Lab01 - Regular Expressions and filters

Parsing a Windows Firewall log with regular expressions

Introduction

This lab will ask you to leverage what you have learned about regular expressions to generate some metrics for a simulated Windows Firewall log file.

Getting started

1. Download the **Lab 01 Data File** from the course website
2. Move the file to ASU General (or your chosen environment)
    a. Windows
        i. WinSCP is an excellent SCP (secure copy) tool for windows. Although, anything that supports SFTP should work (FileZilla for instance).

            Make sure to use "SFTP" as the protocol; FTPS is entirely different.
    b. MacOS
        i. Open a terminal and navigate to the folder containing the downloaded file Use the following command to upload the file to ASU General;

```
scp firewall.log.gz ASURITE@general.asu.edu:firewall.log.gz
```

            Replace ASURITE with your username
3. Unzip the data file
    a. In the Linux shell; issue the following command to expand the data file

```
gunzip ./firewall.log.gz
```

4. Create an empty Word or Google document
5. For each numbered question in the following lab provide any commands used in your solution and the resulting output; either copy-pasted text, or a legible screenshot
6. When finished, save your file as **lab01-ASURITE** where ASURITE is your username. Example; lab01-cjingers.pdf
    a. Accepted file formats are; docx, doc, pdf and odt
7. Submit your saved document before the deadline on Sunday, 11:59 PM

Lab

Part 1 - 80 points

The data file is comprised of a header, followed by lines containing firewall events. You can view the head of the file with the following command;

cat firewall.log | *head*

TIP: If you find yourself with a massive number of lines printing to the terminal; pressing CTRL-C will stop the output of the file

QUESTION 1:
(10 points)

Write a command to count the number of firewall events in the file. Your command should exclude the header using a simple regular expression.

Notice that the firewall event fields are delineated by a single space and contain the following data points; date, time, action, protocol, src-ip, dst-ip, src-port, dst-port, size

QUESTION 2:
(10 points)

Write a command to count the number of unique values in the src-ip field.

The date field follows the format YYYY-MM-DD; the month and day values are padded to 2 characters.

QUESTION 3:
(20 points)

Write a command to count the number of events that match these conditions;

- The event occurred in August, 2018 OR on July 4th 2018
  2018-08-xx OR 2018-07-04
- The dst-port field is either 80 or 443
- the action field is ACCEPT

The time field follows the format of; HH:MM:SS

QUESTION 4: **(20 points)**	Write a command to count the number of events that meet this criteria; - The event occurred between midnight and 3 AM 00:00:00 to 03:00:00 - The dst-port is 22 - The action is DROP - The protocol is TCP

For the last remaining question in part 1; recall that man pages provide details on available arguments for the majority of programs on a Linux computer.

QUESTION 5: **(20 points)**	Write a command to display the src-ip value for events that match the following criteria; - The size field is less than or equal to 500 - the dst-ip field starts with 10.202.40

Part 2 - 20 points

For this part, you will need to make use of the **sort**, **tail** and/or **head** programs. Study the man pages for these programs to assist you with answering this question.

QUESTION 6: **(10 points Each)**	Write a command to print the date and time of the earliest event in the firewall.log file. Create a second command to print the date and time of the latest event in the file.