تحديد إستراتيجيات الحماية من هجمات TCP SYN لرفض الخدمة

المحتويات

مجرد

هناك هجوم محتمل لمنع الخدمة على موفري خدمة الإنترنت (ISPs) الذي يستهدف أجهزة الشبكة.

- **هجوم TCP SYN**: يرسل المرسل وحدة تخزين من الاتصالات التي لا يمكن إكمالها. وهذا يتسبب في تعبئة قوائم انتظار الاتصال، وبالتالي رفض الخدمة لمستخدمي TCP الشرعيين.

تحتوي هذه الورقة على وصف فني لكيفية حدوث هجوم TCP SYN المحتمل والطرق المقترحة لاستخدام برنامج Cisco IOS للدفاع ضده.

ملاحظة: لبرنامج Cisco IOS 11.3 ميزة لمنع هجمات رفض الخدمة عبر بروتوكول TCP بشكل فعال. يتم وصف هذه الميزة في المستند الذي يشكل اعتراض TCP (منع هجمات رفض الخدمة).

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

الاصطلاحات

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

وصف المشكلة

هجوم نظام TCP

عندما يبدأ اتصال TCP عادي، يستلم مضيف الوجهة حزمة SYN (مزامنة/بدء) من مضيف مصدر ويرسل مرة أخرى SYN ACK (تزامن الاعتراف). يجب على مضيف الوجهة بعد ذلك سماع ACK (الاعتراف) الخاص ب SYN ACK قبل إنشاء الاتصال. ويشار إلى هذا باسم "مصافحة TCP الثلاثية."

أثناء انتظار ACK إلى SYN ACK، تستمر قائمة انتظار إتصالات ذات حجم محدود على المضيف الوجهة في تعقب الاتصالات التي تنتظر إكمالها. عادة ما تفرغ قائمة الانتظار هذه بسرعة نظرا لأنه من المتوقع وصول ACK بعد SYN ACK ببضع مللي ثانية.

يستغل هجوم نظام TCP هذا التصميم من خلال وجود مضيف مصدر مهاجم يقوم بإنشاء حزم TCP SYN باستخدام عناوين مصدر عشوائية تجاه مضيف الضحايا. يرسل مضيف وجهة الضحية SYN ACK مرة أخرى إلى عنوان المصدر العشوائي ويضيف إدخالا إلى قائمة انتظار الاتصال. نظرا لأن SYN ACK موجهة لمضيف غير صحيح أو غير موجود، فإن الجزء الأخير من "تأكيد الاتصال الثلاثي" لا يتم إتمامه أبدا ويظل الإدخال في قائمة انتظار الاتصال حتى تنتهي صلاحية المؤقت، عادة لمدة دقيقة واحدة تقريبا. من خلال إنشاء حزم TCP SYN وهمية من عناوين IP العشوائية بمعدل سريع، من الممكن ملء قائمة انتظار الاتصال ورفض خدمات TCP (مثل البريد الإلكتروني أو نقل الملفات أو WWW) للمستخدمين الشرعيين.

لا توجد طريقة سهلة لتعقب منشئ الهجوم لأن عنوان IP الخاص بالمصدر مزور.

تتضمن المظاهر الخارجية للمشكلة عدم القدرة على الحصول على البريد الإلكتروني أو عدم القدرة على قبول الاتصالات بخدمات WWW أو FTP أو عدد كبير من إتصالات TCP على المضيف في الحالة SYN_RCVD.

الدفاع ضد الهجمات على أجهزة الشبكة

الأجهزة الموجودة خلف جدران الحماية

يتميز هجوم TCP SYN بتدفق حزم SYN من عناوين IP للمصدر العشوائي. أي جهاز خلف جدار حماية يوقف حزم SYN الواردة يكون محميا بالفعل من وضع الهجوم هذا ولا توجد حاجة إلى إجراء آخر. تتضمن أمثلة جدران الحماية جدار حماية PIX (Cisco Private Internet Exchange) أو موجه Cisco تم تكوينه باستخدام قوائم الوصول. للحصول على أمثلة حول كيفية إعداد قوائم الوصول على موجه Cisco، يرجى الرجوع إلى المستند زيادة الأمان على شبكات IP.

أجهزة توفر خدمات متاحة للجمهور (خوادم البريد وخوادم الويب العامة)

يعد منع هجمات SYN على الأجهزة الموجودة خلف جدران الحماية من عناوين IP العشوائية أمرا بسيطا نسبيا نظرا لأنه يمكنك إستخدام قوائم الوصول للحد بشكل صريح من الوصول الوارد إلى عدد قليل من عناوين IP المحددة. ومع ذلك، في حالة خادم ويب عام أو خادم بريد يواجه الإنترنت، لا توجد طريقة لتحديد عناوين مصدر IP الواردة المألوفة وغير المناسبة. لذلك، لا يوجد دفاع قاطع واضح ضد هجوم من عنوان IP عشوائي. تتوفر العديد من الخيارات للأجهزة

المضيفة:

- زيادة حجم قائمة انتظار الاتصال (قائمة انتظار SYN ACK).
- تقليل الوقت المستغرق في انتظار المصافحة ثلاثية الإتجاه.
- أستخدم تصحيحات برامج المورد لاكتشاف المشكلة والتغلب عليها (إذا كانت متوفرة).

يجب الاتصال بمورد المضيف لمعرفة ما إذا كان قد أنشأ تصحيحات معينة لمعالجة هجوم TCP SYN ACK.

ملاحظة: تصفية عناوين IP على الخادم غير فعالة نظرا لأن المهاجم يمكن أن يغير عنوان IP الخاص به، وقد يكون العنوان هو نفس عنوان المضيف المشروع أو لا يكون كذلك.

منع شبكة من إستضافة هجوم دون قصد

بما أن الآلية الأساسية لهجوم رفض الخدمة هذا هي إنشاء حركة مرور مصدرها عناوين IP العشوائية، نوصي بتصفية حركة المرور الموجهة إلى الإنترنت. والمفهوم الأساسي هو التخلص من الحزم ذات عناوين IP للمصدر غير الصالحة أثناء دخولها إلى الإنترنت. وهذا لا يمنع هجوم رفض الخدمة على شبكتك، ولكنه يساعد الأطراف التي تعرضت للهجوم على إستبعاد موقعك كمصدر للمهاجم. بالإضافة إلى ذلك، فإنه يجعل شبكتك أقل جاذبية كقاعدة لهذا النوع من الهجمات.

منع إرسال عناوين IP غير الصالحة

بتصفية الحزم على الموجهات التي تصل شبكتك بالإنترنت، يمكنك السماح فقط للحزم ذات عناوين IP المصدر الصالحة بمغادرة شبكتك والوصول إلى الإنترنت.

على سبيل المثال، إذا كانت شبكتك تتكون من الشبكة 172.16.0.0، وكان الموجه لديك يتصل ب ISP الخاص بك باستخدام واجهة تسلسلية 1/0، فيمكنك تطبيق قائمة الوصول على النحو التالي:

```
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
```

ملاحظة: يحدد السطر الأخير من قائمة الوصول ما إذا كانت هناك أي حركة مرور بعنوان مصدر غير صالح يدخل الإنترنت. ليس من المهم وجود هذا الخط، لكنه سيساعد على تحديد مصدر الهجمات المحتملة.

منع إستلام عناوين IP غير الصالحة

بالنسبة لموفري خدمات الإنترنت (ISPs) الذين يقدمون خدمة لإنهاء الشبكات، نوصي بشدة بالتحقق من صحة الحزم الواردة من عملائك. ويمكن تحقيق ذلك باستخدام عوامل تصفية الحزم الواردة على موجهات الحدود.

على سبيل المثال، إذا كان لدى عملائك أرقام الشبكات التالية المتصلة بالموجه الخاص بك عبر واجهة تسلسلية تحمل اسم "تسلسلية 0/1"، فيمكنك إنشاء قائمة الوصول التالية:

```
.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
```

ملاحظة: يحدد السطر الأخير من قائمة الوصول ما إذا كانت هناك أي حركة مرور ذات عناوين مصدر غير صالحة تدخل الإنترنت. ليس من المهم وجود هذا الخط، لكنه سيساعد على تحديد مصدر الهجوم المحتمل.

تمت مناقشة هذا الموضوع بشيء من التفصيل في القائمة البريدية ل NANOG [North American Network Operator1S Group]. توجد محفوظات القائمة على الموقع التالي:
http://www.merit.edu/mail.archives/nanog/index.html

للحصول على وصف تفصيلي لهجوم رفض خدمة TCP SYN وانتحال عناوين IP، راجع:
http://www.cert.org/advisories/CA-1996-21.html

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

معلومات ذات صلة

- الدعم الفني - 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).