KerSplunk Teacher Workout Instructions

Background:

Splunk

Splunk can be described as a proprietary log management tool. It is primarily used to search, monitor, analyze, and visualize machine data. With the ever growing threat of Cyber criminals, it is necessary to use tools such as Splunk to more easily keep track of what is going on within your network.

- Basic Searching Concepts
- Splunk's official Splunk query syntax document.

Logging on to Your Computer:

- Log into the Guacamole web server using the credentials provided.
- You may have to refresh the page if a screen does not come up.
- Then, you will log in automatically

Diving In:

The remainder of the workout will be conducted from within the virtual machine.

- From within the virtual machine, click on the Firefox icon. This should automatically direct you to direct you to the local Splunk web interface at *http://127.0.0.1:8000/en-US/app/launcher/home*
- Once you see ta log in screen, use *workout* and *k3r$plunk8!* as the username and password.
- Once logged in to the Splunk web interface, click on the **Search & Reporting** from side bar on the left.

Basic Splunk Tips:

It is best practice to refine your queries to be as exact as possible. For example, it is a lot easier for humans to parse 20 results than 150,000.

- One easy way to do this is to specify a date-time range. To the right of the Splunk search bar is a drop down menu that lets you choose over what range you want Splunk to query over.

- Surrounding a string in quotes will query data with that exact match.
- It is important to know what data you want to query over. Are you looking for an event over a specific protocol? System events?

Assessment Answer Key:

> To ensure that you are querying the correct dataset, be sure to preface each query with *index="botsv3" earliest=0*

1. **What is Peat Cerf's email address?**
    a. *pcerf@froth.ly*
        i. This information can be found by the following query:

```
index="botsv3" earliest=0 "Peat Cerf"
```

2. **In one of Peat's email conversations on 08-20-2018, what was the IP address of the other user in the conversation?**
    a. *172.31.37.181*
        i. First make sure to set the date range to the one provided in the question. In this scenario, one day is good. However, on larger datasets, the closer you can narrow your search to the target event, the better. Use the email found above to help refine the search even more. *This should return exactly one event.*

```
index="botsv3" earliest=0 sender_email="
pcerf@froth.ly"
```

3. **On 08-20-2018, Peat changed his password on a website that didn't properly secure the interaction. What was his old password?**
    a. *dfasdfsad*
        i. Make sure the correct date-time range is selected. Again, we can use the email as the primary search and refine it to pull all events that involve the word, *password.*

```
index="botsv3" earliest=0 "pcerf@froth.ly"
password
```

        The correct answer should be within the second returned result.
4. **From the previous question, what was the URL of the insecure website?**
    a. *microsoftexchangeservervwu2g8sj20.igg.biz*

i. Looking at the same result as the previous question, there will be a field that is labeled, *site*. This will hold the target URL.

Once you've completed the assessment questions, we encourage you to dig around even further. There is plenty of interesting events just waiting to be discovered!