

Práctica de laboratorio: Tutorial de expresiones regulares

Objetivos

En esta práctica de laboratorio, aprenderán a utilizar expresiones regulares para buscar las cadenas de información que deseen.

Antecedentes/Escenario

Una expresión regular (regex) es un patrón de símbolos que describe datos que deben coincidir en una consulta o en cualquier otra operación. Las expresiones regulares se construyen en forma similar a las aritméticas, utilizando diversos operadores para combinar expresiones más pequeñas. Hay dos estándares principales de expresiones regulares: POSIX y Perl.

En esta práctica de laboratorio utilizarán un tutorial en línea para estudiar expresiones regulares. También describirán la información que coincide con expresiones regulares dadas.

Recursos necesarios

- VM CyberOps Workstation
- Conexión a Internet

Paso 1: Completar el tutorial regexone.com.

- a. Abran un navegador web y vayan a [https://regexone.com/](https://regexone.com) desde su computadora host. Regex One es un tutorial que les ofrece lecciones para aprender sobre los patrones de las expresiones regulares.
- b. Después de que hayan terminado el tutorial, describir la función de algunos de los metacaracteres que se utilizan en expresiones regulares.

Metacaracteres	Descripción
\$	
*	
.	
[]	
\.	
\d	
\D	
^	
{m}	
{n,m}	
\$	
*	
abc 123	

Paso 2: Describir el patrón de expresión regular proporcionado.

Patrón de expresión regular	Descripción
^83	
[A-Z]{2,4}	
2015	
05:22:2[0-9]	
\.com	
complete GET	
0{4}	

Paso 3: Verificar sus respuestas.

En este paso verificará sus respuestas del paso anterior con un archivo de texto almacenado en la **VM CyberOps Workstation**.

- Abra la **VM CyberOps Workstation** e inicie sesión (nombre de usuario: **analyst**/contraseña: **cyberops**).
- Abran un terminal y diríjanse a la siguiente carpeta:

```
[analyst@secOps ~]$ cd lab.support.files/
```
- Utilicen el comando **less** para abrir el archivo **logstash-tutorial.log**.

```
[analyst@secOps lab.support.files]$ less logstash-tutorial.log
```
- En la parte inferior de la pantalla verán que **logstash-tutorial.log** está resaltado. Es el cursor en que introducirán la expresión regular. Antecedan la expresión regular con una barra inclinada hacia adelante (**/**). Por ejemplo: el primer patrón de la tabla de arriba es **^83**. Introduzcan **/^83**.

```
Terminal - analyst@secOps:~/lab.support.files
File Edit View Terminal Tabs Help
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:42 +0000] "GET /presentations/logstash-monitorama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:44 +0000] "GET /presentations/logstash-monitorama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
83.149.9.216 - - [04/Jan/2015:05:13:45 +0000] "GET /presentations/logstash-monitorama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicomplete.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.77 Safari/537.36"
/^83
```

El texto que coincide del archivo de registro está resaltado. Utilicen la rueda de desplazamiento del mouse o las teclas **j** o **k** del teclado para ubicar los patrones seleccionados.

- Para la expresión siguiente, introduzcan **/[A-Z]{2,4}** en el cursor de los dos puntos (:).
- Nota:** El signo de los dos puntos se reemplazará por una **/** cuando escriban la expresión.
- Introduzcan el resto de las expresiones regulares de la tabla del Paso 2. Asegúrense de que todas las expresiones estén precedidas por una barra inclinada hacia adelante (**/**). Continúen hasta haber verificado sus respuestas. Presionen **q** para salir del archivo **logstash-tutorial.log**.
 - Cierren el terminal y apaguen la máquina virtual.