عافد زكرم ىلع SNORT_BPF ريغتم نيوكت

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
خطوات التكوين
أمثلة التكوين
السيناريو 1: تجاهل جميع حركات المرور، من ماسح ضوئي لتحديد الثغرات وإليه
السيناريو الثاني: تجاهل كل حركة المرور، من وإلى ماسحي إستشعار الضعف
السيناريو 3: تجاهل حركة مرور علامات VLAN، إلى ومن ماسحات ضوئية للضعف
السيناريو 4: تجاهل حركة مرور البيانات من خادم نسخ إحتياطي
السيناريو 5: لاستخدام نطاقات الشبكات بدلا من الأجهزة المضيفة الفردية

المقدمة

يمكنك إستخدام عامل تصفية حزم (BPF) Berkeley لاستبعاد مضيف أو شبكة من أن يتم فحصها بواسطة مركز دفاع. يستخدم Snort متغير **Snort_BPF** لاستبعاد حركة المرور من سياسة التسلل. يقدم هذا المستند تعليمات حول كيفية إستخدام متغير **snort_bpf** في سيناريوهات مختلفة.

تلميح: يوصى بشدة باستخدام قاعدة ثقة في سياسة التحكم في الوصول لتحديد حركة المرور التي يتم فحصها أو لا يتم فحصها، بدلا من BPF في سياسة الاقتحام. يتوفر المتغير **`snort_bpf`** في الإصدار 5.2 من البرنامج، ويتم إهماله في الإصدار 5.3 من البرنامج أو إصدار أحدث.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة على Defense Center، سياسة إقتحام، Berkeley ربط مرشح، و snort قاعدة.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات المكونات المادية والبرامج التالية:

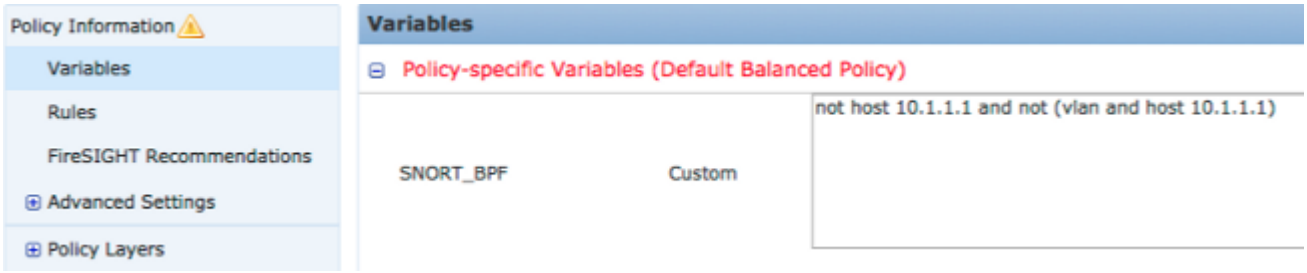
- مركز الدفاع
- برنامج إصدار 5.2

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.

خطوات التكوين

لتكوين متغير **snort_bpf**، اتبع الخطوات التالية:
1. الوصول إلى واجهة مستخدم ويب لمركز الدفاع.
2. انتقل إلى **السياسات > الاقتحام > سياسة الاقتحام**.
3. انقر فوق رمز *القلم الرصاص* لتحرير سياسة التطفل الخاصة بك.
4. انقر فوق **متغيرات** من القائمة الموجودة على اليسار.
5. بمجرد تكوين المتغيرات، سيتعين عليك حفظ التغييرات وإعادة تطبيق سياسة التطفل الخاصة بك حتى تصبح سارية المفعول.



الشكل: لقطة شاشة لصفحة تكوين متغير snort_bpf

أمثلة التكوين

وفيما يلي بعض الأمثلة الأساسية للرجوع إليها:

السيناريو 1: تجاهل جميع حركات المرور، من ماسح ضوئي لتحديد الثغرات وإليه

1. لدينا ماسح ضوئي للقابلية للتأثر على عنوان IP 10.1.1.1
2. نريد تجاهل كل حركات المرور من أو إلى الماسح الضوئي
3. قد تحتوي حركة المرور على علامة vlan) 802.1q) أو لا تحتوي عليها

ال **snort_bpf**:

```
(not host 10.1.1.1 and not (vlan and host 10.1.1.1
```

مقارنة: حركة مرور *ليس* VLAN-tagged، غير أن النقطتين 1 و 2 تبقى حقيقية ستكون:

```
not host 10.1.1.1
```

بلغة إنجليزية واضحة، فإن ذلك يتجاهل حركة المرور حيث أحد نقاط النهاية هي 10.1.1.1 (الماسح الضوئي).

السيناريو الثاني: تجاهل كل حركة المرور، من وإلى ماسحي إستشعار الضعف

1. لدينا ماسح ضوئي للقابلية للتأثر على عنوان IP 10.1.1.1
2. لدينا ماسح ضوئي ثان على عنوان IP 10.2.1.1
3. نريد تجاهل كل حركات المرور من أو إلى الماسح الضوئي
4. قد تحتوي حركة المرور على علامة 802.11 (vlan) أو لا تحتوي عليها

ال snort_bpf:

```
((not (host 10.1.1.1 or host 10.2.1.1) and not (vlan and (host 10.1.1.1 or host 10.2.1.1
```

مقارنة: حركة مرور *ليس* VLAN-tagged، غير أن النقطتين 1 و 2 تبقى حقيقية ستكون:

```
(not (host 10.1.1.1 or host 10.2.1.1
```

باختصار، قد يتجاهل ذلك حركة المرور حيث تكون إحدى نقاط النهاية 10.1.1.1 أو 10.2.1.1.

ملاحظة: من المهم ملاحظة أن علامة شبكة VLAN يجب أن تحدث، في جميع الحالات تقريبا، مرة واحدة فقط في إطار BPF معين. المرات الوحيدة التي يجب عليك رؤيتها أكثر من مرة، هي إذا كانت شبكتك تستخدم علامات تمييز متداخلة لشبكة VLAN (يشار إليها أحيانا باسم "QinQ").

السيناريو 3: تجاهل حركة مرور علامات VLAN، إلى ومن ماسحات ضوئية للضعف

1. لدينا ماسح ضوئي للقابلية للتأثر على عنوان IP 10.1.1.1
2. لدينا ماسح ضوئي ثان على عنوان IP 10.2.1.1
3. نريد تجاهل كل حركات المرور من أو إلى الماسح الضوئي
4. حركة مرور 802.11 (VLAN) حددت، وأنت تريد أن يستعمل خاص (VLAN) بطاقة، بما أن في VLAN 101

ال snort_bpf:

```
((not (host 10.1.1.1 or host 10.2.1.1) and not (vlan 101 and (10.1.1.1 or host 10.2.1.1
```

السيناريو 4: تجاهل حركة مرور البيانات من خادم نسخ إحتياطي

1. لدينا خادم نسخ إحتياطي للشبكة على عنوان IP 10.1.1.1
2. تتصل الأجهزة الموجودة على الشبكة بهذا الخادم على المنفذ 8080 لتشغيل النسخ الاحتياطي الليلي الخاص بها
3. إننا نرغب في تجاهل حركة مرور النسخ الاحتياطي هذه، حيث إنها مشفرة وبحجم كبير

ال snort_bpf:

```
not (dst host 10.1.1.1 and dst port 8080) and not (vlan and (dst host 10.1.1.1
((and dst port 8080
```

مقارنة: حركة مرور *ليس* VLAN-tagged، غير أن النقطتين 1 و 2 تبقى حقيقية ستكون:

```
(not (dst host 10.1.1.1 and dst port 8080
```

ترجمت، هذا يعني أن حركة المرور إلى 10.1.1.1 (خادم النسخ الاحتياطي الافتراضي الخاص بنا) على المنفذ 8080 (منفذ الاستماع) يجب ألا يتم فحصها بواسطة محرك اكتشاف IPS.

من الممكن أيضا إستخدام net بدلا من المضيف لتحديد كتلة شبكة، بدلا من مضيف واحد. على سبيل المثال:

```
not net 10.1.1.0/24
```

وبصفة عامة، من الممارسات الجيدة أن تجعل ملف BPF محددا قدر الإمكان؛ مع إستبعاد حركة المرور من التفتيش التي يلزم إستبعادها، مع عدم إستبعاد أي حركة مرور غير مرتبطة قد تحتوي على محاولات إستغلال.

السيناريو 5: لاستخدام نطاقات الشبكات بدلا من الأجهزة المضيفة الفردية

يمكنك تحديد نطاقات الشبكة في متغير BPF بدلا من البيئات المضيفة لتقصير طول المتغير. للقيام بذلك، سوف تستخدم الكلمة الأساسية net بدلا من المضيف وتحدد نطاق CIDR (التوجيه المتبادل بين المجالات بدون فئات). فيما يلي مثال:

```
not (dst net 10.8.0.0/16 and dst port 8080) and not (vlan and (dst net 10.8.0.0/16
((and dst port 8080
```

ملاحظة: الرجاء التأكد من إدخال عنوان الشبكة باستخدام تدوين توجيه المجال التبادلي دون فئات (CIDR) وعنوان قابل للاستخدام داخل مساحة عنوان كتلة توجيه المجال التبادلي دون فئات (CIDR). على سبيل المثال، أستخدم net 10.8.0.0/16 بدلا من net 10.8.2.16/16.

يعرض الأمر **SNORT_BPF** يتم إستخدام المتغير لمنع فحص حركة مرور معينة بواسطة محرك كشف IPS؛ غالبا لأسباب تتعلق بالأداء. يستخدم هذا المتغير تنسيق عوامل تصفية حزمة Berkeley القياسية (BPF). حركة المرور المطابقة **SNORT_BPF** سيتم فحص المتغير، بينما لا تتطابق حركة المرور مع **SNORT_BPF** لن يتم فحص المتغير بواسطة محرك كشف IPS.

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).