تمييز حالات فيض الحزم والتتبع باستخدام موجهات Cisco

المحتويات

المقدمة

تعتبر هجمات رفض الخدمة (DoS) شائعة على الإنترنت. الخطوة الأولى التي تستخدمها للرد على مثل هذا الهجوم هي أن تعرف بالضبط ما هو الهجوم. وتعتمد العديد من هجمات رفض الخدمة (DoS) المستخدمة بشكل شائع على فيضانات الحزم ذات النطاق الترددي العالي أو على التدفقات المتكررة الأخرى للحزم.

يمكن عزل الحزم الموجودة في العديد من تدفقات هجوم رفض الخدمة (DoS) عندما تقوم بمطابقتها مقابل إدخالات قائمة الوصول إلى برنامج Cisco IOS®. إن هذا أمر قيم لتصفية الهجمات. كما أنه مفيد أيضا عندما تقوم بتوصيف هجمات غير معروفة، ولعندما تقوم بتتبع تدفقات الحزمة "المنتحلة" رجوعا إلى مصادرها الحقيقية.

يمكن في بعض الأحيان إستخدام ميزات موجه Cisco مثل تسجيل الأخطاء ومحاسبة IP لأغراض مماثلة، وخاصة مع الهجمات الجديدة أو غير العادية. ومع ذلك، باستخدام الإصدارات الأخيرة من برنامج Cisco IOS، تعد قوائم الوصول وتسجيل قائمة الوصول الميزات الأولى ل عند تحديد الهجمات الشائعة وتتبعها.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

أكثر هجمات رفض الخدمة (DoS) شيوعا

هناك مجموعة واسعة من هجمات رفض الخدمة المحتملة. حتى إذا قمت بتجاهل الهجمات التي تستخدم أخطاء البرامج لإيقاف تشغيل الأنظمة التي تحتوي على حركة مرور قليلة نسبيا، تظل الحقيقة هي أن أي حزمة IP يمكن إرسالها عبر الشبكة يمكن إستخدامها لتنفيذ هجوم رفض الخدمة (DoS) الذي يفيض. عندما تكون تحت هجوم، يجب أن تفكر دائما في إمكانية أن ما تراه هو شيء لا يندرج ضمن التصنيفات المعتادة.

ولكن إذا اخذنا هذا التحذير بعين الاعتبار، فمن الجيد أيضا ان نتذكر ان هجمات كثيرة متشابهة. ويختار المهاجمون الملاحقات الشائعة لأنها فعالة بشكل خاص، أو لأنها غير قابلة للتعقب بشكل خاص، أو لأن الأدوات متاحة. ويفتقر العديد من مهاجميي "حركة طالبان باكستان" إلى المهارة أو الحافز لإنشاء أدواتهم الخاصة، واستخدام البرامج الموجودة على الإنترنت. وتميل هذه الأدوات إلى التحول إلى الموضة أو الخروج منها.

في وقت كتابة هذا المقال، في يوليو/تموز 1999، كانت معظم طلبات العملاء للحصول على مساعدة Cisco تتضمن هجوم "smurf". هذا الهجوم ضحيتان: "هدف نهائي" و"عاكس". يرسل المهاجم تدفق تنبيه من ICMP صدى طلب ("pings") إلى عنوان البث من العاكس شبكة فرعية. يتم تزوير عناوين المصدر لهذه الحزم لتكون عنوان الهدف النهائي. لكل حزمة مرسلة من المهاجم، يستجيب العديد من البيئات المضيفة على الشبكة الفرعية للعاكس. ويؤدي ذلك إلى إغراق الهدف النهائي وإهدار النطاق الترددي لكل من الضحايا.

ويستخدم هجوم مماثل، يسمى "التضييق"، عمليات البث الموجهة بنفس الطريقة، ولكنه يستخدم طلبات صدى UDP بدلا من طلبات صدى بروتوكول رسائل التحكم في الإنترنت (ICMP). وعادة ما يحقق هذا الاختلال عامل تضخيم أقل من سنفور، كما أنه أقل شعبية بكثير.

يتم عادة ملاحظة هجمات smurf لأن إرتباط الشبكة يصبح مثقلا بشكل زائد. يوجد وصف كامل لهذه الهجمات، وللتدابير الدفاعية، في صفحة معلومات هجمات رفض الخدمة .

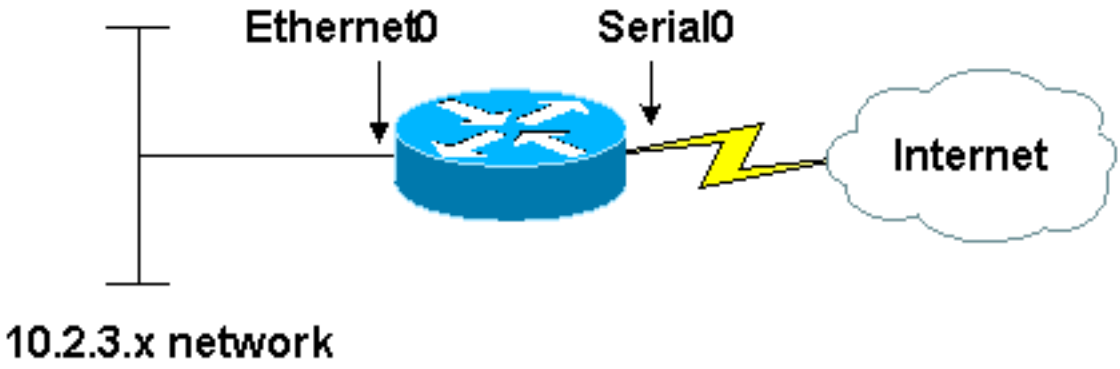
هناك هجوم شائع آخر هو طوفان SYN، حيث يتم تدفق جهاز هدف به طلبات اتصال TCP. يتم تقسيم عناوين المصدر ومنافذ TCP المصدر لحزم طلب الاتصال عشوائيا. الغرض هو إجبار المضيف الهدف على الحفاظ على معلومات الحالة للعديد من الاتصالات التي لا يتم إكمالها أبدا.

يتم عادة ملاحظة هجمات فيضان SYN لأن المضيف الهدف (غالبا ما يكون HTTP أو خادم SMTP) يكون بطيئا للغاية أو يتعطل أو يتعطل. من الممكن أيضا لحركة المرور التي ترجع من المضيف الهدف أن تتسبب في حدوث مشكلة على الموجهات. وهذا يرجع لأن حركة المرور العائدة هذه تذهب إلى عناوين المصدر العشوائية للحزم الأصلية، وهي تفتقر إلى الخصائص المحلية لحركة مرور IP "الحقيقية"، ويمكن أن تتجاوز مخازن المسار. في موجهات Cisco، غالبا ما تظهر هذه المشكلة نفسها في الموجه الذي نفدت الذاكرة منه.

تشكل هجمات فيضانات Smurf و SYN معا الأغلبية العظمى من هجمات رفض الخدمة (DoS) التي تم إبلاغ Cisco بها، كما أن التعرف عليها بسرعة يعد أمرا بالغ الأهمية. يمكن التعرف بسهولة على كلا الهجومين (وكذلك بعض هجمات "الطبقة الثانية"، مثل فيضانات إختبار الاتصال) عند إستخدام قوائم الوصول من Cisco.

قائمة الوصول إلى وصف رفض الخدمة (DoS)

صورة موجه باستخدام واجهتين. يتصل Ethernet 0 بشبكة LAN داخلية في شركة أو مزود خدمة الإنترنت (ISP) الصغير. يوفر Serial 0 اتصال إنترنت عبر ISP للتحميل. يتم "تثبيت" معدل حزمة الإدخال في التسلسل 0 على النطاق الترددي الكامل للارتباط، كما تقوم الأجهزة المضيفة الموجودة على الشبكة المحلية بالعمل ببطء أو عطل أو تعليق أو إظهار علامات أخرى لهجوم رفض الخدمة (DoS). لا يحتوي الموقع الصغير الذي يتصل به الموجه على أي محلل شبكة، كما أن الأشخاص الموجودين هناك لديهم خبرة قليلة أو معدومة في قراءة آثار محلل حتى إذا كانت التتبع متوفرة.



الآن، افترض أنك قمت بتطبيق قائمة الوصول كما يوضح هذا الإخراج:

```
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
```

لا تقوم هذه القائمة بتصفية أي حركة مرور على الإطلاق، جميع الإدخالات مسموح بها. ومع ذلك، نظرا لأنها تصنف الحزم بطرق مفيدة، يمكن إستخدام القائمة لتشخيص جميع أنواع الهجمات الثلاثة بشكل افتراضي: smurf، وسيول SYN، والتلاعب.

الهدف النهائي ل Smurf

إذا قمت بإصدار الأمر **show access-list** ، فيمكنك رؤية مخرجات مماثلة لهذا:

```
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
```

يتكون معظم حركة المرور التي تصل إلى الواجهة التسلسلية من حزم الرد على ICMP Echo. هذا على الأرجح توقيع هجوم سنفور، وموقعنا هو الهدف النهائي، بدلا من العاكس. يمكنك تجميع المزيد من المعلومات حول الهجوم عند مراجعة قائمة الوصول، كما يوضح هذا الإخراج:

```
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
```

يكمن التغيير هنا في إضافة الكلمة الأساسية **إدخال السجل** إلى إدخال قائمة الوصول التي تطابق حركة مرور البيانات المشتبه فيها. (تفتقر الإصدارات الأقدم من 11.2 من برنامج Cisco IOS software إلى هذه الكلمة الأساسية. أستخدم الكلمة الأساسية **log**" بدلا من ذلك.) وهذا يتسبب في أن يقوم الموجه بتسجيل المعلومات حول الحزم التي تطابق إدخال القائمة. إذا افترضت أنه تم تكوين **التسجيل المخزن مؤقتا**، فيمكنك رؤية الرسائل التي ينتج عنها الأمر **show log** (قد يستغرق تراكم الرسائل بعض الوقت بسبب تحديد المعدل). تظهر الرسائل مماثلة لهذا المخرج:

```
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)
```

يتم تجميع عناوين المصدر لحزم الرد على الصدى في بادئات العناوين 24/192.168.212.0 و 24/192.168.45.0 و 24/172.16.132.0. (العناوين الخاصة في شبكات x.x.192.168 و x.x.172.16 لن تكون على الإنترنت؛ هذا رسم توضيحي للمختبر.) هذا سمة جدا من هجوم السنفور، والمصدر عنوان من العاكس سنفور. إذا بحثت عن أصحاب هذه العناوين في قواعد البيانات المناسبة على الإنترنت "WHOIS"، يمكنك العثور على مسؤولي هذه الشبكات وطلب مساعدتهم في التعامل مع الهجوم.

من المهم في هذه المرحلة من الحوادث المتكررة أن نتذكر أن العاكس هؤلاء هم ضحايا رفقاء وليس مهاجمين. من النادر جدا للمهاجمين إستخدام عناوين المصدر الخاصة بهم على حزم IP في أي تدفق لرفض الخدمة (DoS)، ومن المستحيل بالنسبة لهم القيام بذلك في هجوم يتم بسرعة فائقة. وأي عنوان في حزمة فيضان ينبغي افتراض أنه إما أن يكون مزورا تماما، أو أن يكون عنوان الضحية من نوع ما. المنهج الأكثر إنتاجية لهدف هجوم السنفور في نهاية المطاف هو الاتصال بالعاكسين، إما لمطالبتهم بإعادة تكوين شبكاتهم لإيقاف الهجوم، أو لطلب مساعدتهم في تتبع تيار التحفيز.

لأن الضرر الذي يصيب الهدف النهائي لهجوم سنفور عادة ما يكون بسبب الحمولة الزائدة على الرابط القادم من الإنترنت، فإنه غالبا ما لا يكون هناك أي إستجابة غير الاتصال بالعاكسات. في الوقت الذي تصل فيه الحزم إلى أي جهاز تحت التحكم في الهدف، يكون قد حدث معظم الضرر بالفعل.

واحد مؤقت مقياس أن يطلب من مزود شبكة المنبع أن يصفي كل ردود صدى ICMP، أو كل ردود صدى ICMP من عاكس معين. لا يوصى بترك هذا النوع من عوامل التصفية في موضعه بشكل دائم. حتى لعامل تصفية مؤقت، يجب تصفية ردود الارتداد فقط، وليس جميع حزم ICMP. إمكانية أخرى هي أن يقوم موفر البث باستخدام ميزات جودة الخدمة وتحديد المعدل لتقييد النطاق الترددي المتاح لردود صدى. يمكن ترك قيود معقولة على عرض النطاق الترددي في مكانها لأجل غير مسمى. يعتمد كلا النهجين على معدات مقدم خدمات المنبع التي لديها القدرة اللازمة، وفي بعض الأحيان تكون هذه القدرة غير متاحة.

عاكس سنفوري

إذا كانت حركة المرور الواردة تتألف من طلبات echo بدلا من ردود الارتداد (بمعنى آخر، إذا كان إدخال قائمة الوصول الأولى، بدلا من الثانية، يحسب العديد من التطابقات أكثر مما يمكن توقعه بشكل معقول)، فقد تشك في حدوث هجوم smurf يتم فيه إستخدام الشبكة كعاكس، أو ربما يكون فيضان إختبار الاتصال بسيطا. في كلتا الحالتين، إذا نجحت الهجمة، فأنتم تتوقعون غرق الجانب الخارج من الخط التسلسلي، وكذلك الجانب القادم. في الواقع، بسبب عامل التضخيم، فإنك تتوقع أن يكون الجانب الخارج محملا أكثر من الجانب القادم.

هناك عدة طرق للتمييز بين هجوم "السنفور" وفيض "بينج" البسيط:

- يتم إرسال حزم تنبيه Smurf إلى عنوان بث موجه، بدلا من عنوان البث الأحادي، في حين تستخدم فيضانات ping العادية دائما تقريبا السواحل الأحادية. يمكنك رؤية العناوين التي تستخدم الكلمة الأساسية **إدخال السجل** في إدخال قائمة الوصول المناسب.
- إذا كنت تستخدم كعاكس Smurf، فهناك عدد غير متناسب من عمليات بث الإخراج في عرض **الواجهة show** على جانب الإيثرنت في النظام، وعادة ما يكون عددا غير متناسب من عمليات البث المرسلة في شاشة **عرض حركة مرور IP**. لا يزيد فيض إختبار الاتصال القياسي حركة مرور بيانات البث في الخلفية.
- إن يكون أنت استعملت كعاكس smurf، هناك كثير حركة مرور يصدر إلى الإنترنت من حركة مرور قادم من الإنترنت. بشكل عام، هناك المزيد من حزم المخرجات من حزم الإدخال على الواجهة التسلسلية. حتى إذا امتلأ تدفق التحفيز بواجهة الإدخال بشكل كامل، فإن تدفق الاستجابة يكون أكبر من تدفق التحفيز، ويتم حساب عمليات إسقاط الحزم.

يحتوي عاكس Smurf على خيارات أكثر من الهدف النهائي لهجوم Smurf. إذا اختار العاكس إيقاف تشغيل الهجوم، يكفي عادة الاستخدام المناسب **لعدم توجيه البث** (أو ما يعادل ذلك من الأوامر بخلاف IOS). تنتمي هذه الأوامر إلى كل تكوين، حتى إذا لم يكن هناك هجوم نشط. لمزيد من المعلومات حول منع إستخدام أجهزة Cisco في هجوم smurf، ارجع إلى تحسين الأمان على موجهات Cisco. لمزيد من المعلومات العامة حول هجمات smurf بشكل عام، ولمعلومات حول حماية المعدات غير التابعة لشركة Cisco، ارجع إلى صفحة معلومات هجمات رفض الخدمة .

إن عاكس سنفور هو خطوة أقرب من المهاجم أكثر من الهدف النهائي، وبالتالي فهو في وضع أفضل لتتبع الهجوم. إذا أخترت تعقب الهجوم، فإنك بحاجة إلى العمل مع مزودي خدمة الإنترنت المعنيين. إذا كنت ترغب في إتخاذ أي إجراء عند إكمال التتبع، فإنك بحاجة للعمل مع وكالات فرض القانون المناسبة. إذا كنت تسعى لتتبع هجوم ما، يوصى بأن تقوم بفرض القانون في أقرب وقت ممكن. راجع قسم التتبع للحصول على معلومات فنية حول تعقب هجمات الفيضانات.

هزال

يماثل هجوم التخاذل هجوم smurf، باستثناء أن طلبات صدى UDP تستخدم لتدفق التحفيز بدلا من طلبات صدى ICMP. يحدد الخطان الثالث والرابع من قائمة الوصول الهجمات المتهالكة. الاستجابة المناسبة للضحايا هي نفسها، باستثناء أن صدى UDP هو خدمة أقل أهمية في معظم الشبكات من صدى ICMP. لذلك، يمكنك تعطيلها تماما مع نتائج سلبية أقل.

سيلز والفيضانات

الأسطر الخامس والسادس من قائمة الوصول هي:

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

يتطابق أول هذه الخطوط مع أي حزمة TCP مع مجموعة بت ACK. لأغراضنا، ما يعنيه هذا حقا هو أنها تطابق أي حزمة ليست نظام TCP. ويطابق السطر الثاني الحزم التي تكون TCP SYNs فقط. يمكن التعرف بسهولة على تدفق SYN من العدادات الموجودة في إدخالات القائمة هذه. في حركة المرور العادية، تتجاوز حزم TCP غير SYN عدد SYN بمعامل إثنين على الأقل، وعادة أكثر من أربعة أو خمسة. في طوفان SYN، يفوق SYNs عادة عدد حزم TCP غير SYN عدة مرات.

الشرط الوحيد غير الهجوم الذي يقوم بإنشاء هذا التوقيع هو الحمل الزائد الهائل لطلبات الاتصال الأصلية. وبشكل عام، لن يأتي هذا التحميل الزائد بشكل غير متوقع، ولن يشمل العديد من حزم SYN مثل فيضان SYN الحقيقي. كما أن فيضانات SYN غالبا ما تحتوي على حزم ذات عناوين مصدر غير صحيحة تماما؛ باستخدام الكلمة الأساسية **إدخال السجل**، من الممكن معرفة ما إذا كانت طلبات الاتصال تأتي من هذه العناوين.

هناك هجوم يسمى "هجوم جدول العمليات" الذي يحمل بعض الشبه بفيضان النظام. في هجوم جدول العملية، يتم إكمال إتصالات TCP، ومن ثم يسمح لها بانتهاء المهلة الزمنية دون مزيد من حركة مرور البروتوكول، بينما في تدفق SYN، يتم إرسال طلبات الاتصال الأولية فقط. نظرا لأن هجوم جدول العملية يتطلب إكمال مصافحة TCP الأولية، فيجب إطلاقه بشكل عام باستخدام عنوان IP الخاص بجهاز حقيقي يمكن للمهاجم الوصول إليه (عادة الوصول المسروق). لذلك يمكن تمييز هجمات جدول العملية بسهولة من فيضانات SYN باستخدام تسجيل الحزم. تأتي جميع عناصر SYN الموجودة في هجوم جدول عملية من عنوان واحد أو عدة عناوين، أو على الأكثر من شبكة فرعية أو عدة شبكات فرعية.

خيارات الاستجابة لضحايا فيضانات الشعاب المرجانية محدودة للغاية. والنظام الذي يتعرض للهجوم هو عادة خدمة مهمة، وعادة ما يحقق منع الوصول إلى النظام ما يريده المهاجم. تحتوي العديد من منتجات الموجهات وجدار الحماية، بما في ذلك منتجات Cisco، على ميزات يمكن إستخدامها للحد من تأثير فيضانات SYN. ولكن فعالية هذه الميزات تعتمد على البيئة. أحلت ل كثير معلومة، التوثيق ل ال cisco ios جدار حماية مجموعة، التوثيق ل ال cisco ios TCP اعتراض سمة، وتحسين الأمان على cisco مسحاج تخديد.

ومن الممكن تتبع فيضانات الشبكة، ولكن عملية التعقب تتطلب مساعدة كل من مقدمي خدمات الإنترنت على طول الطريق من المهاجم إلى الضحية. إذا قررت محاولة تعقب طوفان من نظام SYN، فاتصل بسلطات إنفاذ القانون في وقت مبكر، واعمل مع موفر خدمة المنبع الخاص بك. راجع قسم التتبع في هذا المستند للحصول على تفاصيل حول التتبع باستخدام أجهزة Cisco.

هجمات أخرى

إذا كنت تعتقد أنك تتعرض لهجوم، وإذا كنت قادرا على وصف ذلك الهجوم باستخدام عناوين مصدر IP والوجهة وأرقام البروتوكولات وأرقام المنافذ، فيمكنك إستخدام قوائم الوصول لاختبار فرضيتك. قم بإنشاء إدخال قائمة وصول تطابق حركة المرور المشتبه فيها، وطبقتها على واجهة مناسبة، وإما راقب عدادات المطابقة أو سجل حركة المرور.

تحذيرات العداد والتسجيل

يقوم العداد الموجود على إدخال قائمة الوصول بحساب جميع التطابقات مقابل هذا الإدخال. إذا قمت بتطبيق قائمة وصول على واجهتين، فإن الأرقام التي تراها هي أعداد تجميعية.

لا يعرض تسجيل قائمة الوصول كل حزمة تطابق إدخالا. التسجيل محدود المعدل لتجنب الحمل الزائد لوحدة المعالجة المركزية. ما يظهره التسجيل هو عينة تمثيلية معقولة، ولكن ليس تتبع حزمة كامل. تذكر أن هناك حزم لا تراها.

في بعض إصدارات البرامج، يعمل تسجيل قائمة الوصول فقط في أوضاع تحويل معينة. إذا كان إدخال قائمة الوصول يعد الكثير من التطابقات، ولكنه لا يسجل أي شيء، فحاول مسح ذاكرة التخزين المؤقت للمسار لإجبار الحزم على أن يتم تحويلها للعملية. كن حذرا إذا قمت بذلك على الموجهات التي يتم تحميلها بشدة باستخدام العديد من الواجهات. يمكن إسقاط الكثير من حركة المرور أثناء إعادة بناء ذاكرة التخزين المؤقت. إستخدام إعادة التوجيه السريع Cisco Express Forwarding كلما أمكن ذلك.

يكون لقوائم الوصول والتسجيل تأثير على الأداء، ولكن ليس كبيرا. كن حذرا من الموجهات التي تعمل بنسبة تزيد عن 80 في المائة من حمل وحدة المعالجة المركزية (CPU)، أو عند تطبيق قوائم الوصول على الواجهات عالية السرعة.

إستشفاء

يتم تعيين عناوين المصدر لحزم رفض الخدمة (DoS) دائما تقريبا على قيم لا علاقة لها بالمهاجمين أنفسهم. وبالتالي، فهي غير مفيدة في تحديد هوية المهاجمين. الطريقة الوحيدة الموثوقة للتعرف على مصدر الهجوم هي تتبعه على الجانب الخلفي من الشبكة. وتشتمل هذه العملية على إعادة تكوين الموجهات وفحص معلومات السجل. ويلزم تعاون جميع مشغلي الشبكة على طول الطريق من المهاجم إلى الضحية. ويتطلب تأمين ذلك التعاون عادة مشاركة وكالات إنفاذ القانون، التي يجب أن تشارك أيضا إذا ما أريد إتخاذ أي إجراء ضد المهاجم.

وعملية اقتفاء آثار فيضانات الوقود المستنفد بسيطة نسبيا. ابتداء من موجه (يسمى "A") معروف بأنه يحمل حركة مرور الفيضانات، يحدد المرء الموجه (المسمى "B") الذي يستقبل منه A حركة المرور. يدخل واحد بعد ذلك إلى b، ويجد الموجه (المسمى "C") الذي يستلم منه B حركة المرور. ويستمر الحال هكذا حتى يتم العثور على المصدر النهائي.

هناك عدة تعقيدات في هذه الطريقة، والتي تصفها هذه القائمة:

- ويمكن أن يكون "المصدر النهائي" حاسوبا تعرض للخطر من قبل المهاجم، ولكنه في الواقع يملكه ويديره ضحية أخرى. وفي هذه الحالة، فإن تتبع فيضان صحيفة دو إس ليس سوى الخطوة الأولى.
- ويدرك المهاجمون أنه لا يمكن تتبع اثرهم، وعادة ما يواصلون هجماتهم إلا لفترة محدودة. قد لا يكون هنالك وقت كاف لتتبع الطوفان فعليا.
- ويمكن ان تأتي الهجمات من مصادر متعددة، وخصوصا إذا كان المهاجم متطورا نسبيا. ومن المهم محاولة تحديد أكبر عدد ممكن من المصادر.
- مشاكل الإتصال تبطئ عملية التتبع. في كثير من الأحيان لا يكون لدى واحد أو أكثر من مشغلي الشبكة المعنيين موظفون مؤهلون بشكل مناسب.
- وقد تجعل الشواغل القانونية والسياسية من الصعب العمل ضد المهاجمين حتى لو وجد.

إن أغلب الجهود الرامية إلى تتبع الهجمات التي تستهدف مسئولي خدمة الإنترنت (DoS) تفشل. ولهذا السبب، لا يحاول العديد من مشغلي الشبكة حتى تعقب هجوم ما لم يكونوا تحت الضغط. بينما لا يتتبع العديد من الآخرين سوى الهجمات "الشديدة"، مع أختلاف تعريفات ما هو "خطير". فالبعض لا يساعدون في العثور على أثر إلا إذا كان إنفاذ القانون مشمولا.

التتبع ب "إدخال السجل"

إذا أخترت تتبع هجوم يمر عبر موجه Cisco، فإن الطريقة الأكثر فعالية للقيام بذلك هي إنشاء إدخال قائمة الوصول الذي يطابق حركة مرور الهجوم، وإرفاق الكلمة الأساسية **إدخال السجل** عليه، وتطبيق قائمة الوصول الصادرة على الواجهة التي يتم من خلالها إرسال تدفق الهجوم نحو هدفه النهائي. تعرف إدخالات السجل التي تم إنتاجها بواسطة قائمة الوصول واجهة الموجه التي تصل حركة المرور من خلالها، وإذا كانت الواجهة عبارة عن اتصال متعدد النقاط، فعليك إعطاء عنوان الطبقة 2 للجهاز الذي يتم استقبالها منه. يمكن بعد ذلك إستخدام عنوان الطبقة 2 لتعريف الموجه التالي في السلسلة، باستخدام، على سبيل المثال، الأمر **show ip arp *mac address***.

سين فلوود

لتتبع تدفق SYN، يمكنك إنشاء قائمة وصول مماثلة لهذا:

```
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
```

يقوم هذا بتسجيل جميع حزم SYN الموجهة للمضيف الهدف، بما في ذلك أنظمة SYN الشرعية. لتحديد المسار الفعلي الأكثر ترجيحا نحو المهاجم، قم بفحص إدخالات السجل بالتفصيل. بشكل عام، مصدر الفيضان هو المصدر الذي منه يصل أكبر عدد من الحزم المطابقة. عناوين IP المصدر نفسها لا تعني شيئا. أنت تبحث عن واجهات مصدر وعناوين MAC مصدر. في بعض الأحيان، من الممكن تمييز حزم التدفق من الحزم الشرعية لأن حزم التدفق يمكن أن يكون لها عناوين مصدر غير صالحة. من المحتمل أن تكون أي حزمة عنوان المصدر الخاص بها غير صالح جزءا من التدفق.

يمكن ان يأتي الطوفان من مصادر متعددة، مع ان ذلك غير عادي نسبيا بالنسبة إلى فيضانات الشيفان.

منبه سنفور

لتتبع تدفق منبهات Smurf، أستخدم قائمة وصول مثل:

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

لاحظ أن الإدخال الأول لا يقيد نفسه إلى الحزم الموجهة لعنوان العاكس. السبب في هذا أن معظم هجمات smurf تستخدم شبكات عاكس متعددة. إذا لم تكن على اتصال مع الهدف النهائي، قد لا تعرف كل عناوين العاكس. ومع اقتراب تعقبك من مصدر الهجوم، قد تبدأ في رؤية طلبات الارتداد تذهب إلى وجهات أكثر وأكثر، وهذه علامة جيدة.

ومع ذلك، إذا قمت بالتعامل مع عدد كبير من حركة مرور ICMP، فقد يؤدي ذلك إلى توليد قدر كبير جدا من معلومات التسجيل لك حتى تتمكن من القراءة بسهولة. إذا حدث هذا، أنت يستطيع قيدت الغاية عنوان أن يكون واحد من العاكس أن يكون معروف أن يكون استعملت. وهناك تكتيك مفيد آخر هو إستخدام مدخل يستفيد من حقيقة أن أقنعة الشبكة 255.255.255.0 شائعة جدا في الإنترنت. وبسبب الطريقة التي يجد بها المهاجمين عاكسات smurf، فإن عناوين العاكس المستخدمة بالفعل لهجمات smurf هي أكثر إحتمالا لمطابقة هذا القناع. عناوين المضيف التي تنتهي في .0 أو .255 غير شائعة جدا في الإنترنت. لذلك، يمكنك بناء أداة تعريف محددة نسبيا لتيارات حوافز سنفور كما يوضح هذا الناتج:

```
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
```

من خلال هذه القائمة، يمكنك التخلص من العديد من حزم "الضوضاء" في سجلك، في حين لا تزال لديك فرصة جيدة لمشاهدة تدفقات إضافية من التحفيز في الوقت الذي تقترب فيه من المهاجم.

التتبع بدون "إدخال السجل"

توجد الكلمة الأساسية **إدخال السجل** لإدخال السجل في الإصدارات 11.2 من برنامج Cisco IOS والإصدارات الأحدث، وفي بعض البرامج المستندة إلى 11.1 التي تم إنشاؤها خصيصا لسوق مزود الخدمة. لا يدعم البرنامج الأقدم هذه الكلمة الرئيسية. إذا كنت تستخدم موجه مع برامج قديمة، فلديك ثلاثة خيارات قابلة للتطبيق:

- قم بإنشاء قائمة وصول دون تسجيل الدخول، ولكن باستخدام إدخالات تطابق حركة مرور البيانات المشتبه فيها. قم بتطبيق القائمة على جانب *الإدخال* لكل واجهة في المقابل، ثم راقب العدادات. ابحث عن واجهات ذات معدلات تطابق عالية. تتميز هذه الطريقة بقيمة أداء منخفضة للغاية، كما أنها مفيدة للتعرف على واجهات المصدر. إن أكبر عقبة له هي أنه لا يعطي عناوين مصدر طبقة الارتباط، وبالتالي يكون مفيدا في الغالب لخطوط الاتصال من نقطة إلى نقطة.
- قم بإنشاء إدخالات قائمة الوصول باستخدام الكلمة الأساسية **السجل** (في مقابل **إدخال السجل**). مرة أخرى، قم بتطبيق القائمة على الجانب الوارد لكل واجهة بدورها. لا تزال هذه الطريقة لا توفر عناوين MAC للمصدر، ولكن يمكن أن تكون مفيدة لعرض بيانات IP. على سبيل المثال، للتحقق من أن تدفق الحزمة هو بالفعل جزء من هجوم. تأثير الأداء يمكن أن يكون من متوسط إلى مرتفع، والبرامج الأحدث تعمل بشكل أفضل من البرامج الأقدم.
- أستخدم الأمر **debug ip packet detail** لجمع معلومات حول الحزم. توفر هذه الطريقة عناوين MAC، ولكن يمكن أن يكون لها تأثير خطير على الأداء. من السهل إرتكاب خطأ مع هذه الطريقة وجعل الموجه غير قابل للاستخدام. إذا كنت تستخدم هذه الطريقة، فتأكد من أن الموجه يحول حركة مرور الهجمات في الوضع السريع أو الذاتي أو الأمثل. أستخدم قائمة وصول لتقييد تصحيح الأخطاء على المعلومات التي تحتاج إليها فقط. قم بتسجيل معلومات تصحيح الأخطاء إلى المخزن المؤقت للسجل المحلي، ولكن قم بإيقاف تشغيل تسجيل معلومات تصحيح الأخطاء إلى جلسات عمل Telnet وإلى وحدة التحكم. إن أمكن، قم بالترتيب لكي يكون شخص ما موجودا بالقرب من الموجه فعليا، حتى يمكن تدوير الطاقة حسب الضرورة.تذكر أن الأمر **debug ip packet** لا يعرض معلومات حول الحزم سريعة التحويل. أنت تحتاج أن يصدر **ال clear ip cache** أمر in order to على قبض معلومة. كل **أمر واضح** يعطيك حزمة أو إثنتين من إخراج تصحيح الأخطاء.

معلومات ذات صلة

- Kerberos
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).