This was my first time using Logstash, and it has definitely been an enjoyable and challenging experience thus far. I have been leaning heavily on both my troubleshooting experience and web tools to teach myself how to use Logstash.

I initially downloaded and configured the full ELK stack and was using it to test, which included Elasticsearch, Logstash, and Kibana. After encountering issues with the output connector related to an indexing problem, I decided to simplify things and fall back on using file inputs and outputs. Unfortunately, I’m still having a problem getting the output file to create when using the Security Log Data from the skills test. I was able to get an output file created using

I also