كيف تستخدم تعابير عادية (regex) مع GREP للبحث في السجلات؟

المحتويات

سؤال

كيف تستخدم تعابير عادية (regex) مع GREP للبحث في السجلات؟

البيئة

أجهزة أمان الويب من Cisco
أجهزة أمان البريد الإلكتروني Cisco Email Security Appliance
أجهزة إدارة الأمان من Cisco

الحل

العبارات العادية (regex) يمكن أن تكون أداة قوية عند إستخدامها مع الأمر "grep" للبحث خلال السجلات المتاحة على الجهاز، مثل سجلات الوصول وسجلات الوكيل وغيرها. يمكننا البحث في السجلات بناء على موقع الويب، أو أي جزء من عنوان ربط URL، أو أسماء المستخدمين، لتسمية البعض، عند إستخدام أمر واجهة سطر الأوامر ((CLI grep"".

فيما يلي بعض السيناريوهات الشائعة حيث يمكنك إستخدام regex مع GREP للمساعدة في أستكشاف الأخطاء وإصلاحها.

السيناريو 1: العثور على موقع ويب معين في سجلات الوصول

السيناريو الأكثر شيوعا هو محاولة العثور على طلبات يتم إجراؤها على موقع ويب في سجلات الوصول الخاصة بجهاز أمان الويب (WSA) من Cisco.

على سبيل المثال:
قم بالاتصال بالجهاز عبر SSH. ما إن يتلقى أنت الإيعاز، نحن يستطيع كتبت الأمر "grep" أن يسرد السجلات المتاحة.

CLI> GREP
أدخل رقم السجل الذي ترغب في "GREP". []> 1 (أختر # لسجلات الوصول هنا)
أدخل التعبير العادي إلى "grep". []> **موقع الويب\.com**

السيناريو 2: محاولة العثور على ملحق ملف معين أو مجال من المستوى الأعلى

يمكننا إستخدام الأمر "grep" للعثور على امتداد ملف معين (.pptx، .doc) في عنوان ربط أو مجال على المستوى الأعلى (.org، .com).

على سبيل المثال:
للعثور على جميع عناوين URL التي تنتهي ب .crl يمكننا إستخدام regex التالي: **\.crl$**

للعثور على جميع عناوين URL التي تحتوي على امتداد الملف .pptx، يمكننا إستخدام regex التالي: **\.pptx**

السيناريو 3: محاولة العثور على كتلة معينة لموقع ويب

عند البحث عن موقع ويب معين، قد نقوم أيضا بالبحث عن إستجابة HTTP معينة.

على سبيل المثال:
إذا أردنا البحث عن كافة رسائل TCP_DENY/403 ل domain.com، فيمكننا إستخدام regex التالي:
tcp_deny/403.*domain\.com

السيناريو 4: العثور على اسم جهاز في سجلات الوصول

عند إستخدام نظام مصادقة NTLMSSP، قد نصادف مثيلا يقوم فيه وكيل المستخدم (Microsoft NCSI هو الأكثر شيوعا) بإرسال بيانات اعتماد الجهاز بشكل غير صحيح بدلا من بيانات اعتماد المستخدم عند المصادقة. لتعقب عنوان URL/عامل المستخدم الذي يسبب ذلك، يمكننا إستخدام regex مع "GREP" لعزل الطلب الذي تم إجراؤه عند حدوث المصادقة.

إذا لم يكن لدينا اسم الجهاز الذي تم إستخدامه، يمكننا إستخدام "GREP" والعثور على جميع أسماء الأجهزة التي تم إستخدامها كأسماء مستخدمين عند المصادقة باستخدام regex التالي: **\$@**

ما إن يصبح لدينا الخط حيث يقع هذا، نحن يستطيع ال GREP لاسم الآلة المحدد أن كان استعملت ب يستعمل التالي
$\regex:MachineName

يجب أن يكون الإدخال الأول الذي يظهر هو الطلب الذي تم إجراؤه عند مصادقة المستخدم باسم الجهاز بدلا من اسم المستخدم.

السيناريو 5: العثور على فترة زمنية محددة في سجلات الوصول

بشكل افتراضي، لن تتضمن اشتراكات سجل الوصول الحقل الذي يظهر التاريخ/الوقت القابل للقراءة. إذا أردنا التحقق من سجلات الوصول لفترة زمنية معينة، فيمكننا اتباع الخطوات التالية:

ابحث عن الطابع الزمني ل UNIX من موقع مثل http://www.onlineconversion.com/unix_time.htm. بمجرد حصولك على الطابع الزمني، يمكنك البحث عن وقت معين داخل سجلات الوصول.

على سبيل المثال:
طابع وقت UNIX ل 1325419200 يعادل 2012/01/01 12:00:00.

يمكننا إستخدام إدخال regex التالي للبحث في سجلات الوصول في حوالي الساعة 12:00 من يوم 1 يناير 2012:
13254192

السيناريو 6: البحث عن رسائل حساسة أو تحذيرية

يمكن البحث عن رسائل حساسة أو تحذيرية في أي سجلات متوفرة، مثل سجلات الوكيل أو سجلات النظام، باستخدام تعبيرات عادية.

على سبيل المثال:
للبحث عن رسائل التحذير في سجلات الوكيل، يمكننا إدخال regex التالي:

1. **CLI>** GREP
2. أدخل رقم السجل الذي ترغب في "GREP".
   []> 17 (أختر # لسجلات الوكيل هنا)
3. أدخل التعبير العادي إلى "grep".
   []> **تحذير**

روابط مفيدة أخرى:

التعبيرات العادية - دليل المستخدم

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).