ESA و SMA و WSA GREP مع Regex للبحث في السجلات

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يستعمل تعبير عادي (regex) مع ال **grep** أمر in order to بحثت سجل.

المتطلبات الأساسية

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

- أجهزة أمان الويب (WSA) من Cisco
- أجهزة أمان البريد الإلكتروني (ESA) Cisco Email Security Appliance)
- أجهزة إدارة الأمان (SMA) من Cisco

GREP مع Regex

يمكن أن يكون Regex أداة فعالة عند إستخدامه مع أمر **GREP** للبحث في السجلات المتاحة على الجهاز، مثل سجلات الوصول وسجلات الوكيل وغيرها. يمكنك البحث في السجلات بناء على موقع الويب، أو أي جزء من عنوان الربط، وأسماء المستخدمين باستخدام أمر واجهة سطر الأوامر (**GREP** (CLI.

هنا بعض السيناريوهات المشتركة حيث يمكنك إستخدام regex مع الأمر **grep** للمساعدة في أستكشاف الأخطاء وإصلاحها.

السيناريو 1: البحث عن موقع ويب معين في سجلات الوصول

أكثر السيناريوهات شيوعا هو عندما تحاول العثور على طلبات تم إجراؤها على موقع ويب في سجلات الوصول الخاصة ب WSA.

فيما يلي مثال:

قم بالاتصال بالجهاز عبر طبقة الأمان (SSH). ما إن يتلقى أنت الإيعاز، دخلت **ال grep** أمر in order to عددت ال يتوفر سجل.

```
CLI> grep
```
أدخل رقم السجل الذي تريد **تحديده**.

```
(Choose the # for access logs here) 1 <[]
```
دخلت التعبير عادي إلى **GREP**.

```
website\.com <[]
```

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

يمكنك إستخدام الأمر **grep** للعثور على امتداد ملف معين (.pptx. ،doc) في URL أو مجال على المستوى الأعلى (.org. ،com).

فيما يلي مثال:

للعثور على جميع عناوين URL التي تنتهي ب .crl، أستخدم هذا regex:

```
\.crl$
```
للعثور على جميع عناوين URL التي تحتوي على امتداد الملف .pptx، أستخدم هذا regex:

```
\.pptx
```

السيناريو 3: محاولة العثور على كتلة معينة لموقع ويب

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

فيما يلي مثال:

إذا كنت تريد البحث عن جميع رسائل TCP_DENY/403 ل domain.com، فاستخدم هذا regex:

```
tcp_denied/403.*domain\.com
```

السيناريو 4: البحث عن اسم جهاز في سجلات الوصول

عند إستخدام نظام مصادقة NTLMSSP، قد تواجه مثيلا حيث يرسل عامل المستخدم (Microsoft NCSI الأكثر شيوعا) بيانات اعتماد الجهاز بشكل غير صحيح بدلا من بيانات اعتماد المستخدم عندما يقوم بمصادقة. in order to تتبعت ال URL/مستعمل عامل أن يسبب هذا إصدار، استعملت regex مع in order to **GREP** عزلت الطلب صنع عندما المصادقة حدثت.

إذا لم يكن لديك اسم الجهاز الذي تم إستخدامه، أستخدم **GREP** وابحث عن جميع أسماء الأجهزة التي تم إستخدامها كأسماء مستخدمين عند المصادقة مع هذا regex:

```
@$\
```
ما إن يتلقى أنت الخط حيث يقع هذا، GREP ل الخاص آلة إسم أن كان استعملت مع هذا 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، لا تتضمن اشتراكات سجل الوصول الحقل الذي يظهر تاريخ/وقت البشر القابل للقراءة. إذا أردت التحقق من سجلات الوصول لفترة زمنية معينة، أكمل الخطوات التالية:

1. ابحث عن الطابع الزمني ل UNIX من موقع مثل التحويل عبر الإنترنت.
2. بمجرد حصولك على الطابع الزمني، ابحث عن وقت معين داخل سجلات الوصول.

فيما يلي مثال:

طابع وقت **1325419200** UNIX يعادل **2012/01/01 12:00:00**.

يمكنك إستخدام إدخال regex هذا للبحث في سجلات الوصول القريبة من 12:00 في 1 يناير 2012:

13254192

السيناريو 6: البحث عن رسائل حساسة أو تحذيرية

يمكنك البحث عن رسائل حساسة أو تحذيرية في أي سجلات متوفرة، مثل سجلات الوكيل أو سجلات النظام، مع التعبيرات العادية.

فيما يلي مثال:

للبحث عن رسائل التحذير في سجلات الوكيل، أدخل هذا regex:

```
CLI> grep
```
أدخل رقم السجل الذي تريد **تحديده**.

```
(Choose the # for proxy logs here) 17 <[]
```
دخلت التعبير عادي إلى **GREP**.

```
warning <[]
```

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).