

Lab - Regular Expression Tutorial

Objectives

In this lab, you will learn how to use regular expressions to search for desired strings of information.

Part 1: Complete the regexone.com tutorial.

Part 2: Describe the provided regular expression pattern.

Part 3: Verify your answers.

Background / Scenario

A regular expression (regex) is a pattern of symbols that describes data to be matched in a query or other operation. Regular expressions are constructed similarly to arithmetic expressions, by using various operators to combine smaller expressions. There are two major standards of regular expression, POSIX and Perl.

In this lab, you will use an online tutorial to explore regular expressions. You will also describe the information that matches given regular expressions.

Required Resources

- CyberOps Workstation virtual machine
- Internet connection

Instructions

Part 1: Complete the regexone.com tutorial.

- Open a web browser and navigate to <https://regexone.com/> from your host computer. Regex One is a tutorial that provides you with lessons to learn about regular expression patterns.
- After you have finished with the tutorial, record the function of some of the metacharacters that are used in regular expressions.

Metacharacters	Description
\$	strings ends with
*	0 or more
.	anything alphabet number or character
[]	range a-z 0-9 etc
\.	escape char to match .
\d	substitutue for digits
\D	non digit chars
^	start of string
{m}	repeat m times

Metacharacters	Description
{n,m}	repeat range
abc 123	option

Part 2: Describe the provided regular expression pattern.

Regex pattern	Description
^83	starts with 83
[A-Z]{2,4}	2 or more Alphabet less than 4
2015	direct match
05:22:2[0-9]	ending with 20-29
\.com	matching .com literally
complete GET	either complete or GET
0{4}	0000

Part 3: Verify your answers.

In this step, you will verify your answers in the previous step using a text file stored in the **CyberOps Workstation VM**.

a. Launch and log in to the **CyberOps Workstation VM** (username: **analyst** / password: **cyberops**).

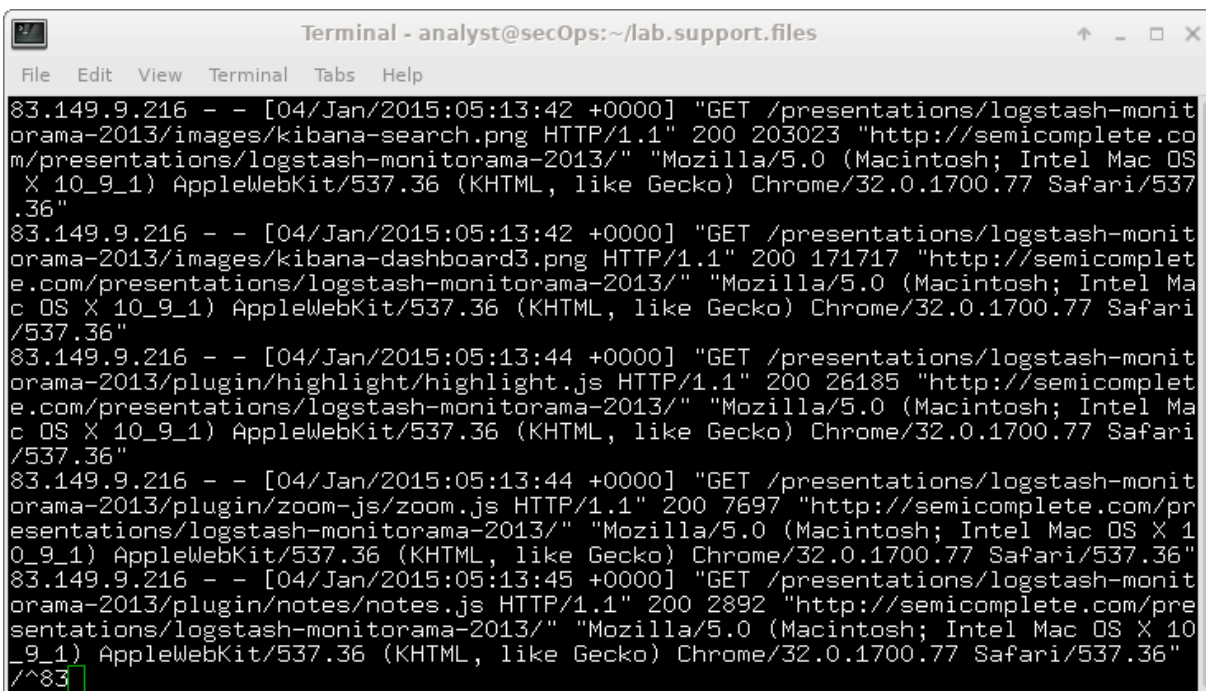
b. Open a terminal and navigate to the following folder:

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

c. Use the **less** command to open the **logstash-tutorial.log** file.

```
[analyst@secOps lab.support.files]$ less logstash-tutorial.log
```

- d. At the bottom of the screen, you will see **logstash-tutorial.log**: highlighted. This is the cursor at which you will enter the regular expression. Precede the regular expression with a forward slash (/). For example, the first pattern in the above table is ^83. Enter **/^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-monit
orama-2013/images/kibana-search.png HTTP/1.1" 200 203023 "http://semicomplete.co
m/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-monit
orama-2013/images/kibana-dashboard3.png HTTP/1.1" 200 171717 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c 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-monit
orama-2013/plugin/highlight/highlight.js HTTP/1.1" 200 26185 "http://semicomplet
e.com/presentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Ma
c 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-monit
orama-2013/plugin/zoom-js/zoom.js HTTP/1.1" 200 7697 "http://semicomplete.com/pr
esentations/logstash-monitorama-2013/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 1
0_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-monit
orama-2013/plugin/notes/notes.js HTTP/1.1" 200 2892 "http://semicomplete.com/pre
sentations/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
  
```

The matching text from the log file is highlighted. Use the scroll wheel on the mouse or use the **j** or **k** keys on your keyboard to locate the highlighted patterns.

- e. For the next expression, enter **/[A-Z]{2,4}** at the colon (:) prompt.
Note: The colon is replaced by / as you type the expression.
- f. Enter the rest of the regular expressions from the table in Step 2. Make sure all the expressions are preceded with a forward slash (/). Continue until you have verified your answers. Press **q** to exit the logstash-tutorial.log file.
- g. Close the terminal and shut down the VM.