المرحلة 7 من أستكشاف أخطاء مسار بيانات Firepower وإصلاحها: نهج الاقتحام

المحتويات

المقدمة

هذه المقالة هي جزء من سلسلة مقالات توضح كيفية أستكشاف مسار البيانات في أنظمة FirePOWER وإصلاحها بشكل منهجي لتحديد ما إذا كانت مكونات FirePOWER قد تؤثر على حركة المرور. يرجى الرجوع إلى [مقالة "نظرة عامة"](#) للحصول على معلومات حول بنية الأنظمة الأساسية FirePOWER وارتباطاتها بمقالات "أستكشاف أخطاء مسارات البيانات وإصلاحها" الأخرى.

تغطي هذه المقالة المرحلة السابعة من أستكشاف أخطاء مسار بيانات FirePOWER وإصلاحها، وهي ميزة "سياسة التسلل".

المتطلبات الأساسية

- تنطبق هذه المقالة على جميع منصات FirePOWER التي تقوم بتشغيل سياسة الاختراق لا تتوفر ميزة **التتبع** إلا في الإصدار 6.2 وما بعده للنظام الأساسي للدفاع عن تهديد FirePOWER (FTD) فقط
- معرفة مصدر الشخر المفتوح مفيدة، على الرغم من أنها غير مطلوبة لمزيد من المعلومات حول برنامج Open Source Snort، يرجى زيارة موقع https://www.snort.org/

أستكشاف أخطاء مرحلة سياسة الاقتحام وإصلاحها

إستخدام أداة "التتبع" لاكتشاف حالات إسقاط سياسة الاقتحام (في وضع FTD فقط)

يمكن تشغيل أداة تتبع دعم النظام من واجهة سطر أوامر FTD (CLI). وهذه مشابه لأداة **تصحيح أخطاء محرك الحماية** المذكورة في [مقال](#) مرحلة سياسة التحكم بالوصول، باستثناء أنها تتعمق بشكل أعمق في طرق العمل الداخلية لتقنية Snort. قد يكون هذا مفيدا لمعرفة ما إذا كان هناك أي قواعد لسياسة الاقتحام سيتم تشغيلها على حركة المرور المثيرة

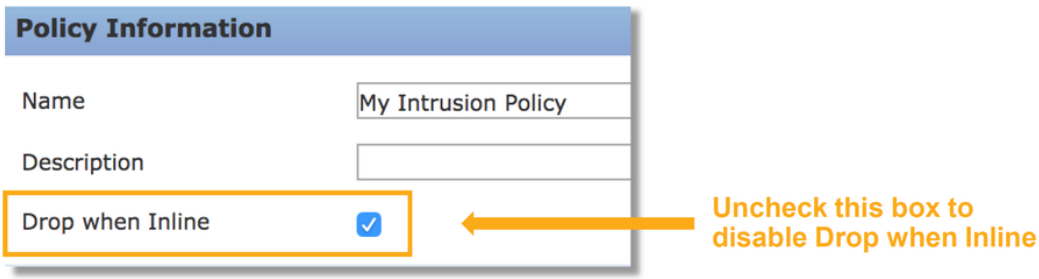
للاهتمام.

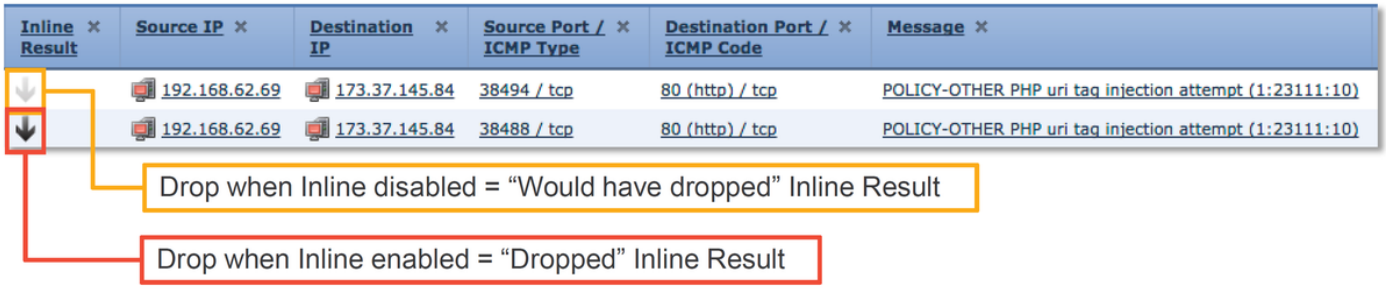
في المثال التالي، يتم حظر حركة المرور من المضيف بعنوان IP 192.168.62.6 بواسطة قاعدة سياسة التسلل (في هذه الحالة، **1:2311**)

```
> system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[... output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38488 6 Packet: TCP, ACK, seq 3594105349, ack 3856774965
173.37.145.84-80 - 192.168.62.69-38488 6 AppID: service HTTP (676), application Cisco (2655)
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://www.cisco.com/<?php") returned 0
...
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38488 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38488 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, drop
192.168.62.69-38488 > 173.37.145.84-80 6 AS 1 I 0 Deleting session
192.168.62.69-38488 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict BLACKLIST
192.168.62.69-38488 > 173.37.145.84-80 6 ===> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

لاحظ أن الإجراء المطبق من قبل الشيري كان **إسقاط**. عندما كشفت عملية إسقاط بواسطة الشيري، فإن تلك الجلسة الخاصة عندئذ يتم وضعها في القائمة السوداء حتى أن أي حزم إضافية يتم إسقاطها أيضا.

يتمثل السبب وراء قدرة المشرف على تنفيذ إجراء **الإسقاط** في تمكين خيار "الإسقاط عندما يكون مضمنا" ضمن نهج التسلل. يمكن التحقق من هذا الإجراء في صفحة الإنزال الأولية ضمن نهج الاقتحام. في مركز إدارة Firepower (FMC)، انتقل إلى **السياسات > التحكم في الوصول > التطفل** وانقر فوق رمز التحرير الموجود بجوار السياسة المعنية.





إذا تم تعطيل "الإسقاط عندما يكون مضمنا"، لم يعد الشيري يقوم بإسقاط الحزم المسيئة، ولكنه يظل ينبه **بنتيجة مضمنة** ل "كان سيسقط" في أحداث التسلل.

مع تعطيل "الإسقاط عندما يكون السطر مضمنا"، يظهر إخراج التتبع إجراء **سيسقط**

لجلسة مرور البيانات المعنية.

```
> system support trace


Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.69
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages

[… output omitted for brevity]

173.37.145.84-80 - 192.168.62.69-38494 6 Packet: TCP, ACK, seq 2900935719, ack 691924600
173.37.145.84-80 - 192.168.62.69-38494 6 AppID: service HTTP (676), application Cisco (2655)
…
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 I 0 match rule order 5, 'inspect it all', action Allow
192.168.62.69-38494 > 173.37.145.84-80 6 AS 1 I 0 allow action
192.168.62.69-38494 > 173.37.145.84-80 6 Firewall: allow rule, 'inspect it all', allow
192.168.62.69-38494 > 173.37.145.84-80 6 IPS Event: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 Snort detect_drop: gid 1, sid 23111, would drop
192.168.62.69-38494 > 173.37.145.84-80 6 NAP id 1, IPS id 0, Verdict PASS
192.168.62.69-38494 > 173.37.145.84-80 6 ===> Blocked by IPS
Verdict reason is sent to DAQ's PDTS
```

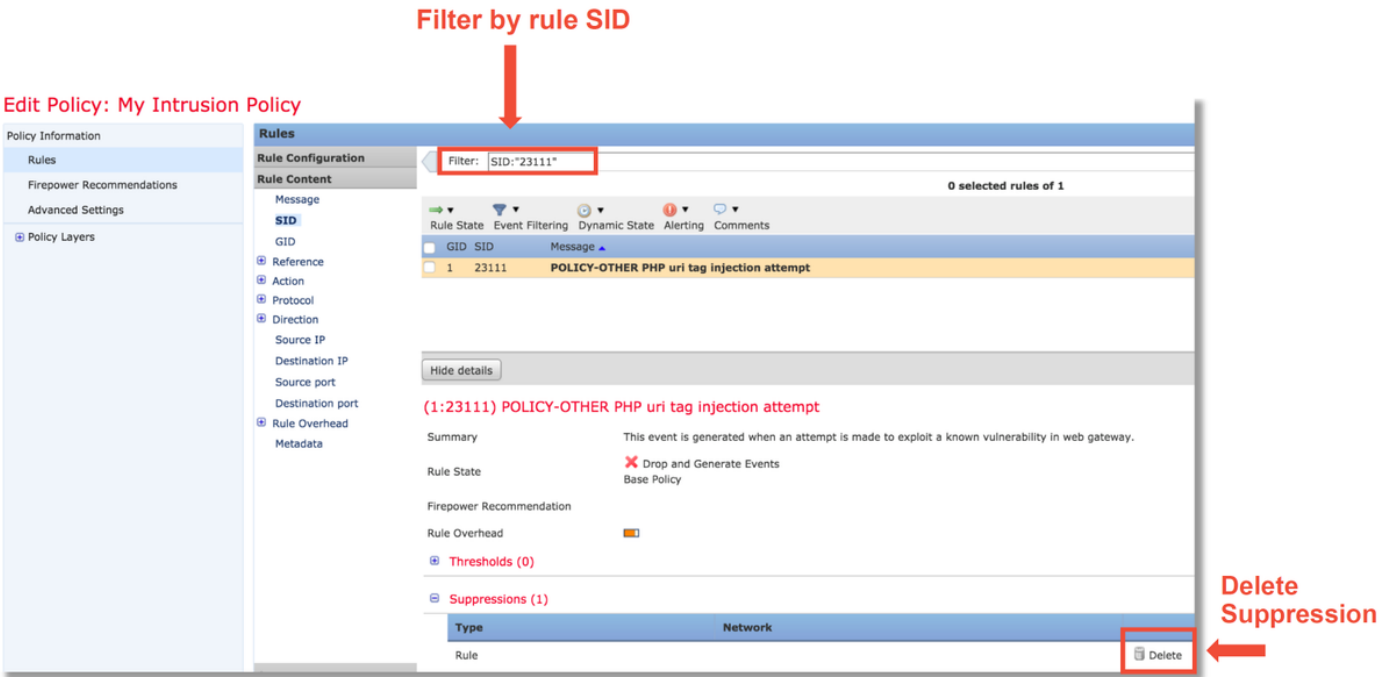
تحقق من وجود حالات قمع في نهج التطفل

من الممكن أن يقوم الشرخ بإسقاط حركة المرور دون إرسال أحداث التطفل إلى FMC (إسقاط بصمت). ويتحقق ذلك من خلال تكوين **عمليات القمع**. للتحقق مما إذا تم تكوين أي قمع في "نهج التسلل"، يمكن فحص "طبقة الخبراء" على الطرف الخلفي، كما هو موضح أدناه.

```
[ Look for suppressions ]
> expert
$ cd /var/sf/detection_engines/*/
$ grep -H '^suppress' intrusion/*/snort_suppression.conf
intrusion/68acdfa2-e31a-11e6-b866-dd9e65c01d56/snort_suppression.conf:suppress gen_id 1, sig_id 23111

[ Get the policy name ]
$ grep Name intrusion/snort.conf.68acdfa2-e31a-11e6-b866-dd9e65c01d56
# Name        : My Intrusion Policy
```

لاحظ أن سياسة التطفل التي تسمى "سياسة التطفل الخاصة بي" تحتوي على قمع القاعدة 1:2311. لذلك، يمكن إسقاط حركة المرور بسبب هذه القاعدة، دون أي أحداث. وهذا سبب آخر يجعل أداة التتبع مفيدة، حيث أنها لا تزال تظهر حالات الهبوط التي تحدث.

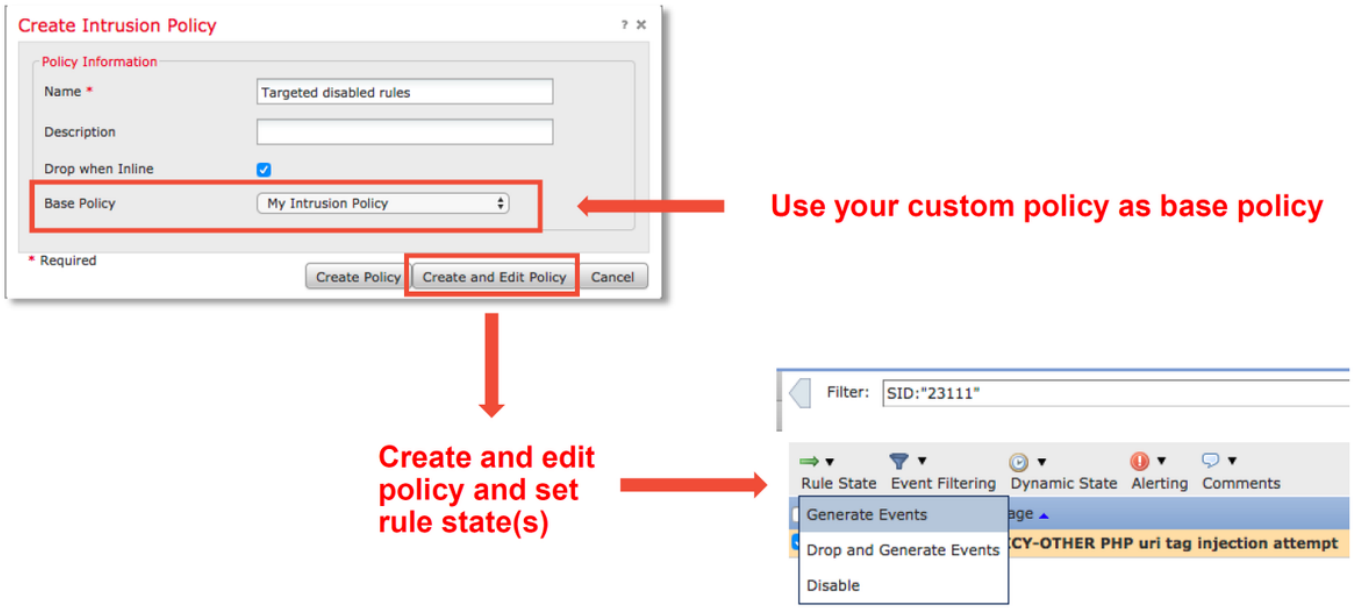
لحذف القمع، يمكن تصفية القاعدة المعنية ضمن طريقة عرض **قواعد** سياسة التسلل. وهذا يطرح خيارا لحذف القمع، كما هو موضح أدناه.



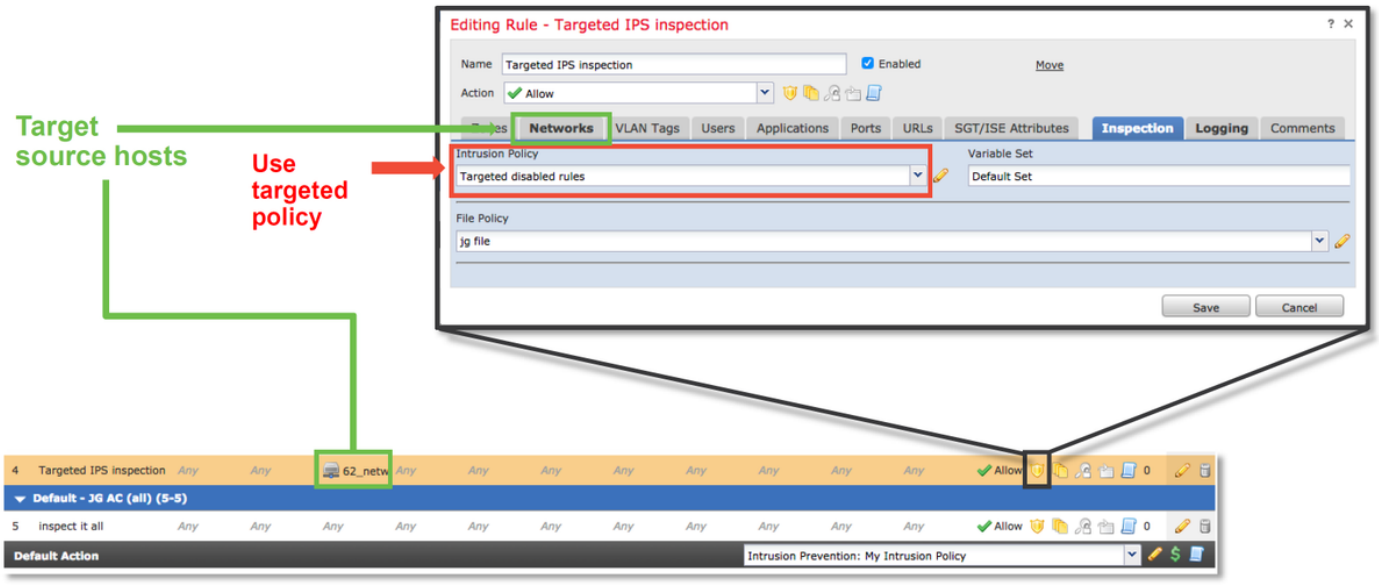
إنشاء سياسة أختراق مستهدفة

إذا تم إسقاط حركة المرور بواسطة قاعدة معينة من قواعد نهج الاقتحام، فقد لا ترغب في إسقاط حركة المرور المعينة ولكن قد لا ترغب أيضا في تعطيل القاعدة. الحل هو إنشاء سياسة إقتحام جديدة مع تعطيل القاعدة (القواعد) المخالفة ثم جعلها تقيم حركة مرور البيانات من الأجهزة المضيفة المستهدفة.

وفيما يلي مثال على كيفية إنشاء سياسة الاقتحام الجديدة (ضمن **السياسات > التحكم في الوصول > الاقتحام**).



وبعد إنشاء سياسة الاقتحام الجديدة، يمكن إستخدامها بعد ذلك ضمن قاعدة جديدة لسياسة التحكم بالوصول تستهدف المضيفين المعنيين، الذين تم إسقاط حركة المرور الخاصة بهم من قبل سياسة الاقتحام الأصلية.



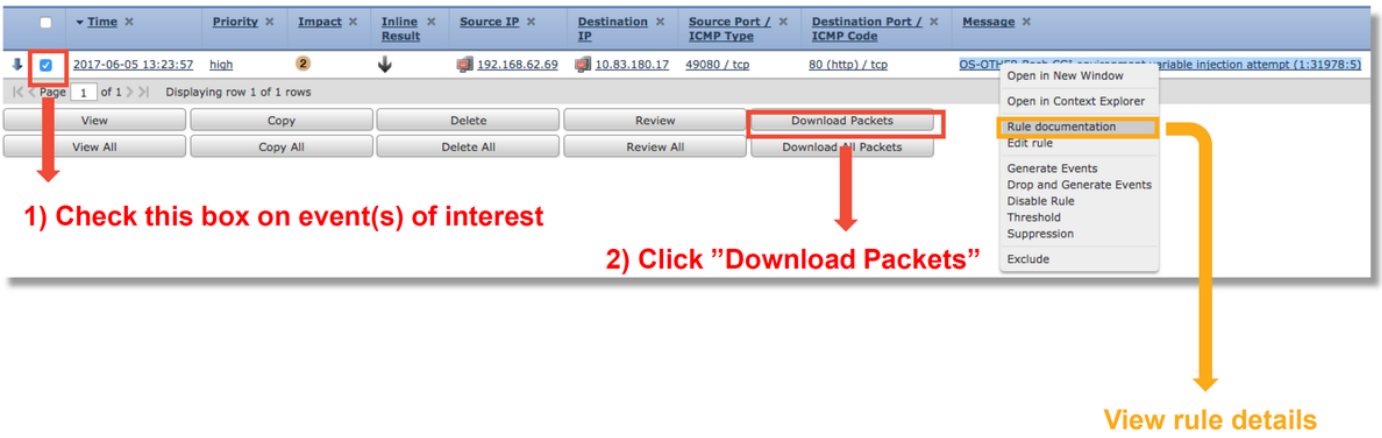
أستكشاف الأخطاء وإصلاحها بشكل إيجابي خاطئ

أحد السيناريوهات الشائعة هي التحليل الإيجابي الكاذب لأحداث الاختراق. هناك عدة أشياء يمكن فحصها قبل فتح قضية إيجابية خاطئة.

1. من صفحة **عرض جدول أحداث التسلل**، انقر فوق خانة الاختيار الخاصة بالحدث المعني

2. انقر فوق **تنزيل الحزم** للحصول على الحزم التي تم التقاطها بواسطة الشخير عند تشغيل حدث الاقتحام.

3. انقر بزر الماوس الأيمن فوق اسم القاعدة في عمود **الرسالة** ثم **وثائق القاعدة**، للاطلاع على صياغة القاعدة والمعلومات الأخرى ذات الصلة.



فيما يلي صياغة القاعدة للقاعدة التي أدت إلى تشغيل الحدث في المثال أعلاه. تكون أجزاء القاعدة التي يمكن التحقق منها مقابل ملف التقاط الحزمة (PCAP) الذي تم تنزيله من FMC لهذه القاعدة غامقة.

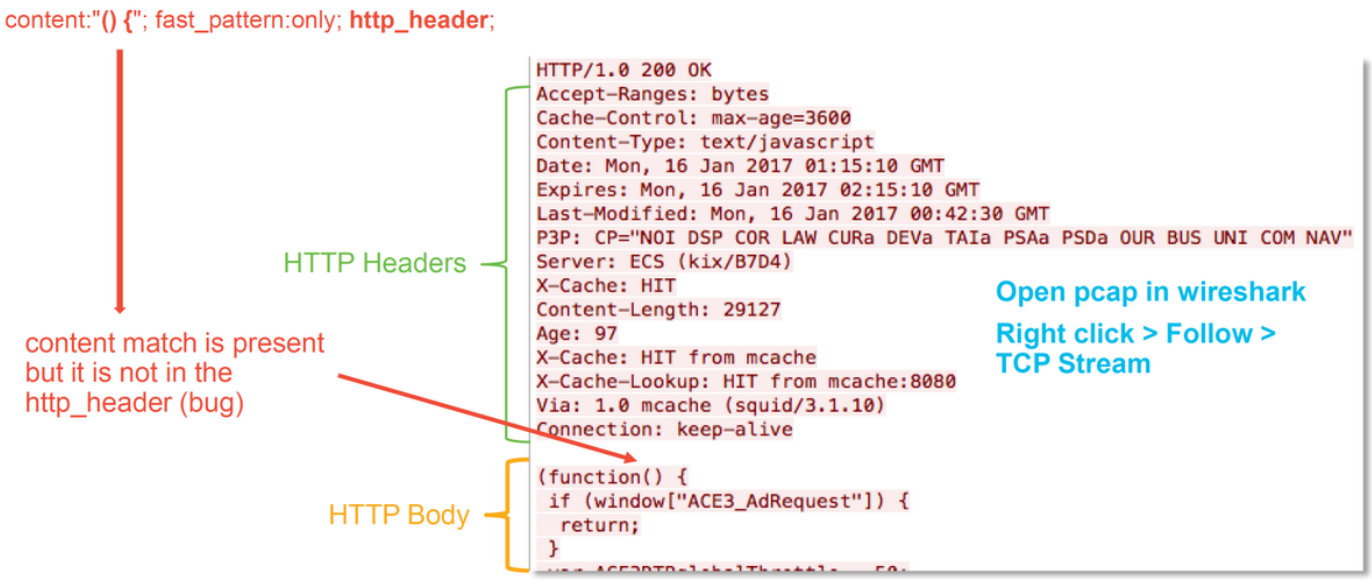
تنبيه TCP$EXTERNAL_NET أي -> $HOME_NET$HTTP_PORTS \
(msg:"محاولة حقن متغير بيئة OS-OTHER BASH CGI"؛ \
التدفق:to_server، تم إنشاؤه؛ \
المحتوى:() {"؛ fast_pattern:فقط؛ http_header؛ \
بيانات التعريف:policy balanced-ipsdrop، policy max-detect-ipsdrop، policy security-ipsdrop،

ruleEt community، **service http**؛ \
المرجع:CVE،2014-6271؛ المرجع:CVE،2014-6277؛ المرجع:CVE،2014-6278؛ المرجع:CVE،2014-7169؛ \
classtype:attempted-admin؛ \
sid:31978؛ rev:5؛)

ويمكن بعد ذلك اتباع هذه الخطوات الأولية لإجراء عملية التحليل، لمعرفة ما إذا كان يجب أن تتطابق حركة المرور مع القاعدة التي تم تشغيلها.

1. تحقق من قاعدة التحكم في الوصول التي تطابقت معها حركة المرور. يتم العثور على هذه المعلومات كجزء من الأعمدة الموجودة في علامة التبويب "أحداث التسلل".
2. العثور على مجموعة المتغيرات المستخدمة في قاعدة التحكم بالوصول المذكورة. يمكن عندئذ مراجعة مجموعة المتغيرات تحت **الكائنات > إدارة الكائن > مجموعات المتغيرات**
3. تأكد من أن عناوين IP في متغيرات ملف PCAP (في هذه الحالة، مضيف مضمن في متغير **$EXTERNAL_NET** متصل بمضيف مضمن في تكوين متغير **$HOME_NET**)
4. بالنسبة **للتدفق**، قد يلزم التقاط جلسة عمل/اتصال كامل. لن يلتقط الشخير التدفق الكامل لأسباب تتعلق بالأداء. ومع ذلك، في معظم الحالات، من الآمن افتراض أنه إذا تم تأسيس قاعدة مع flow:enabled triggered، فإنه تم إنشاء الجلسة في الوقت الذي تم فيه تشغيل القاعدة، لذلك ال يكون ملف PCAP الكامل ضروريا للتحقق من هذا الخيار في قاعدة شخير. ولكن قد يكون من المفيد أن نفهم بشكل أفضل السبب وراء إطالق النار.
5. للحصول على **http للخدمة**، راجع ملف PCAP في Wireshark لترى ما إذا كان يبدو كحركة مرور HTTP. إذا تم تمكين اكتشاف الشبكة للمضيف وشوهد التطبيق "HTTP" من قبل، فقد يؤدي ذلك إلى مطابقة الخدمة في جلسة عمل.

مع وضع هذه المعلومات في االعتبار، يمكن إعادة النظر في الحزمة (الحزم) التي تم تنزيلها من وحدة التحكم في إدارة اللوحة الأساسية (FMC) في Wireshark. يمكن تقييم ملف PCAP لتحديد ما إذا كان الحدث الذي تم تشغيله إيجابيا خاطئا أم ال.



في الرسم التوضيحي أعاله، المحتوى الذي تكشف عنه القاعدة كان موجودا في ملف PCAP - **"() {"**

ومع ذلك، تحدد القاعدة أنه يجب الكشف عن المحتوى في رأس HTTP الخاص بالحزمة - **http_header**

في هذه الحالة، تم العثور على المحتوى في نص HTTP. لذلك هذا موجب خاطئ. لكنه ليس موجبا بالطبع بمعنى ان القاعدة تكتب بطريقة غير صحيحة. القاعدة صحيحة والكن يمكن تحسينها في هذه الحالة. من المحتمل أن يكون هذا المثال في مواجهة خطأ غير متوقع

يتسبب في حدوث إرتباك في المخزن المؤقت في الشرخ. هذا يعني أن Snort قد عرف http_headers بشكل غير صحيح.

في هذه الحالة، يمكنك التحقق من وجود أي أخطاء لمحرك snort/IPS في الإصدار الذي يقوم الجهاز بتشغيله، وإذا لم يكن هناك أي أخطاء، يمكن فتح حالة مع مركز المساعدة التقنية (TAC) من Cisco. يلزم التقاط جلسة العمل الكاملة للتحقيق في مشكلة مثل أن فريق Cisco يحتاج إلى مراجعة كيفية دخول Snort إلى هذه الحالة، والذي لا يمكن القيام به باستخدام حزمة واحدة.

مثال إيجابي حقيقي

يوضح الرسم التوضيحي التالي تحليل الحزمة لنفس حدث الاختراق. هذه المرة، يكون الحدث موجبا حقيقيا لأن المحتوى الظاهر في رأس HTTP.

البيانات التي سيتم تقديمها إلى TAC

البيانات	تعليمات
أستكشاف أخطاء الملف وإصلاحها من جهاز FirePOWER الذي يقوم بفحص حركة المرور حزم الالتقاط التي تم تنزيلها من FMC	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techn
أي إخراج سطر واجهة الأوامر (CLI) ذي صلة تم تجميعه، مثل إخراج التتبع	طالع هذه المقالة للحصول على تعليمات
	طالع هذه المقالة للحصول على تعليمات

الخطوات التالية

إذا تم تحديد أن مكون سياسة الاقتحام ليس هو سبب المشكلة، فإن الخطوة التالية ستكون أستكشاف ميزة "سياسة تحليل الشبكة" وإصلاحها.

انقر هنا للمتابعة إلى المقالة الأخيرة.

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).