

Laboratório - Tutorial Expressão

Objetivos

Neste laboratório, você aprenderá a usar expressões regulares para procurar cadeias de informações desejadas.

Parte 1: Competir o tutorial regexone.com.

Parte 2: Descreva o padrão de expressão regular fornecido.

Parte 3: Verifique suas respostas.

Histórico/Cenário

Uma expressão regular (regex) é um padrão de símbolos que descreve dados a serem correspondidos em uma consulta ou outra operação. Expressões regulares são construídas de forma semelhante às expressões aritméticas, usando vários operadores para combinar expressões menores. Existem dois principais padrões de expressão regular, POSIX e Perl.

Neste laboratório, você usará um tutorial on-line para explorar expressões regulares. Você também descreverá as informações que correspondem a expressões regulares dadas.

Recursos necessários

- Máquina virtual CyberOps Workstation
- Conexão com a Internet

Instruções

Parte 1: Complete o tutorial regexone.com.

- Abra um navegador da Web e navegue até <https://regexone.com/> do computador host. Regex One é um tutorial que lhe fornece lições para aprender sobre padrões de expressão regular.
- Depois de terminar o tutorial, registre a função de alguns dos metacaracteres usados em expressões regulares.

Metacaracteres	Descrição
\$	
*	
.	
[]	
\.	
\d	
\D	
^	

Metacaracteres	Descrição
{m}	
{n,m}	
abc 123	

Parte 2: Descreva o padrão de expressão regular fornecido.

Padrão Regex	Descrição
^83	
[A-Z]{2,4}	
2015	
05:22:2[0-9]	
\.com	
complete GET	
0{4}	

Parte 3: Verifique suas respostas.

Nesta etapa, você verificará suas respostas na etapa anterior usando um arquivo de texto armazenado na **VM CyberOps Workstation**.

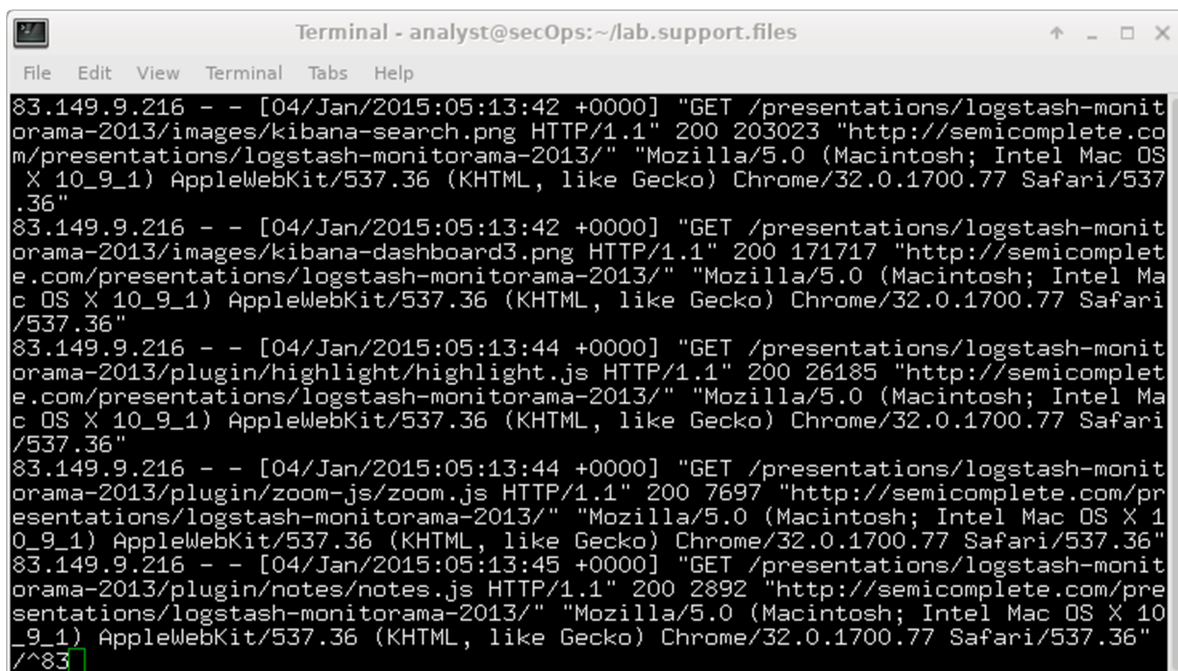
- Inicie e faça login na **VM do CyberOps Workstation** (nome de usuário: **analista** /senha: **cyberops**).
- Abra um terminal e navegue até a seguinte pasta:

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

- Use o comando **less** para abrir o arquivo **logstash-tutorial.log**.

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

- d. Na parte inferior da tela, você verá **logstash-tutorial.log**: destacado. Este é o cursor no qual você irá inserir a expressão regular. Precede a expressão regular com uma barra (/). Por exemplo, o primeiro padrão na tabela acima é ^83. Digite /**^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

```

O texto correspondente do arquivo de log é realçado. Use a roda de rolagem no mouse ou use as teclas **j** ou **k** no teclado para localizar os padrões realçados.

- e. Para a próxima expressão, digite **/[A-Z] {2,4}** no prompt de dois-pontos (:).

Nota: Os dois-pontos são substituídos por à medida que escreve a expressão.

- f. Insira o restante das expressões regulares da tabela na Etapa 2. Certifique-se de que todas as expressões são precedidas com uma barra (/). Continue até ter verificado suas respostas. Pressione **q** para sair do arquivo logstash-tutorial.log.
- g. Feche o terminal e desligue a VM.