Assignment 4 - Log Analysis

Submit Assignment

Due Oct 6 by 11:59pm **Points** 7 **Submitting** a text entry box or a file upload
Available after Sep 28 at 12am

Background:

You are an employee in the Georgia Tech SOC, you receive a report from a system adminstrator that one of their websites is acting "funny." The website is running Wordpress and is accesible from the world. You have access to the access logs for the site as well as the directory that the website lives under. Both of these are available in the Files section of Canvas.

Georgia Tech's IP ranges are:

- 128.61.0.0/16
- 130.207.0.0/16
- 143.215.0.0/16

Assignment:

You will use the logs and site directory to figure out what happened and when. You should turn in a document that:

- Describes what happened in a way that the system administrator and also the web developer would understand. Include some understandable, technical details backing up your conclusion.
- Illustrates the timeline of the incident
- Details the process you took to arrive at your conclusion
- Answers the questions at the bottom of this document

Steps:

We will be teaching using Splunk, but if you are more comfortable using Elastic (ELK) or some other log searching mechanism you are free to do so. While you can definitely succeed at this assignment using plain old grep, I would recommend you don't. While grep will work due to the small size of the log files being provided, grep fails to perform when you are in an actual Enterprise with massive amounts of data.

1. Create a virtual machine, using Virtualbox or some other vm host software. Splunk runs on Linux, Windows, and OS X.
2. Install Splunk using the documentation shown here: http://docs.splunk.com/Documentation/Splunk/6.6.3/Installation/Chooseyourplatform
3. You will need to register with Splunk to gain access to the Splunk installers. Splunk is free for a limited use license. Splunk has asked that you register with your GT email addresses, if possible, so that they know they don't need to call you to try to sell you the product.
4. Once logged in to Splunk, you will see an "Explore Splunk Enterprise" box. In that box, click "Add Data"
5. Drag and drop the attached "access_log" file into the box that says "Drop your data file here." Click next.
6. Splunk should automatically detect that the log "Source type" is access_combined. If not, select "Web -> access_combined" in the "Source type" drop down. Click next.
7. Click next again. And then finally submit.
8. Click "start searching"

You can get to the data by searching for "index=main earliest=0"

Questions:

Using the logs, answer the following questions. Please include the Splunk (or Elastic) queries you used to find each answer. This will allow us to understand your thought process if you come to a different answer or interpret the question in a different way.

1. Which IP(s) attempted to brute force the Wordpress login?
2. How many attempts did it/they make?
3. How many of the IP(s) were successful? When were each successful?
4. What did each IP do after it logged in?
5. What file was changed?
6. When was it changed?
7. How was it changed?
8. What was the purpose of the change?

Assignment 4		
Criteria	**Ratings**	**Pts**
Understandable description of the event.		1.0 pts
Description of investigation methodology		0.5 pts
Question 1		0.5 pts
Question 2		0.5 pts
Question 3		0.5 pts
Question 4		0.5 pts
Question 5		0.5 pts
Question 6		0.5 pts
Question 7		0.5 pts
Question 8		1.0 pts
Timeline of the event		1.0 pts
		Total Points: 7.0