

# 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 <a href="https://regexone.com/">https://regexone.com/</a> 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}	

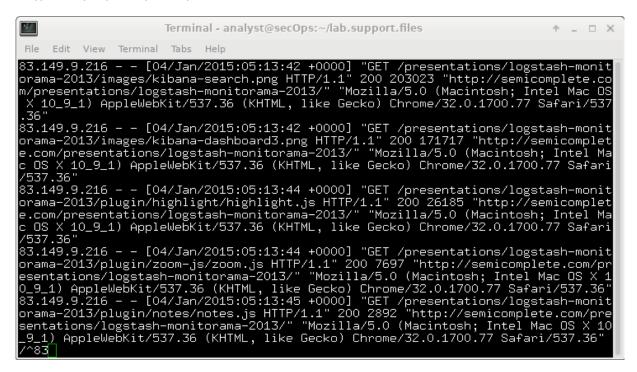
## Paso 3: Verificar sus respuestas.

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

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

```
[analyst@secOps ~]$ cd lab.support.files/
```

- c. Utilicen el comando less para abrir el archivo logstash-tutorial.log. [analyst@secOps lab.support.files]\$ less logstash-tutorial.log
- **d.** 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 (*I*). Por ejemplo: el primer patrón de la tabla de arriba es ^83. Introduzcan *I*^83.



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

- e. 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.
- **f.** 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 (*I*). Continúen hasta haber verificado sus respuestas. Presionen **q** para salir del archivo logstash-tutorial.log.
- g. Cierren el terminal y apaguen la máquina virtual.