HW#4 - Splunk

Due Date: Apr 22 2016

CIS4361 Spring 2016

50 pts

This assignment can be worked with a **group of 3 people**. I advise that you find a group (let me know if you need assistance with that) because that way you will be able to develop the team before the harder assignments later in the course come.

**Instructions:**

It is advised you work on your host computer so that what you build in this work can be used over the long time, and you have more realistic data. You are to install Splunk light; the installation link is located at the web courses module. In this assignment we shall use Splunk as a tool to detect intruders in a system.

Some of the questions below ask for IPTables or logrotate commands. Both of these are Unix specific. Windows has its own equivalent files, but to standardize the response among all I am asking to provide the answer as if you were running the Splunk part in a Unix box. However, you are more than welcome give the Windows equivalent too.

You must be able to do the following:

1. Identify a file or resource that can be used by Splunk for getting login information. Give both the name of the file and path.
2. What other files can be found in the path and for what?
3. Setup ingestion for the file in question 1 into Splunk
4. Make a report of login/logout attempts and the session duration. Use the command rex to extract fields.
5. Find if a session went into admin rights. You may use eval to create a new column using if.
6. Find the average duration of a session, and the average user session duration. For this you will need to use stats avg.
7. Make a dashboard which has a graph of: average session duration time chart, login errors time chart, event table with session info (\_time, user name, successful?, went into root?). Provide a screenshot of the dashboard and the queries used to generate each of the parts.
8. Explain what settings or information you could use from this dashboard to create alerts to detect potential intruders. Which IPtables command(s) would you use to react if the alert fires? Assume that you can get all the information needed from the log file event.
9. Use IPtables MAC address filter to allow login only from specific local machines. You may write any valid/non-valid MAC address in your command.
10. Specify a logrotate that could handle this file to rotate every day, keeping only one week of files. Anything older must be zipped into a tar file. Once past one month it should be deleted.

**References:**

* <http://docs.splunk.com/Documentation/Splunk/latest/SearchTutorial/WelcometotheSearchTutorial>
* <https://answers.splunk.com>
* <http://linux.die.net/man/8/iptables>
* <http://www.linuxcommand.org/ma>n\_pages/logrotate8.html