**CSE TEST – Write up**

The purpose of this documentation is to depict the context of having worked towards an objective set forth in a task I was given to gage my ability to learn new or unfamiliar skill and apply it to creating solution level work. I must say that I did learn a great deal of new skill and information which was very novel. Having been a long time SIEM engineer and content developer this was very refreshing as I had been specialized in a niche now outmoded being *legacy SIEM*. That being said, I was both empowered and stumped at the seemingly simple task of:

* **Parsing one log (syslog) to normalization and output to JSON format**

Said task not only allowed for absorption of fresh skill and insight, it also delivered a considerable magnitude of challenges which I still pursue resolution of although I am past my deadline. I will first explain the solution I was working towards and then supply some additional data to depict the challenges and issues I faced and how I approached those.

* **Solution:** Use the **file** **input plugin** of Logstash to read the file, the **filter plugins** **grok** and **dissec**t to normalize it, and the **file** **output plugin** to render the resultant data to the specified format. Grok is just amazing, I look forward to using it much more. Regex and such are very fascinating to me on both a professional and personal level so I was very intrigued by grok and dissect. I have uploaded two associated configuration files which I had mixed success with. In short, I was able to grab the syslog priority, timestamp and other classic header parts and isolate them from the message. I learned that the message part would be more easily normalized and operated on with *dissect* and mutate plugins. This solution evolved over the course of the 7 days between being handed the task and the deadline for submission and continues to evolve the more it sits on my mind. Having stated the solution I must add that I am yet to see the results in fruition although this repo will be updated when I reach that point.

**Issues and troubleshooting:**

* **First Issue**: I quickly learned that my laptop asset was less than sufficient to run all of the associated processes required. The first 12 hours of the task on the first day were striving with eager momentum only to subsequently sustain loss of all progress theretofore as the laptop froze and had to be manually powered down. This allowed for much reinstalling and re-configuring Logstash and such from scratch. System crash events due to one external display being plugged into it were amplified once I started actually using it.
  + **REMEDIATION:** I procured a refurbished desktop PC the following morning. It was sufficient to run the needed items (VMware, Logstash, many browser windows and tabs). In my haste to acquire a working machine I mistakenly overlooked the less than optimal aspect of the PC only supporting one display.
* **Next issue:** Traditionally I run a VM or so on one monitor and my base OS on another for maximal workflow and the capacity to work on things as I am simultaneously learning it for the first time. With only one display supported I was unable to do this. Considering that VMware Workstation Player only allows for one tiny window even in full screen mode, it was very challenging to run all of the shells and such I needed to, which were themselves often larger than the VMware window itself. (See image in this repo.)
  + **REMEDIATION:** I re-purposed the laptop and sat it up next to my workspace so as to leverage tutorials and other internet resources. This was still far from optimal in that I could not copy and paste from one machine to the other. I sat up a simple network so I could SFTP between the machines but it was very slow and thus my workflow and learning curve were more complicated than is normal plus the time taken to set all of that up.
* **Subsequent Issue:** My VM would freeze up every few hours which I attempted to rectify yet did have to resort to manually powering down the VM. This not only blew away my Logstash and other processes as with the laptop the day prior.
  + **REMEDIATION:** I found a happy medium between the host OS and the VM, not overloading the VM by using it as a syslog server which sent messages to the localhost thus I started using it to send syslog RFC5424 stimuli to 514/UDP. I instanced Logstash\ELK on the host OS and was actually getting somewhere with that. I got it to populate an index in Kibana with that setup. However, I had to re-install a couple of times. Windows does not like to run ELK nor does ELK like to be run on it, which was made painfully evident after having run it in the Linux context again on the VM. ELK can be instanced on Windows but it is not exactly what one should do. I used it on both the host and guest OS with mixed results but more functionality than I had been encountering.
* **Logstash issues:** There were issues with running Logstash when I would use the elasticsearch localhost:9200 output, as either Elasticsearch or Kibana would fail after reboots. I think the Windows OS hasn’t the ‘right stuff’ such as a complex directory structure in which to instance the elastic platform, and the VMware would have been much more manageable on a full blown version versus the freeware offering. So I ran into errors and nuances which would only occur respective to one or the other OS
  + **REMEDIATION:** Going back and forth between the instances on both OS’ was great for getting my basic and advanced Linux skills back in check after a little while of not using it daily at work. I was not in a position to go and procure additional resources, yet it was a great refresher for both VMware and Linux. Thus resolution of these systemic issues was toughing it out and growing very aware of the reasons why I don’t use Windows and prefer Linux.

**Wrap-**up: Well, in retrospect and with some feedback from the Elastic community I see clearly that I over complicated the entire task and rendered a bit of an ordeal of it. I installed all of the Jruby \ Bundle stuff for making my own plugins, ran the entire elastic stack when I needed but Logstash to read the file and spit it out.

(Please see associated files for conf and screenshots)

* Skills acquired and applied Logstash - Git/Guthub - GitKraken - GitGui – Github Desktop – Vmware – Grok – PyCharm – Jruby/Bundle/Gems –Elastic Discussion forum (User = Markparser) **https://github.com/Markparser**