تنزيل بيانات الحزمة (ملف PCAP) باستخدام واجهة مستخدم الويب

المحتويات

المقدمة

باستخدام واجهة مستخدم الويب، يمكنك تنزيل الحزمة (الحزم) التي أدت إلى تشغيل قاعدة snort.يوفر المقال الخطوات اللازمة لتنزيل بيانات التقاط الحزمة (ملف PCAP) باستخدام واجهة مستخدم الويب الخاصة بنظام إدارة Sourcefire FireSIGHT.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بجهاز Sourcefire FirePOWER ونماذج الأجهزة الظاهرية.

المكونات المستخدمة

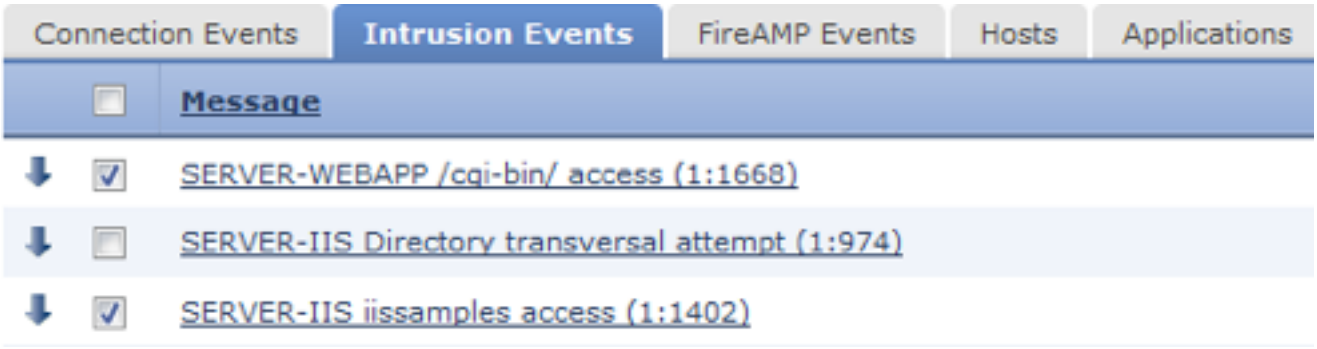
تستند المعلومات الواردة في هذا المستند إلى Sourcefire FireSIGHT Management Center، المعروف أيضا باسم Defense Center، الذي يشغل الإصدار 5.2 من البرنامج أو إصدار أحدث.

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 لتنزيل ملف PCAP

الخطوة 1: تسجيل الدخول إلى مركز حماية Sourcefire أو مركز إدارة، والتنقل إلى صفحة أحداث التسلل كما يلي:

الخطوة 2: باستخدام خانة الاختيار، حدد الحدث (الأحداث) الذي تريد تنزيل بيانات التقاط الحزمة (ملف PCAP).



الخطوة 3: انزلاق إلى أسفل الصفحة وإما:

- انقر فوق تنزيل الحزمة لتنزيل الحزم التي أدت إلى تشغيل حدث (أحداث) الاقتحام المحددة
- انقر فوق تنزيل جميع الحزم لتنزيل جميع الحزم التي أدت إلى أحداث التطفل في طريقة العرض المقيدة الحالية

ملاحظة: سيتم حفظ الحزم التي تم تنزيلها على هيئة PCAP. إذا كنت تريد تحليل التقاط الحزمة، ستحتاج إلى تنزيل وتثبيت برنامج قادر على قراءة ملف PCAP.

الخطوة 4: عندما يطلب منك، احفظ ملف PCAP إلى قرصك الصلب.

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).