Activity IV : Log Analysis

Instructors : Kunwadee Sripanidkulchai, Ph.D.

Overview

Pretend you are on the security/incident management team of a (supposed) company named buttercup. You have access to a set of **system logs (secure.log)** and **web logs (access.log)** from your company infrastructure consisting of:

- 1 mail server named mailsv
- 3 web servers named www1, www2, www3

It is your job to identify successful/failed attempts to hack, scan, login, or access protected information on the servers.

The logs are at

https://drive.google.com/file/d/15bXMVCHSoe1D9RDGywOsmadVGBLTtpYa/view?usp=sharing .

Reading/parsing the logs manually will be PAINFUL. We will use a popular tool, Splunk, to help us with our job.

Figure 1. Magic Quadrant for Security Information and Event Management

Source: Gartner (December 2018)

Getting Started

1. You will use Splunk, a popular log analysis tool, that you can download from: http://www.splunk.com/ → Choose Free Splunk. You will need to provide your information to Splunk before you download. Install Splunk on your computer and start running it (Start Splunk Lite and launch Splunk Web).
2. In your browser, go to your newly installed Splunk Web at: http://localhost:8000.
3. Import the data downloaded above (the entire zip file) into Splunk following these steps (Add Data, Use Segment in Path to identify Host).
   WARNING: do this only once or you will have multiple copies of the data in your analysis, and your count will be incorrect.
   http://docs.splunk.com/Documentation/Splunk/latest/SearchTutorial/GettheturialdataintoSplunk .
   After import, if you cannot see the data, look at the time frame of your analysis and select as far back in time as possible.

Understand the Data

Use Splunk's "Search" feature to explore the data.
http://docs.splunk.com/Documentation/Splunk/latest/SearchTutorial/Aboutthesearchapp

Part I. Can you find people trying to break into the servers?

Use Splunk's "Search" feature to try to answer the questions below.

Hint 1: On linux servers, **secure.log** contains security-related information. Typically in response to incidents, it is one of the first files people look at to see if there are compromises. Read this to see what to look for on Linux.
https://zeltser.com/security-incident-log-review-checklist/

Hint 2: To process the logs for analysis, first parse it using regular expressions to "extract fields" and turn unstructured data into structured data.

Answer the following questions and provide evidence with your answer.
Q1. How many hackers are trying to get access to our servers? And how many attempts are there?
Q2. What time do hackers appear to try to hack our servers? 12:15 AM
Q3. Which server (mailsv, www1, www2, www3) seem to see the most attempts?
Q4. What is the most popular account that hackers use to try to break in? root djohnson

Screenshotted
Screenshotted

Part II. Sensitive Files on Web Servers

Hint: On web servers, **access.log** contains web access-related information. Typically in response to incidents, it is one of the first files people look at to see if there are compromises. Read this to see what to look for on Web Servers.
https://zeltser.com/security-incident-log-review-checklist/

Q5. Can you find attempts to get access to sensitive information from our web servers? How many attempts were there? 16
Q6. What resource/file are hackers looking for?
password.pdf?

Part III. (Optional) Are there bots crawling our websites?

Q7. Can you find any bots crawling our websites?
Q8. What are they doing on the site? (Hint: Look for User-Agent in the web access.logs.)

Cleaning up

Shutting down splunk on your notebook (otherwise, it will keep running in the background). Mac users should follow Unix instructions. The splunk command is located at /Applications/Splunk/bin/.

http://docs.splunk.com/Documentation/Splunk/latest/Admin/StartSplunk

Submission

Upload your answers and evidence for your answers (i.e., screenshots, commands) as a pdf containing all parts to the Assignment in classdeedee.