2110413/2110640/2190413 Computer/Information/System Security
Dept. of Computer Engineering
Chulalongkorn University

Activity : Log Analysis

Instructor: Kunwadee Sripanidkulchai, Ph.D.

Overview

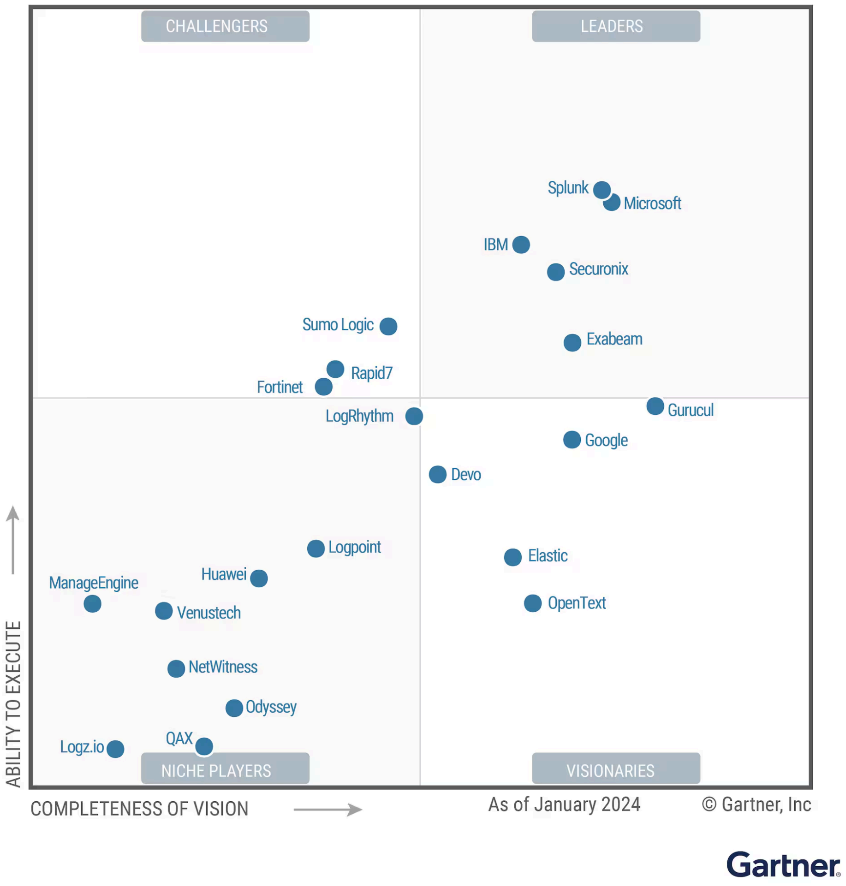
Suppose you are on the security/incident management team of a (supposed) company named buttercup. You have access to a set of **system logs (secure.log)** and **web logs (access.log)** from your company infrastructure consisting of:

- 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 the link I posted on facebook. Reading/parsing the logs manually will be PAINFUL. You could write code to do this, but that will also take some time and effort. Instead, we will use a popular tool, Splunk, to help us with our job.

Figure 1: Magic Quadrant for Security Information and Event Management



Getting Started

1. You will use Splunk, a popular log analysis tool, that you can download from: http://www.splunk.com/ → Choose Free Splunk -> Software Download → Download Splunk Enterprise. You will need to provide your information to Splunk before you download. Download and install Splunk Enterprise on your computer and start running it (Start Splunk Enterprise and launch Splunk Web).
2. In your browser, go to your newly installed Splunk Web on your computer 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. Look at how to load data in the example in this link first..
   http://docs.splunk.com/Documentation/Splunk/latest/SearchTutorial/GetthetutorialdataintoSplunk .
   After the import, if you cannot see the data, look at the **time frame** of your analysis and select as far back in time as possible.
   You must use only the data set I provided via facebook. Using other data sets will have different results when grading.

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 (this file is available in google drive). 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? Explain/define how you count distinct hackers.
Q2. What time do hackers appear to try to hack our servers?
Q3. Which server (mailsv, www1, www2, www3) had the most attempts?
Q4. What is the most popular account that hackers use to try to break in?

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?
Q6. What resource/file are hackers looking for?

Part III. 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

Shut 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/. You may uninstall splunk after you are done with this assignment.

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.