فهم قواعد snort3

المحتويات

المقدمة

يصف هذا المستند قواعد لـ Snort3 المحرك في Cisco Secure Firewall Threat Defense (FTD).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco Secure Firewall Threat Defense (FTD)
- Intrusion Prevention System (IPS)
- Snort2 بناء جملة

الترخيص

لا توجد متطلبات ترخيص محددة، ويدعم الترخيص الأساسي كافي، كما يتم تضمين الميزات المذكورة في محرك Snort داخل FTD وفي إصدارات Snort3 مفتوحة المصدر.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco Secure Firewall Threat Defense (FTD),Cisco Secure Firewall Management Center (FMC) الإصدار 7.0+ مع Snort3.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة.

بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

Snort هو محرك Cisco IPS القادر على تحليل حركة مرور البيانات في الوقت الفعلي وتسجيل الحزم.

Snort إجراء تحليل للبروتوكول، والبحث عن المحتوى، واكتشاف الهجمات.

Snort3 عبارة عن إصدار محدث من نظام منع الاختراقات (IPS) طرازSnort2 مزود ببنية برامج جديدة تعمل على تحسين الأداء واكتشاف المشكلات وقابلية التطوير وسهولة الاستخدام.

قواعد Snort3

يستعملون تنسيق LUA هذا Snort3 قواعد أسهل في القراءة والكتابة والتحقق.

إجراءات القاعدة

يقوم هذا الإصدار الجديد بتغيير إجراءات القاعدة، وتكون التعريفات الجديدة:

- **Pass**: إيقاف تقييم القواعد اللاحقة في حالة الحزمة
- **Alert**: إنشاء حدث فقط
- **Block**: إسقاط الحزمة، حظر جلسة المتبقي
- **Drop**: إسقاط الحزمة فقط
- **Rewrite**: مطلوب في حالة إستخدام خيار الاستبدال
- **React**: إرسال صفحة إستجابة كتلة HTML
- **Reject**: إدخال TCP RST أو ICMP الذي يتعذر الوصول إليه

تشريح القاعدة

التشريح هو:

يحتوي رأس القاعدة على الإجراء والبروتوكول وشبكة (شبكات) المصدر والوجهة والمنفذ (المنافذ).

في Snort3، يمكن أن يكون رأس القاعدة أحد الخيارات التالية:

- رأس قاعدة الخدمة

```
<iline" lang="lua">alert http ( msg:"Alert HTTP rule"; flow:to_client,established;
content:"evil", nocase; sid:1000001; )
```

- رأس قاعدة الملف

```
alert file ( msg: “Alert File example”; file_data; content:”malicious_stuff”; sid:1000006; )
```

- رأس القاعدة التقليدية

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"Alert HTTP rule";
flow:to_client,established; content:"evil", nocase; sid:1000001; )
```

مميزات القاعدة

بعض المميزات الجديدة هي:

- مساحة بيضاء عشوائية (كل خيار على سطره الخاص)

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS ( msg:"Alert TCP rule";
flow:to_client,established; content:"evil", nocase; sid:1000000; )
```

- الاستخدام المتسق لـ و

```
content:"evil", offset 5, depth 4, nocase;
```

- الشبكات والمنافذ إختيارية

```
alert http ( Rule body )
```

- إضافة المزيد من المخازن المؤقتة اللاصقة (هذه ليست القائمة الكاملة)

```
http_uri http_raw_uri http_header http_raw_header http_trailer http_raw_trailer http_cookie
http_raw_cookie http_true_ip http_client_body http_raw_body http_method http_stat_code
http_stat_msg http_version http2_frama_header script_data raw_data
```

- تعليقات النمط C

```
alert http ( msg:"Alert HTTP rule"; /* I can write a comment here */ ... )
```

- الكلمة الأساسية ملاحظة (rem)

```
alert http ( msg:"Alert HTTP rule"; flow:to_client,established; rem:"Put comments in the rule
anywhere"; content:"evil", nocase; sid:1000001; )
```

- كلمات أساسية لـ appids

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any ( msg:"Alert on apps"; appids:"Google, Google
Drive"; content:"evil", nocase; sid:1000000; )
```

- sd_pattern لتصفية البيانات الحساسة
- الكلمة الأساسية Regex مع إستخدام تقنية HyperFlex
- تستبدل الكلمة الأساسية للخدمة البيانات الأولية

الأمثلة

مثال عن رأس خدمة http و http_uri المخزن المؤقت اللاصق

المهمة: اكتب قاعدة تكشف الكلمة **malicious** في URI لـ HTTP.

الحل:

```
alert http ( msg:"Snort 3 http_uri sticky buffer"; flow:to_server,established; http_uri;
content:"malicious", within 20; sid:1000010; )
```

مثال مع رأس خدمة الملف

المهمة: اكتب قاعدة تكتشف ملفات PDF.

الحل:

```
alert file ( msg:"PDF File Detected"; file_type: "PDF"; sid:1000008; )
```

روابط ذات صلة

تنزيل برنامج IDS و قواعد التشغيل

جيثوب

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).