إستخدام NBAR وقوائم التحكم في الوصول لحظر الدودة "Code Red" (ACL)

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
كيفية حظر دودة "الشفرة الحمراء"
الأنظمة الأساسية المدعومة
اكتشاف محاولة الإصابة في سجلات ويب IIS
وضع علامة "Code Red" على الهاكرز الوارد باستخدام ميزة التميز المستندة إلى فئة IOS
الطريقة أ: إستخدام قائمة تحكم في الوصول (ACL)
الطريقة ب: إستخدام التوجيه القائم على السياسة (PBR)
الطريقة ج: إستخدام النهج المستند إلى الفئة
تقييدات NBAR
مشكلات معروفة
معلومات ذات صلة

المقدمة

يزود هذا وثيقة طريقة أن يمنع ال "رمز أحمر" دودة في شبكة نقطة مدخل من خلال شبكة baser تطبيق تمييز (NBAR) و منفذ تحكم قائمة (ACLs) ضمن cisco ios ® برمجية على cisco مسحاج تخديد. يجب إستخدام هذا الحل بالاقتران مع برامج التصحيح الموصى بها لخوادم IIS من Microsoft.

ملاحظة: لا تعمل هذه الطريقة على موجهات سلسلة 1600 من Cisco.

ملاحظة: لا يمكن حظر بعض حركة مرور P2P بشكل كامل بسبب طبيعة بروتوكول P2P الخاص بها. تقوم بروتوكولات P2P هذه بتغيير تواقيعها بشكل ديناميكي لتخطي أي محركات DPI تحاول حظر حركة المرور الخاصة بها بشكل كامل. لذلك، يوصى بتقييد النطاق الترددي بدلا من حظره بالكامل. كبح النطاق الترددي لحركة المرور هذه. وفر عرض نطاق ترددي أقل بكثير، ومع ذلك، دع الاتصال يمر من خلال.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- سياسات خدمة جودة الخدمة (QoS) باستخدام أوامر واجهة سطر أوامر جودة الخدمة (CLI) النمطية.
- نبار

- ACLs
- التوجيه القائم على السياسة

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة. تم إختبار التكوين في هذا المستند على المحول Cisco 3640 الذي يشغل الإصدار 12.2(24a) من Cisco IOS

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

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

كيفية حظر دودة "الشفرة الحمراء"

أول شيء يجب عليك فعله لمكافحة "رمز أحمر" هو تطبيق التصحيح المتوفر من Microsoft (راجع الارتباطات في أسلوب القسم A: إستخدام قائمة التحكم بالوصول (ACL) أدناه). وهذا يحمي الأنظمة الضعيفة ويزيل الدودة من الجهاز المصاب. ومع ذلك، فإن تطبيق التصحيح على الخوادم الخاصة بك يمنع الفيروسات المتنقلة من إصابة الخوادم فقط، كما أنه لا يمنع طلبات HTTP GET من الوصول إلى الخوادم. ولا تزال هنالك امكانية ان ينهال على الخادم فيض من محاولات الخمج.

تم تصميم الحل المفصل في هذا الإصدار الاستشاري للعمل جنبا إلى جنب مع تصحيح Microsoft لحظر طلبات "HTTP GET "Code Red عند نقطة دخول شبكة.

يحاول هذا الحل حظر العدوى، ولكنه لن يعالج المشاكل الناجمة عن تراكم أعداد كبيرة من إدخالات ذاكرة التخزين المؤقت، وإدخالات التجاور، وإدخالات NAT/PAT، حيث إن الطريقة الوحيدة لتحليل محتويات طلب HTTP GET هي بعد إنشاء اتصال TCP. لن يساعد الإجراء التالي في الحماية من إجراء مسح ضوئي للشبكة. ومع ذلك، فإنه سيحمي الموقع من الإصابة من شبكة خارجية أو يقلل من عدد محاولات الإصابة التي يجب أن يقوم الجهاز بتشغيلها. وبالإضافة إلى التصفية الواردة، تمنع التصفية الصادرة العملاء المصابين من نشر دودة "الشفرة الحمراء" على الإنترنت العالمية.

الأنظمة الأساسية المدعومة

يتطلب الحل الموضح في هذا المستند ميزة التمييز المستندة إلى الفئة داخل برنامج Cisco IOS software. وعلى وجه الخصوص، تستخدم القدرة على المطابقة على أي جزء من عنوان URL HTTP ميزة تصنيف المنفذ الفرعي HTTP داخل NBAR. يتم أدناه تلخيص الأنظمة الأساسية المدعومة والحد الأدنى من متطلبات برنامج Cisco IOS:

النظام الأساسي	الحد الأدنى لبرنامج Cisco IOS
7200	12,1(5)T
7100	12,1(5)T
3745	12,2(8)T
3725	12,2(8)T
3660	12,1(5)T
3640	12,1(5)T
3620	12,1(5)T

2600	T(5)12,1
1700	T(2)12,2

ملاحظة: يلزمك تمكين إعادة التوجيه السريع من Cisco (CEF) لاستخدام NBAR.

تتوفر أيضا العلامات المستندة إلى الفئة وشريط الشبكة الموزع (NBAR) على الأنظمة الأساسية التالية:

النظام الأساسي	الحد الأدنى لبرنامج Cisco IOS
7500	E(6)12,1
FlexWAN	E(6)12,1

اكتشاف محاولة الإصابة في سجلات ويب IIS

تقوم محاولة الإصابة الأولية بإرسال طلب HTTP GET كبير إلى خادم IIS الهدف. تظهر بصمة "الرمز الأحمر" الأصلية أدناه:

```
GET /default.ida 80 10.1.1.75 - 10.101.17.216 16:32:23 2001-08-04
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u
7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403
```

يتم عرض "رمز أحمر" II على المساحة أدناه:

```
GET /default.ida XXXXXXXXXXX 80 10.1.1.75 - 10.7.35.92 15:57:35 2001-08-04
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090
u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%%
- u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a 403
```

لاحظ أن طلب GET يبحث دائما عن ملف بامتداد .ida. هذه سلسلة شائعة في جميع محاولات الإصابة وبالتالي يمكن إستخدامها كمعيار مطابقة مع العلامات المستندة إلى الفئة في IOS. لن يكون باقي طلب GET متناسقا بالضرورة لأنه يحاول فقط إنشاء تجاوز سعة التخزين المؤقت. ويمكن رؤية ذلك بمقارنة الادخالين المذكورين اعلاه.

وتفيد التقارير الآن بأن الفرق بين هذين التوقيعين يرجع إلى سلالة جديدة من الدودة "الشفرة الحمراء"، تسمى CodeRed.v3 أو CodeRed.C. يحتوي النوع الأصلي "Code Red" على السلسلة "NNNNNN" في طلب GET، بينما يحتوي النوع الجديد على "XXXXXXX". ارجع إلى Symantec Advisory للحصول على مزيد من التفاصيل.

في الساعة 6:24 مساء بتوقيت شرق الولايات المتحدة، 6 أغسطس 2001، سجلنا بصمة جديدة. ومنذ ذلك الحين تعلمنا أن هذه هي البصمة التي تركها برنامج eEye Vulnerability .

```
GET /x.ida AAAAAAAAAAAAA 80 10.1.1.9 - 10.30.203.202 22:24:02 2001-08-06
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
- AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=X 403 HTTP/1.1
```

كما يمكن لتقنية حظر "الرمز الأحمر" الواردة في هذا الاستشارة منع محاولات المسح هذه ببساطة من خلال تشديد تعريف خريطة الفئة كما هو موضح في القسم التالي.

وضع علامة "Code Red" على الهاكرز الوارد باستخدام ميزة التمييز المستندة إلى فئة IOS

لمنع الدودة "الشفرة الحمراء"، أستخدم إحدى الطرق الثلاث الموضحة أدناه. تصنف جميع الطرق الثلاث حركة المرور الضارة باستخدام ميزة Cisco IOS MQC. يتم بعد ذلك إسقاط حركة المرور هذه كما هو موضح أدناه.

الطريقة أ: إستخدام قائمة تحكم في الوصول (ACL)

تستخدم هذه الطريقة قائمة تحكم في الوصول (ACL) على واجهة الإخراج لإسقاط الحزم التي تم وضع علامة "رمز أحمر" عليها. لنستخدم الرسم التخطيطي للشبكة التالي لتوضيح الخطوات الواردة في هذه الطريقة:

فيما يلي خطوات تكوين هذه الطريقة:

1. قم بتصنيف أخطاء "الرمز الأحمر" الواردة باستخدام ميزة العلامة المستندة إلى الفئة في برنامج Cisco IOS، كما هو موضح أدناه:

```
Router(config)#class-map match-any http-hacks
"*Router(config-cmap)#match protocol http url "*default.ida
"*Router(config-cmap)#match protocol http url "*cmd.exe
"*Router(config-cmap)#match protocol http url "*root.exe
```

تبدو خريطة الفئة أعلاه داخل عناوين URL ل HTTP وتطابق أي من السلاسل المحددة. لاحظ أننا قمنا بتضمين أسماء ملفات أخرى إلى جانب الإعداد الافتراضي.IDA من "رمز أحمر". يمكنك إستخدام هذا الأسلوب لمنع محاولات قرصنة مماثلة، مثل فيروس Sadmind، والذي يتم شرحه في الوثائق التالية:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-078.asphttp://www.sophos.com/virusinfo/analyses/unixsadmind.html

2. قم بإنشاء سياسة واستخدم الأمر **set** لوضع علامة على عمليات الاختراق "Code Red" الواردة باستخدام خريطة سياسة. يستخدم هذا المستند قيمة DSCP قدرها 1 (عشرية) نظرا لأنه من غير المحتمل أن تكون أي حركة مرور أخرى على الشبكة تحمل هذه القيمة.هنا نقوم بوضع علامة "رمز أحمر" للقرصنة بخريطة سياسة تسمى "وضع علامة بالداخل-http-hacks".

```
Router(config)#policy-map mark-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap-c)#set ip dscp 1
```

3. قم بتطبيق النهج كسياسة واردة على واجهة الإدخال لوضع علامة "رمز أحمر" على الحزم القادمة.

```
Router(config)#interface serial 0/0
Router(config-if)#service-policy input mark-inbound-http-hacks
```

4. قم بتكوين قائمة تحكم في الوصول (ACL) تطابق قيمة DSCP الخاصة ب 1، كما تم تعيينها بواسطة نهج الخدمة.

```
Router(config)#access-list 105 deny ip any any dscp 1
Router(config)#access-list 105 permit ip any any
```

ملاحظة: يقدم برنامج Cisco IOS الإصدار 12.2(11) و 12.2T(11) دعم الكلمة الأساسية **السجل** في قائمة التحكم في الوصول (ACL) في التعريف على خرائط الفئة للاستخدام مع NBAR (CSCdv48172). إذا كنت

تستخدم إصدار أقدم، فلا تستخدم الكلمة الأساسية **log** على قائمة التحكم في الوصول (ACL). يؤدي ذلك إلى فرض تبديل جميع الحزم للعملية بدلا من تحويل CEF، ولن يعمل NBAR لأنه يتطلب CEF.

5. تطبيق قائمة التحكم في الوصول (ACL) الصادرة على واجهة الإخراج التي تتصل بخوادم الويب الهدف.

```
Router(config)#interface ethernet 0/1
Router(config-if)#ip access-group 105 out
```

6. تحقق من أن الحل يعمل كما هو متوقع. قم بتنفيذ الأمر **show access-list** وتأكد من زيادة قيمة "تطابق" عبارة الرفض.

```
Router#show access-list 105
Extended IP access list 105
(deny ip any any dscp 1 log (2406 matches
(permit ip any any (731764 matches
```

في خطوة التكوين، يمكنك أيضا تعطيل إرسال رسائل IP التي يتعذر الوصول إليها باستخدام الأمر **no ip** interface-level **unreachable** لتجنب التسبب في قيام الموجه بإنفاق الموارد الزائدة.لا يوصى باستخدام هذا الأسلوب إذا كان يمكنك توجيه حركة مرور بيانات DSCP=1 إلى قيمة خالية 0، كما هو موضح في قسم الطريقة B.

الطريقة ب: إستخدام التوجيه القائم على السياسة (PBR)

يستخدم هذا الأسلوب التوجيه المستند إلى السياسة لحظر الحزم التي تم وضع علامة "رمز أحمر" عليها. لا تحتاج إلى تطبيق الأوامر في هذه الطريقة إذا تم تكوين الطريقتين A أو C بالفعل.

فيما يلي الخطوات لتنفيذ هذه الطريقة:

1. تصنيف حركة المرور ووضع علامة عليها. أستخدم أوامر **class-map** و**policy-map** الموضحة في الطريقة A.
2. أستخدم الأمر **service-policy** لتطبيق النهج كسياسة واردة على واجهة الإدخال لوضع علامة على الحزم "رمز أحمر" الواردة. راجع الطريقة A.
3. قم بإنشاء قائمة تحكم في الوصول (ACL) إلى IP موسعة تطابق الحزم ذات العلامة "Code Red".

```
Router(config)#access-list 106 permit ip any any dscp 1
```

4. أستخدم الأمر **route-map** لإنشاء سياسة توجيه.

```
Router(config)#route-map null_policy_route 10
Router(config-route-map)#match ip address 106
Router(config-route-map)#set interface Null0
```

5. تطبيق خريطة المسار على واجهة الإدخال.

```
Router(config)#interface serial 0/0
Router(config-if)#ip policy route-map null_policy_route
```

6. تحقق من أن الحل لديك يعمل كما هو متوقع باستخدام الأمر **show access-list**. إذا كنت تستخدم قوائم التحكم في الوصول إلى الإخراج وقد قمت بتمكين تسجيل قائمة التحكم في الوصول، فيمكنك أيضا إستخدام أوامر **show log**، كما هو موضح أدناه:

```
Router#show access-list 106
Extended IP access list 106
(permit ip any any dscp 1 (1506 matches

Router#show log
:Aug 4 13:25:20: %SEC-6-IPACCESSLOGP
```

```
list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
:Aug 4 13:26:32: %SEC-6-IPACCESSLOGP
list 105 denied tcp A.B.C.D.(0) -> 10.1.1.75(0), 6 packets
```

نحن قادرون على إتخاذ القرار المرفوض على واجهة الدخول للموجه، بدلا من الحاجة إلى قائمة التحكم في الوصول للإخراج على كل واجهة مخرج. مرة أخرى، نوصي بتعطيل رسائل IP التي يتعذر الوصول إليها باستخدام الأمر **no ip unreachables**.

الطريقة ج: إستخدام النهج المستند إلى الفئة

هذه الطريقة عموما هي الأكثر قابلية للتطوير حيث أنها لا تعتمد على قوائم التحكم في الوصول (ACL) إلى الإخراج أو إلى PBR.

1. تصنيف حركة المرور باستخدام أوامر **class-map** الموضحة في الطريقة A.
2. قم بإنشاء سياسة باستخدام الأمر **policy-map** واستخدم الأمر **police** لتحديد إجراء إسقاط لحركة المرور هذه.

```
Router(config)#policy-map drop-inbound-http-hacks
Router(config-pmap)#class http-hacks
Router(config-pmap-c)#police 1000000 31250 31250
conform-action drop exceed-action drop violate-action drop
```

3. أستخدم الأمر **service-policy** لتطبيق النهج كسياسة واردة على واجهة الإدخال لإسقاط الحزم "رمز أحمر".

```
Router(config)#interface serial 0/0
Router(config-if)#service-policy input drop-inbound-http-hacks
```

4. تحقق من أن الحل لديك يعمل كما هو متوقع باستخدام الأمر **show policy-map interface**. تأكد من رؤية قيم متزايدة لفئة ومعايير مطابقة فردية.

```
Router#show policy-map interface serial 0/0

                                                    Serial0/0

                                  Service-policy input: drop-inbound-http-hacks

                                                        (Class-map: http-hacks (match-any
                                                                    packets, 300 bytes 5
                                      minute offered rate 0 bps, drop rate 0 bps 5
                                          "*Match: protocol http url "*default.ida
                                                                packets, 300 bytes 5
                                                                 minute rate 0 bps 5
                                              "*Match: protocol http url "*cmd.exe
                                                                 packets, 0 bytes 0
                                                                minute rate 0 bps 5
                                             "*Match: protocol http url "*root.exe
                                                                 packets, 0 bytes 0
                                                                minute rate 0 bps 5
                                                                           :police
                                    bps, 31250 limit, 31250 extended limit 1000000
                                      conformed 5 packets, 300 bytes; action: drop
                                         exceeded 0 packets, 0 bytes; action: drop
                                         violated 0 packets, 0 bytes; action: drop
                                      conformed 0 bps, exceed 0 bps, violate 0 bps

                                                            (Class-map: class-default (match-any
                                                                    packets, 300 bytes 5
                                      minute offered rate 0 bps, drop rate 0 bps 5
                                                                       Match: any
```

تقييدات NBAR

عند إستخدام NBAR مع الأساليب في هذا المستند، لاحظ أن الميزات التالية غير مدعومة من قبل NBAR:

- أكثر من 24 عنوان URL أو مضيف أو نوع MIME متطابق
- مطابقة ما بعد أول 400 بايت في عنوان URL
- حركة مرور غير خاصة ب IP
- أوضاع التحويل للبث المتعدد وغيرها من الأوضاع غير CEF
- حزم مجزأة
- طلبات HTTP الثابتة المجزأة
- تصنيف URL/المضيف/MIME/ باستخدام HTTP الآمن
- التدفقات غير المتماثلة مع البروتوكولات ذات الحالة
- الحزم التي يتم إنشاؤها من أو توجيهها إلى الموجه التي تعمل عبر NBAR

لا يمكنك تكوين NBAR على الواجهات المنطقية التالية:

- قناة EtherChannel السريعة
- الواجهات التي تستخدم الاتصال النفقي أو التشفير
- VLANs
- واجهات المتصل
- Multilink PPP

ملاحظة: يمكن تكوين NBAR على شبكات VLAN وفقا لبرنامج Cisco IOS، الإصدار 12.1(13)E، ولكنه مدعوم في مسار تحويل البرنامج فقط.

نظرا لأنه لا يمكن إستخدام NBAR لتصنيف حركة مرور الإخراج على إرتباط WAN حيث يتم إستخدام الاتصال النفقي أو التشفير، قم بتطبيقها بدلا من ذلك على واجهات أخرى على الموجه، مثل واجهة شبكة LAN، لإجراء تصنيف الإدخال قبل تحويل حركة مرور البيانات إلى إرتباط WAN للإخراج.

لمزيد من معلومات NBAR، راجع الروابط الموجودة في المعلومات ذات الصلة

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).