KerSplunk Student 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.

> ⚠ Splunk typically takes around 10 minutes to start up after a fresh machine boot. The web service will not display until Splunk is fully functional.

- 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. This is where the workout will take place.

> ℹ This workout is centered around an indexed dataset. In order to access this data, you will need to preface each query with the following line:
>
> *index=”botsv3” earliest=0*

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 Questions:

1. **What is Peat Cerf's email address?**
2. **In one of Peat's email conversations on 08-20-2018, what was the IP address of the other user in the conversation?**
3. **On 08-20-2018, Peat changed his password on a website that didn't properly secure the interaction. What was his old password?**
4. **From the previous question, what was the URL of the insecure website?**
5. **What is the AWS account ID for Frothly's account?**
6. **List the IAM users that accessed an AWS service in Frothly's AWS environment? (Separate each username with a comma)**
7. **From the usernames found in question 6, which was the only user that was unauthorized?**
8. **From the unauthorized user in question 7, what was the user agent for the *least common* source IP address?**