**Dynnis Feliciano**

**Activity File: Exploring Kibana**

* You are a DevOps professional and have set up monitoring for one of your web servers. You are collecting all sorts of web log data and it is your job to review the data regularly to make sure everything is running smoothly.
* Today, you notice something strange in the logs and you want to take a closer look.
* Your task: Explore the web server logs to see if there is anything unusual. Specifically, you will:

⚠ **Heads Up**: These sample logs are specific to the time you view them. As such, your answers will be different from the answers provided in the solution file.

**Instructions**

1. Add the sample web log data to Kibana.
2. Answer the following questions:
   * In the last 7 days, how many unique visitors were located in India?

**Ans: 236 visitors from India**

* + In the last 24 hours, of the visitors from China, how many were using Mac OSX?

**Ans: 7 visitors from China using Mac OSX**

* + In the last 2 days, what percentage of visitors received 404 errors? How about 503 errors?

**Ans: Both errors, 404 and 503, received 50% each in the last 2 days.**

* + In the last 7 days, what country produced the majority of the traffic on the website?

**Ans: China**

* + Of the traffic that's coming from that country, what time of day had the highest amount of activity?

Ans: **China is most active during noontime with 36 activities.**

* + List all the types of downloaded files that have been identified for the last 7 days, along with a short description of each file type (use Google if you aren't sure about a particular file type).

**deb** *– (Debian Software Package) Deb file is the format as well as extension of the software package format for the Linux distribution Debian and its derivatives*

**zip –** *are single files often called “archives” that contain one or more compressed files for easy transporting, e-mailing, downloading, and storing data and software faster and more efficient.*

**rpm** – *(Red Hat Package Manager) a file that’s used to store installation packages on Linux operating systems for easy software distribution, installed, upgraded, and removed since they’re “package” in one place.*

**gz *–*** *compressed archives that are created by the standard GNU zip (gzip) compression algorithm.*

**css – *(Cascading style sheet)*** *file used to format contents of a webpage.*

1. Now that you have a feel for the data, Let's dive a bit deeper. Look at the chart that shows Unique Visitors Vs. Average Bytes.
   * Locate the time frame in the last 7 days with the most amounts of bytes (activity).

**Ans: At 12 Dec 2020 at 1500, there was 8,586 average bytes during that timeframe**

* + In your own words, is there anything that seems potentially strange about this activity?

Ans: **During that registered timeframe, there was only 2 average unique visitors**

1. Filter the data by this event.
   * What is the timestamp for this event?

**Ans: 12 Dec 2020 at 1500**

* + What kind of file was downloaded?

**Ans: gz**

* + From what country did this activity originate?

**Ans: Germany and Moscow**

* + What HTTP response codes were encountered by this visitor?

**404 Response codes had 85.714% and 503 was 14.286%**

1. Switch to the Kibana Discover page to see more details about this activity.
   * What is the source IP address of this activity?

**164.68.112.178 and 81.161.63.100**

* + What are the geo coordinates of this activity?

**55.73 degrees Lat 37.60 degrees Long**

**49.40 degrees Lat 11.16 degrees Long**

* + What OS was the source machine running?

**Ans:** **Unix**

* + What is the full URL that was accessed?

**Ans:** **/var/log/auth.log**

* + From what website did the visitor's traffic originate?

**Ans:** **log**

1. Finish your investigation with a short overview of your insights.
   * What do you think the user was doing?

**Ans: The attacker who wishes to modify the contents of the /var/log/auth.log file to have root privileges and not by a general user. This is done to erase any footprints of the attacker.**

* + Was the file they downloaded malicious? If not, what is the file used for?

**Ans: No malicious files downloaded. This file has a particular set of system access permission associated with it.**

* + Is there anything that seems suspicious about this activity?

**Ans: Attackers are tracking the usage of authorization to include user logins and authentication mechanism.**

* + Is any of the traffic you inspected potentially outside of compliance guidelines?

**Ans: No. This file contains logs of all connections from multiple user system and there are ways of obtaining this information.**