo-Antwortpakete werden in den Adresspräfixen 192.168.212.0/24, 192.168.45.0/24 und 172.16.132.0/24 geclustert. (Private Adressen in den Netzwerken 192.168.x.x und 172.16.x.x sind nicht im Internet verfügbar. Dies ist eine Laborbeispiel.) Dies ist ein sehr charakteristisches Merkmal eines SMURF-Angriffs, und die Quelladressen sind die Adressen der SMURF-Reflektoren. Wenn Sie die Besitzer dieser Adressblöcke in den entsprechenden "WHOIS"-Datenbanken des Internets suchen, können Sie die Administratoren dieser Netzwerke finden und um Hilfe bei der Bewältigung des Angriffs bitten.

An dieser Stelle ist es wichtig, bei einem klügelten Vorfall daran zu denken, dass diese Reflektoren andere Opfer sind, nicht Angreifer. Angreifer verwenden ihre eigenen Quelladressen in IP-Paketen in einer DoS-Flut nur selten und können dies bei einem funktionierenden, schnellen Angriff nicht tun. Jede Adresse in einem Flood-Paket sollte entweder vollständig gefälscht oder die Adresse eines Opfers irgendeiner Art. Der produktivste Ansatz für das ultimative Ziel eines intelligenten Angriffs ist es, die Reflektoren zu kontaktieren, entweder um sie zu bitten, ihre Netzwerke neu zu konfigurieren, um den Angriff abzuschalten, oder um ihre Unterstützung bei der Rückverfolgung des Konjunkturstroms zu bitten.

Da der Schaden am Ziel eines intelligenten Angriffs in der Regel durch das Überladen der eingehenden Verbindung aus dem Internet verursacht wird, gibt es oft keine andere Antwort als die Reflektoren zu kontaktieren. Wenn die Pakete auf einem Rechner ankommen, der unter Kontrolle des Ziels steht, ist der größte Teil des Schadens bereits entstanden.

Eine Stopphhole-Maßnahme besteht darin, den Upstream-Netzwerkanbieter zu bitten, alle ICMP-Echoantworten oder alle ICMP-Echoantworten von bestimmten Reflektoren herauszufiltern. Es wird nicht empfohlen, diese Art von Filter dauerhaft einzustellen. Selbst bei einem temporären

Filter sollten nur Echoantworten gefiltert werden, nicht alle ICMP-Pakete. Eine weitere Möglichkeit besteht darin, dass der Upstream-Provider Quality of Service und Funktionen zur Ratenbegrenzung verwendet, um die Bandbreite für Echo-Antworten einzuschränken. Eine angemessene Bandbreitenbeschränkung kann unbegrenzt beibehalten werden. Beide Ansätze hängen davon ab, ob die Geräte des Upstream-Anbieters über die erforderliche Kapazität verfügen, und manchmal ist diese Kapazität nicht verfügbar.

SMURF-Reflektor

Wenn der eingehende Datenverkehr eher aus Echoanfragen als aus Echoantworten besteht (d. h. wenn der erste Eintrag der Zugriffsliste und nicht der zweite viele Übereinstimmungen zählte, die vernünftigerweise erwartet werden konnten), würden Sie einen intelligenten Angriff vermuten, bei dem das Netzwerk als Reflektor oder möglicherweise als einfache Ping-Flood verwendet wurde. Wenn der Angriff erfolgreich ist, erwarten Sie in jedem Fall, dass sowohl die ausgehende Seite der seriellen Leitung als auch die eingehende Seite überlastet werden. Aufgrund des Amplifikationsfaktors ist zu erwarten, dass die ausgehende Seite noch überlasteter ist als die eingehende Seite.

Es gibt mehrere Möglichkeiten, den schlauen Angriff von der einfachen Ping-Flut zu unterscheiden:

- Smurf-Konjunkturpakete werden an eine gezielte Broadcast-Adresse anstatt an eine Unicast-Adresse gesendet, während normale Ping-Flutungen fast immer Unicasts verwenden. Die Adressen, die das **log-input-**Schlüsselwort verwenden, werden im entsprechenden Zugriffslisteneintrag angezeigt.
- Wenn Sie als intelligenter Reflektor verwendet werden, gibt es eine unverhältnismäßig hohe Anzahl von Broadcast-Broadcasts in der **Show Interface**-Anzeige auf der Ethernet-Seite des Systems, und in der Regel eine unverhältnismäßig hohe Anzahl von Broadcasts, die in der **show ip traffic** Anzeige gesendet werden. Eine standardmäßige Ping-Flood erhöht den Broadcast-Datenverkehr im Hintergrund nicht.
- Wenn Sie als intelligenter Reflektor verwendet werden, wird mehr Datenverkehr in Richtung Internet gesendet als Datenverkehr, der aus dem Internet eingeht. Im Allgemeinen gibt es auf der seriellen Schnittstelle mehr Ausgabepakete als Eingabepakete. Selbst wenn der Reiz-Stream die Eingangsschnittstelle vollständig füllt, ist der Antwortstream größer als der Reiz-Stream, und Paketverluste werden gezählt.

Ein intelligenter Reflektor bietet mehr Optionen als das ultimative Ziel eines intelligenten Angriffs. Wenn ein Reflektor den Angriff abschaltet, genügt die entsprechende Verwendung von **no ip directed-broadcast** (oder gleichwertigen Nicht-IOS-Befehlen) in der Regel. Diese Befehle gehören jeder Konfiguration an, selbst wenn kein aktiver Angriff stattfindet. Weitere Informationen dazu, wie Sie verhindern können, dass Ihre Cisco Geräte bei einem SMURF-Angriff verwendet werden, finden Sie unter Verbessern der Sicherheit auf Cisco Routern. Allgemeine Informationen zu SMURF-Angriffen im Allgemeinen und Informationen zum Schutz von Geräten anderer Anbieter finden Sie auf der Seite "Informationen zu Denial of Service Attacks" (Informationen zu DoS-Angriffen).

Ein intelligenter Reflektor ist dem Angreifer einen Schritt näher als das ultimative Ziel und daher besser in der Lage, den Angriff zu verfolgen. Wenn Sie den Angriff verfolgen möchten, müssen Sie mit den beteiligten ISPs zusammenarbeiten. Wenn Sie die Verfolgung abschließen möchten, müssen Sie mit den zuständigen Strafverfolgungsbehörden zusammenarbeiten. Wenn Sie einen Angriff nachverfolgen möchten, sollten Sie so schnell wie möglich die Strafverfolgung einbeziehen. Im Tracing-Abschnitt finden Sie technische Informationen zur Nachverfolgung von Flooding-

Angriffen.

Fracking

Der Fraggle-Angriff entspricht dem SMURF-Angriff, mit der Ausnahme, dass UDP-Echo-Anfragen für den Stimulus-Stream statt für ICMP-Echoanfragen verwendet werden. Die dritte und vierte Zeile der Zugriffsliste identifizieren Fraggle-Angriffe. Die entsprechende Reaktion für die Opfer ist dieselbe, mit der Ausnahme, dass UDP-Echo in den meisten Netzwerken weniger wichtig ist als ICMP-Echo. Sie können sie daher komplett deaktivieren, ohne dass die Folgen negativ sein können.

SYN-Flood

Die fünfte und sechste Zeile der Zugriffsliste sind:

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

Die erste dieser Zeilen stimmt mit jedem TCP-Paket überein, wenn das ACK-Bit festgelegt ist. Für unsere Zwecke bedeutet das wirklich, dass es mit jedem Paket übereinstimmt, das keine TCP-SYN ist. Die zweite Zeile entspricht nur Paketen, die TCP-SYNs sind. Eine SYN-Flut lässt sich leicht an den Zählern in diesen Listeneinträgen erkennen. Im normalen Datenverkehr übersteigen Nicht-SYN-TCP-Pakete die SYNs um mindestens den Faktor zwei, in der Regel mehr als vier oder fünf. Bei einer SYN-Flood übertreffen SYNs in der Regel die Anzahl der nicht SYN-TCP-Pakete um ein Vielfaches.

Die einzige Bedingung ohne Angriff, die diese Signatur erstellt, ist eine massive Überlastung echter Verbindungsanforderungen. Im Allgemeinen kommt eine solche Überladung nicht unerwartet und umfasst nicht so viele SYN-Pakete wie eine echte SYN-Flut. Außerdem enthalten SYN-Floods häufig Pakete mit vollständig ungültigen Quelladressen. Mit dem **log-input-** Schlüsselwort können Sie sehen, ob Verbindungsanforderungen von solchen Adressen stammen.

Es gibt einen Angriff, der als "Prozess-Tabelle-Angriff" bezeichnet wird und der Ähnlichkeit mit der SYN-Flood aufweist. Bei einem Angriff auf die Prozesstabelle werden die TCP-Verbindungen abgeschlossen, und es wird ihnen erlaubt, ohne weiteren Protokolldatenverkehr ein Timeout durchzuführen, während bei der SYN-Flood nur die ersten Verbindungsanforderungen gesendet werden. Da ein Angriff auf eine Prozesstabelle den Abschluss des ursprünglichen TCP-Handshake erfordert, muss er im Allgemeinen mithilfe der IP-Adresse eines echten Rechners gestartet werden, auf den der Angreifer Zugriff hat (in der Regel gestohlener Zugriff). Prozesstabellenangriffe lassen sich daher durch die Verwendung der Paketprotokollierung leicht von SYN-Floods unterscheiden. Alle SYNs in einer Prozesstabelle stammen von einer oder mehreren Adressen oder höchstens von einem oder mehreren Subnetzen.

Die Reaktionsmöglichkeiten für die Opfer von SYN-Überschwemmungen sind sehr begrenzt. Das angegriffene System ist in der Regel ein wichtiger Dienst, und die Blockierung des Zugriffs auf das System erreicht in der Regel das, was der Angreifer wünscht. Viele Router- und Firewall-Produkte, darunter die von Cisco, verfügen über Funktionen, mit denen die Auswirkungen von SYN-Überschwemmungen reduziert werden können. Die Effektivität dieser Funktionen hängt jedoch von der Umwelt ab. Weitere Informationen finden Sie in der Dokumentation zum Cisco IOS Firewall Feature Set, der Dokumentation zur Cisco IOS TCP Intercept-Funktion und zur Verbesserung der Sicherheit auf Cisco Routern.

SYN-Floods können nachverfolgt werden, aber der Ablaufverfolgungsprozess erfordert die Unterstützung jedes ISP auf dem Weg vom Angreifer zum Opfer. Wenn Sie versuchen, eine SYN-Flut nachzuverfolgen, wenden Sie sich frühzeitig an die Strafverfolgungsbehörden und arbeiten Sie mit Ihrem eigenen Upstream-Dienstanbieter zusammen. Weitere Informationen zur Rückverfolgung von Cisco Geräten finden Sie im Abschnitt zur Nachverfolgung dieses Dokuments.

Andere Angriffe

Wenn Sie glauben, dass Sie unter einem Angriff stehen, und wenn Sie diesen Angriff mithilfe von IP-Quell- und Zieladressen, Protokollnummern und Portnummern charakterisieren können, können Sie Ihre Hypothese mithilfe von Zugriffslisten testen. Erstellen Sie einen Zugriffslisteneintrag, der mit dem verdächtigen Datenverkehr übereinstimmt, wenden Sie ihn auf eine geeignete Schnittstelle an, und beobachten Sie die Zähler für die Übereinstimmung, oder protokollieren Sie den Datenverkehr.

Protokollierung und Gegenargumente

Der Zähler eines Zugriffslisteneintrags zählt alle Übereinstimmungen mit diesem Eintrag. Wenn Sie eine Zugriffsliste auf zwei Schnittstellen anwenden, werden aggregierte Zählungen angezeigt.

Die Protokollierung der Zugriffslisten zeigt nicht jedes Paket an, das mit einem Eintrag übereinstimmt. Die Protokollierungsrate ist begrenzt, um eine CPU-Überlastung zu vermeiden. Die Protokollierung zeigt, dass es sich um ein relativ repräsentatives Beispiel handelt, jedoch nicht um eine vollständige Paketverfolgung. Denken Sie daran, dass es Pakete gibt, die Sie nicht sehen.

In einigen Softwareversionen funktioniert die Zugriffslistenprotokollierung nur in bestimmten Switching-Modi. Wenn ein Eintrag in einer Zugriffsliste viele Übereinstimmungen zählt, aber nichts protokolliert, versuchen Sie, den Route-Cache zu löschen, um zu erzwingen, dass Pakete verarbeitet werden. Seien Sie vorsichtig, wenn Sie dies auf stark ausgelasteten Routern mit vielen Schnittstellen tun. Während der Wiederherstellung des Cache kann viel Datenverkehr verloren gehen. Verwenden Sie Cisco Express Forwarding wann immer möglich.

Zugriffslisten und Protokollierung haben zwar Auswirkungen auf die Leistung, aber keine großen. Seien Sie vorsichtig bei Routern, die mit einer CPU-Auslastung von mehr als 80 % betrieben werden, oder wenn Sie Zugriffslisten auf sehr Hochgeschwindigkeitsschnittstellen anwenden.

Ablaufverfolgung

Die Quelladressen von DoS-Paketen werden fast immer auf Werte festgelegt, die nichts mit den Angreifern selbst zu tun haben. Sie sind daher nicht hilfreich bei der Identifizierung der Angreifer. Die einzige zuverlässige Methode, um die Quelle eines Angriffs zu identifizieren, besteht darin, ihn auf Hop-by-Hop-Ebene durch das Netzwerk zu verfolgen. Dieser Prozess umfasst die Neukonfiguration von Routern und die Prüfung von Protokollinformationen. Alle Netzwerkbetreiber müssen auf dem Weg vom Angreifer zum Opfer zusammenarbeiten. Um diese Zusammenarbeit sicherzustellen, müssen in der Regel Strafverfolgungsbehörden einbezogen werden, die ebenfalls beteiligt sein müssen, wenn Maßnahmen gegen den Angreifer ergriffen werden sollen.

Die Nachverfolgung von DoS-Hochwasser ist relativ einfach. Beginnend bei einem Router (der als "A" bezeichnet wird), der bekanntermaßen Hochwasserverkehr überträgt, identifiziert man den Router (als "B" bezeichnet), von dem A den Datenverkehr empfängt. Einer meldet sich dann bei B

an und sucht den Router (mit dem Namen "C"), von dem B den Datenverkehr empfängt. Dies wird so lange fortgesetzt, bis die ultimative Quelle gefunden wird.

Diese Methode hat mehrere Komplikationen, die in dieser Liste beschrieben werden:

- Die "ultimative Quelle" kann ein Computer sein, der durch den Angreifer kompromittiert wurde, der sich aber im Besitz eines anderen Opfers befindet und von diesem betrieben wird. In diesem Fall ist die Nachverfolgung der DoS-Flood nur der erste Schritt.
- Angreifer wissen, dass sie nachverfolgt werden können und setzen ihre Angriffe in der Regel nur für begrenzte Zeit fort. Es wird vielleicht nicht genug Zeit sein, die Flut tatsächlich zu verfolgen.
- Angriffe können aus mehreren Quellen erfolgen, besonders wenn der Angreifer relativ komplex ist. Es ist wichtig, möglichst viele Quellen zu ermitteln.
- Kommunikationsprobleme verlangsamen den Ablaufverfolgungsprozess. Häufig stehen einem oder mehreren der beteiligten Netzbetreiber keine entsprechend qualifizierten Mitarbeiter zur Verfügung.
- Rechtliche und politische Bedenken können es auch dann erschweren, gegen Angreifer vorzugehen, wenn diese erkannt werden.

Die meisten Bemühungen, DoS-Angriffe zurückzuverfolgen, schlagen fehl. Daher versuchen viele Netzwerkbetreiber nicht einmal, einen Angriff zurückzuverfolgen, wenn sie nicht unter Druck gesetzt werden. Viele andere verfolgen nur "schwere" Angriffe, mit unterschiedlichen Definitionen dessen, was "schwerwiegend" ist. Manche helfen nur bei der Verfolgung, wenn die Strafverfolgung betroffen ist.

Ablaufverfolgung mit "log-input"

Wenn Sie einen Angriff verfolgen möchten, der über einen Cisco Router verläuft, können Sie dies am effektivsten tun, indem Sie einen Zugriffslisteneintrag erstellen, der dem Angriffsverkehr entspricht, das **log-input-**Schlüsselwort anfügen und die ausgehende Zugriffsliste auf die Schnittstelle anwenden, über die der Angriffs-Stream an sein ultimatives Ziel gesendet wird. Die von der Zugriffsliste erstellten Protokolleinträge geben die Router-Schnittstelle an, über die der Datenverkehr eingeht. Wenn es sich bei der Schnittstelle um eine Multipoint-Verbindung handelt, geben Sie die Layer-2-Adresse des Geräts an, von dem er empfangen wird. Die Layer-2-Adresse kann dann zum Identifizieren des nächsten Routers in der Kette verwendet werden, z. B. mit dem **Befehl show ip arp** ***mac-address***.

SYN Flood

Um eine SYN-Flood zu verfolgen, können Sie eine Zugriffsliste erstellen, die der folgenden ähnelt:

```
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
```

Dadurch werden alle für den Zielhost bestimmten SYN-Pakete, einschließlich legitimer SYNs, protokolliert. Um den wahrscheinlichsten tatsächlichen Pfad zum Angreifer zu identifizieren, überprüfen Sie die Protokolleinträge im Detail. Im Allgemeinen ist die Quelle der Flut die Quelle, von der die größte Anzahl übereinstimmender Pakete eingeht. Die Quell-IP-Adressen selbst bedeuten nichts. Sie suchen Quellschnittstellen und Quell-MAC-Adressen. Manchmal ist es möglich, Flood-Pakete von legitimen Paketen zu unterscheiden, da Flood-Pakete ungültige Quelladressen haben können. Jedes Paket, dessen Quelladresse ungültig ist, ist wahrscheinlich

Teil der Flut.

Die Flut kann aus mehreren Quellen kommen, obwohl dies bei SYN-Überschwemmungen relativ ungewöhnlich ist.

Smurf-Stimulus

Verwenden Sie eine Zugriffsliste wie diese, um einen smurf-stimulus-Stream zu verfolgen:

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

Beachten Sie, dass sich der erste Eintrag nicht auf Pakete beschränkt, die für die Reflektoradresse bestimmt sind. Der Grund hierfür ist, dass die meisten intelligenten Angriffe mehrere Reflektornetzwerke verwenden. Wenn Sie nicht mit dem ultimativen Ziel in Berührung kommen, kennen Sie möglicherweise nicht alle Reflektoradressen. Wenn Ihre Trace näher an der Quelle des Angriffs ist, können Sie anfangen, Echo-Anfragen an immer mehr Ziele zu senden. Das ist ein gutes Zeichen.

Wenn Sie jedoch viel ICMP-Datenverkehr verarbeiten, kann dies zu viele Protokollierungsinformationen generieren, die Sie einfach lesen können. In diesem Fall können Sie die Zieladresse auf einen der Reflektoren beschränken, die bekanntermaßen verwendet werden. Eine weitere nützliche Taktik ist, einen Eintrag zu verwenden, der die Tatsache ausnutzt, dass Netmasken von 255.255.255.0 sehr häufig im Internet. Und weil Angreifer intelligente Reflektoren finden, sind die Reflektoradressen, die tatsächlich für Smart-Attacken verwendet werden, noch wahrscheinlicher, dass sie dieser Maske entsprechen. Hostadressen, die in .0 oder .255 enden, sind im Internet sehr selten. Daher können Sie einen relativ spezifischen Erkenner für smurf-Reiz-Streams erstellen, wie die folgende Ausgabe zeigt:

```
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
```

Mit dieser Liste können Sie viele der "Rauschpakete" aus Ihrem Protokoll entfernen, während Sie immer noch gute Chancen haben, zusätzliche Reiz-Streams zu beobachten, wenn Sie sich dem Angreifer nähern.

Ablaufverfolgung ohne "log-input"

Das **log-input**-Schlüsselwort ist in den Cisco IOS Software Releases 11.2 und höher sowie in bestimmten, speziell für den Service Provider-Markt entwickelten, auf 11.1 basierenden Software enthalten. Ältere Software unterstützt dieses Schlüsselwort nicht. Wenn Sie einen Router mit älterer Software verwenden, stehen Ihnen drei Optionen zur Verfügung:

- Erstellen Sie eine Zugriffsliste ohne Protokollierung, aber mit Einträgen, die dem verdächtigen Datenverkehr entsprechen. Wenden Sie die Liste nacheinander auf der *Eingangsseite* der einzelnen Schnittstellen an, und beobachten Sie die Zähler. Suchen Sie nach Schnittstellen mit hohen Abgleichraten. Diese Methode hat einen sehr geringen Performance-Overhead und eignet sich gut für die Identifizierung von Quellschnittstellen. Der größte Nachteil besteht darin, dass keine Quelladressen auf der Verbindungsschicht angegeben werden und daher vor allem für Punkt-zu-Punkt-Leitungen nützlich ist.
- Erstellen Sie Zugriffslisteneinträge mit dem **log-**Schlüsselwort (im Gegensatz zu **log-input**).

Wenden Sie die Liste wiederum auf die eingehende Seite jeder Schnittstelle an. Diese Methode gibt noch immer keine Quell-MAC-Adressen aus, kann aber nützlich sein, um IP-Daten anzuzeigen. Zum Beispiel, um zu überprüfen, ob ein Paket-Stream tatsächlich Teil eines Angriffs ist. Die Auswirkungen auf die Leistung können mittelgradig bis hoch sein, und neuere Software arbeitet besser als ältere Software.

- Verwenden Sie den Befehl **debug ip packet detail** , um Informationen über Pakete zu sammeln. Diese Methode gibt MAC-Adressen, kann jedoch schwerwiegende Auswirkungen auf die Leistung haben. Mit dieser Methode kann man leicht Fehler machen und einen Router unbrauchbar machen. Wenn Sie diese Methode verwenden, stellen Sie sicher, dass der Router den Angriffsverkehr im schnellen, autonomen oder optimalen Modus umschaltet. Verwenden Sie eine Zugriffsliste, um das Debuggen auf die Informationen zu beschränken, die Sie wirklich benötigen. Protokollieren Sie Debugging-Informationen in den lokalen Protokollpuffer, deaktivieren Sie jedoch die Protokollierung der Debugging-Informationen für Telnet-Sitzungen und die Konsole. Wenn möglich, stellen Sie sicher, dass sich jemand in der Nähe des Routers befindet, damit dieser bei Bedarf ein- und ausgeschaltet werden kann.Beachten Sie, dass der Befehl **debug ip packet** keine Informationen über Fast-Switched-Pakete anzeigt. Sie müssen den Befehl **clear ip cache** ausstellen, um Informationen zu erfassen. Jeder **clear-**Befehl gibt Ihnen ein oder zwei Pakete Debugausgabe.

Zugehörige Informationen

- Kerberos
- Technischer Support und Dokumentation - Cisco Systems