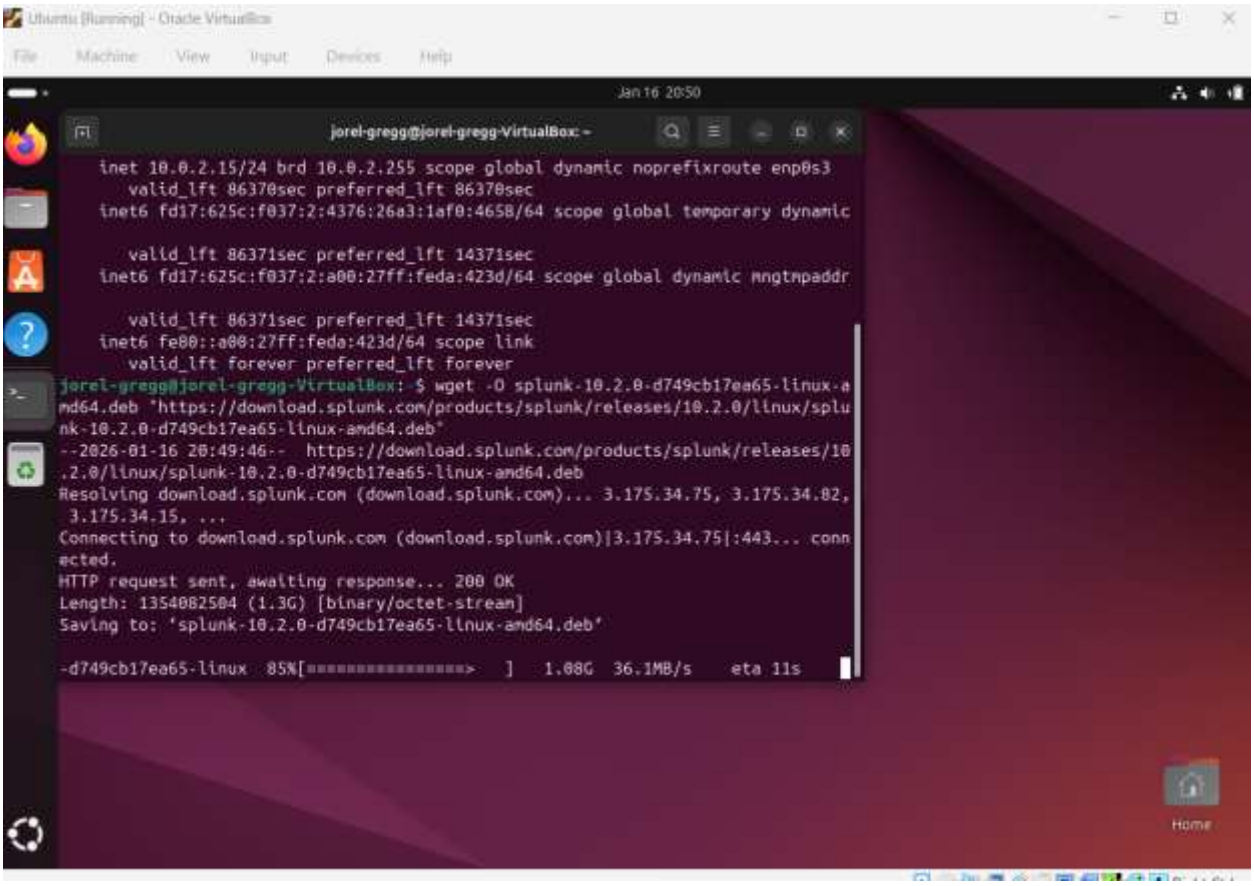
Jorel Gregg

Basic SPLUNK Home Lab

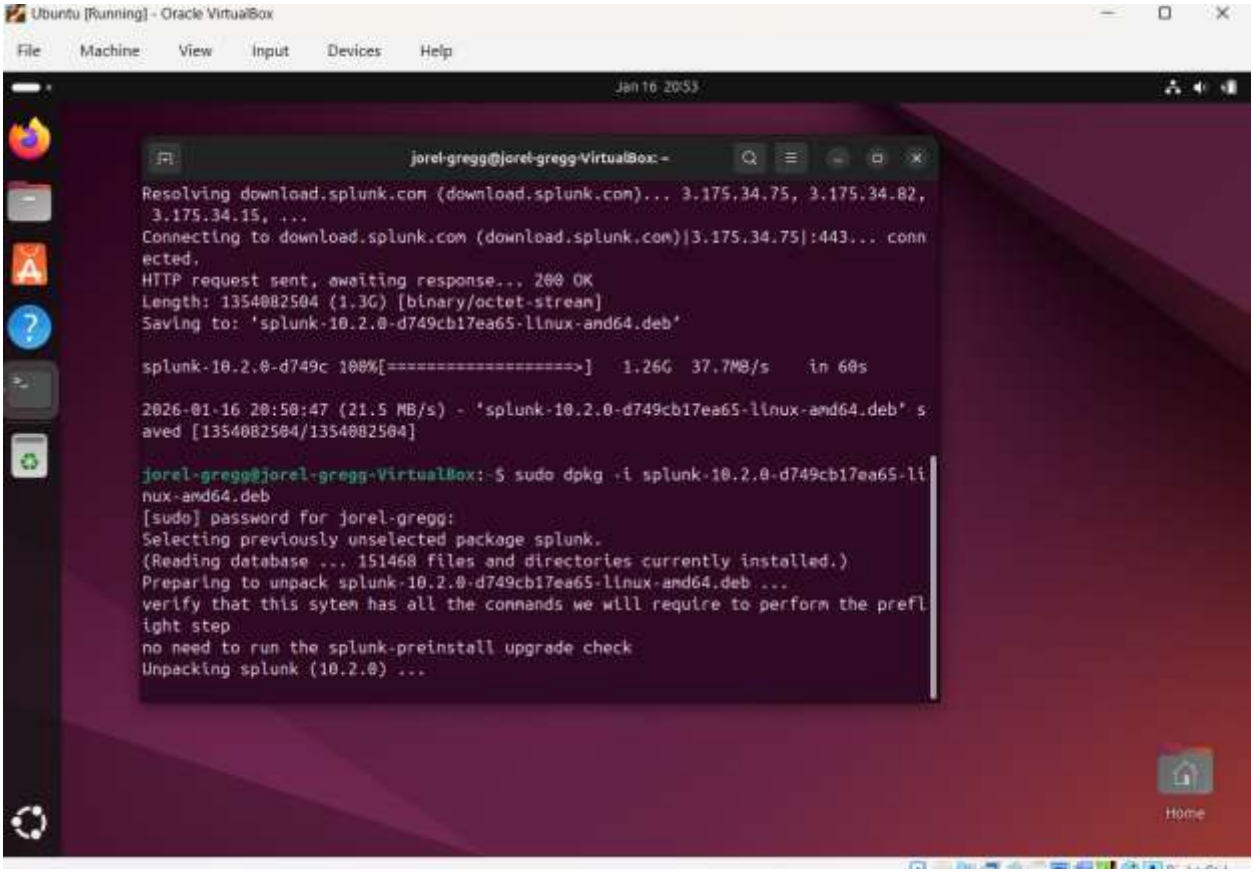
1/16/26

This will be my first time installing and running SPLUNK on my home virtual lab through VirtualBox. I will use the same Kali-Linux and Ubuntu machines I used in my Wireshark lab.

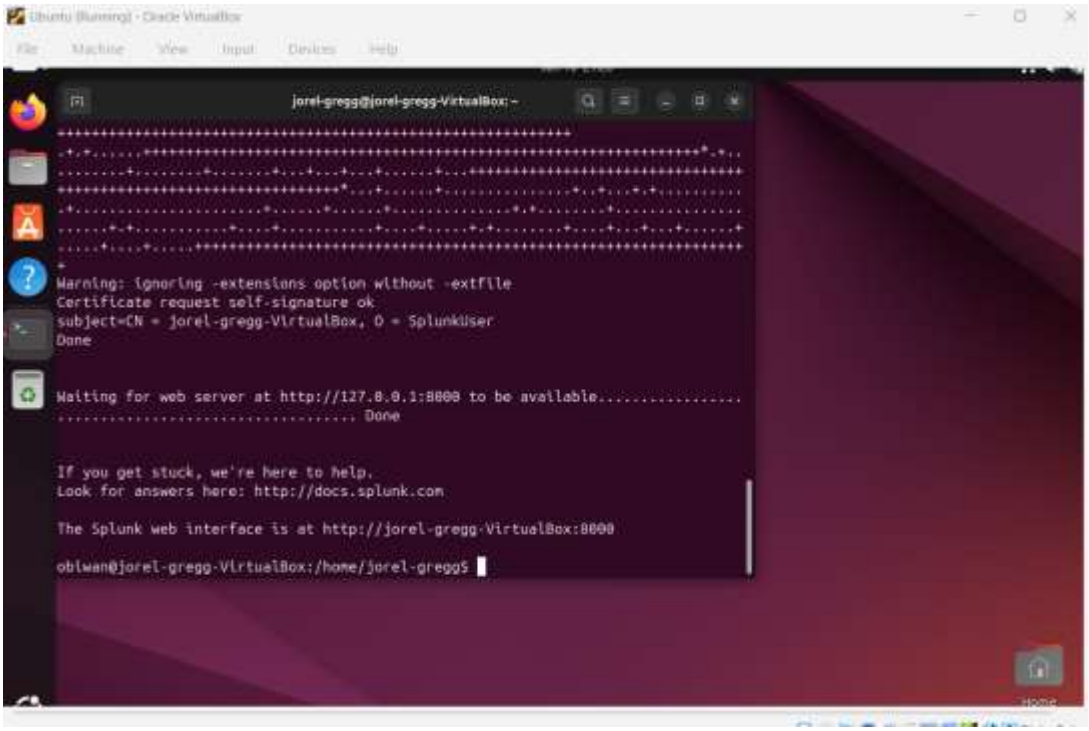
1. First, I created an account in Splunk and then copied the wget link for the .deb installation.



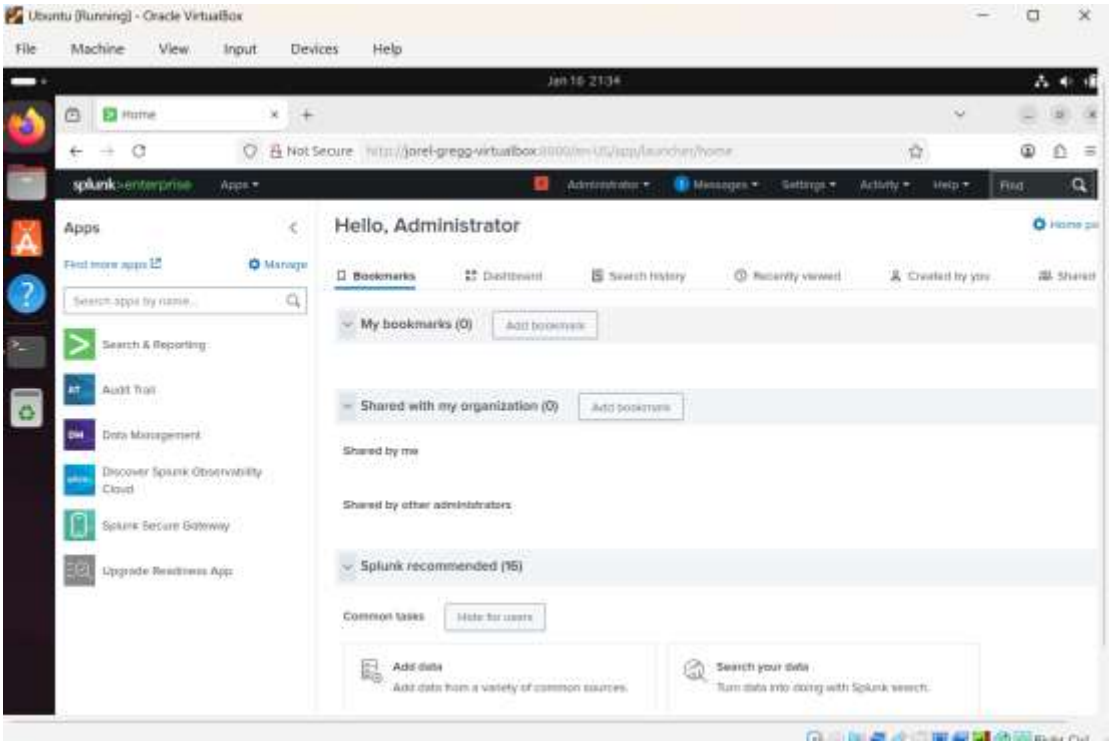
2. I then used the following command to install Splunk on the Ubuntu machine.
    a. sudo dpkg -i splunk-xxx.deb



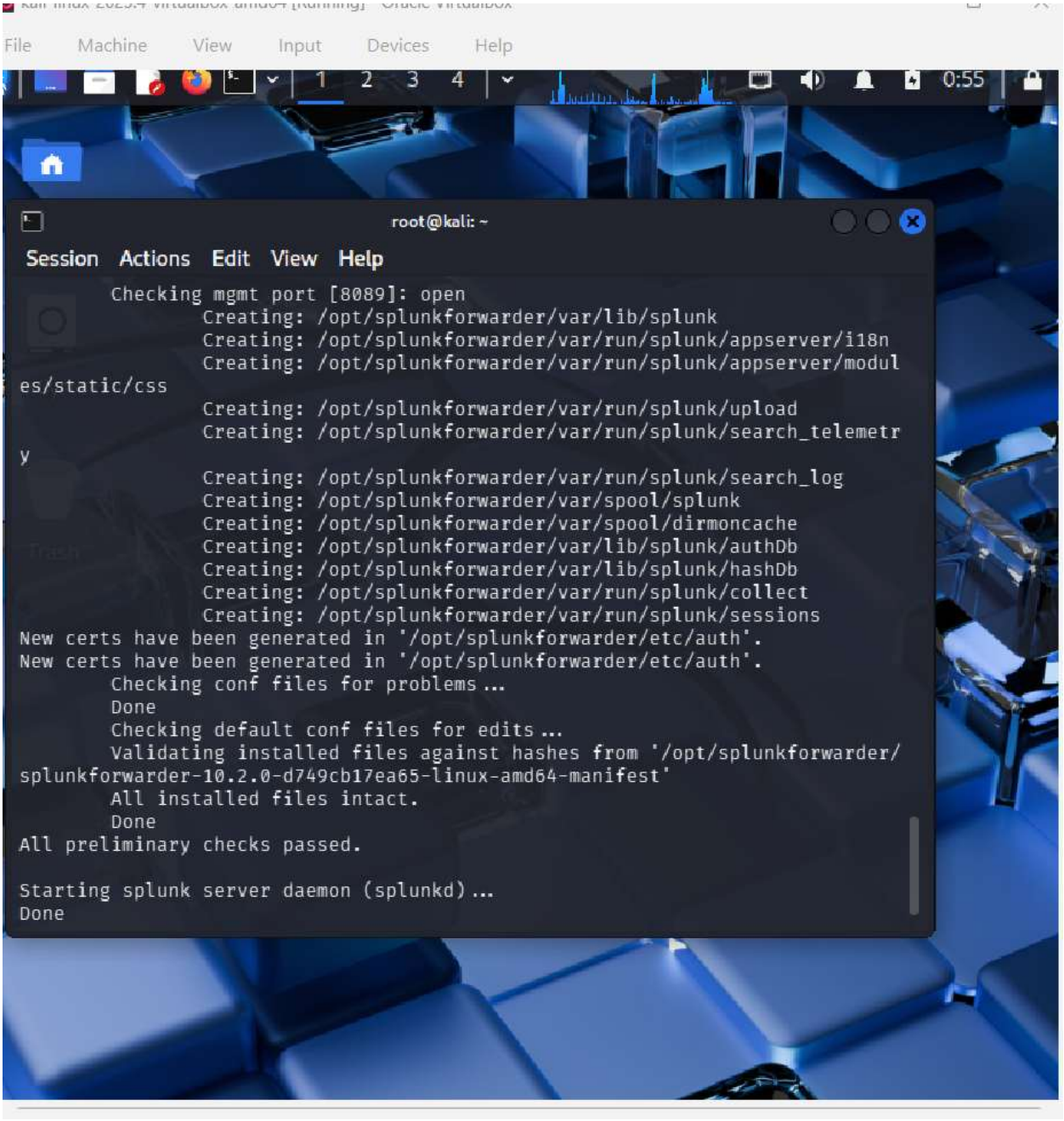
3. The next step was to launch Splunk which, after a lot of failure and research, I found I had to do through a non-root user and set their permissions to run the program.



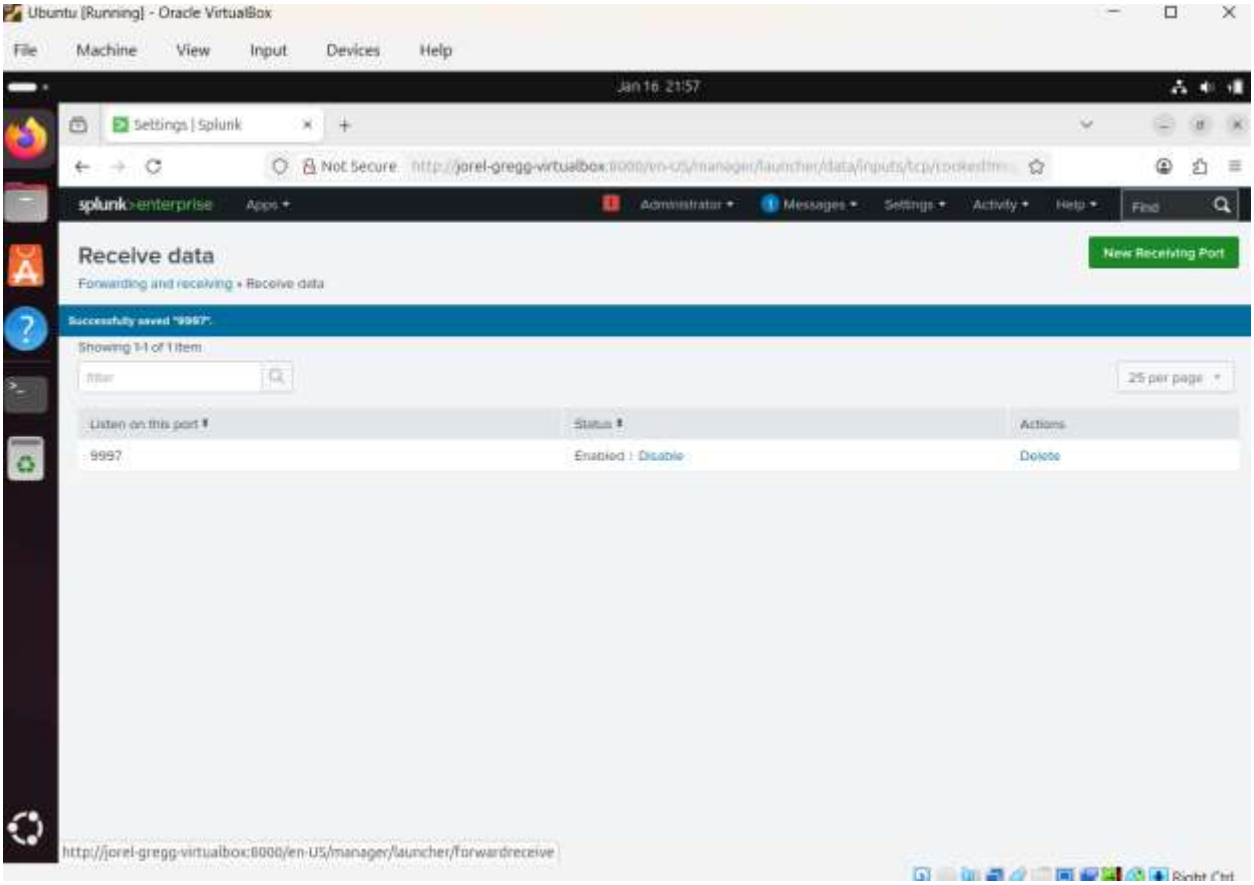
4. Once I knew it was up and running, I needed to reach the Splunk interface in my web browser.



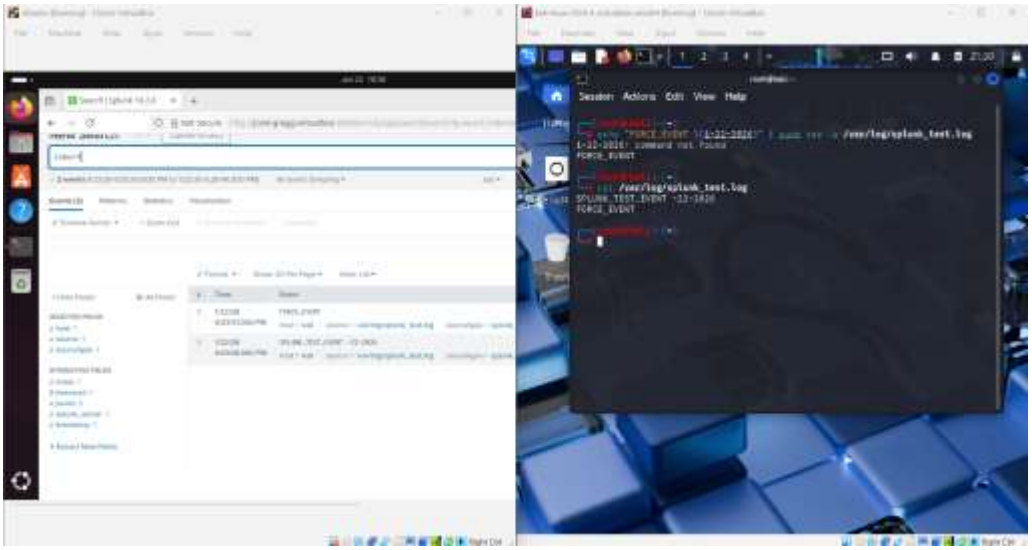
5. I then installed and ran the Splunk Forwarder program on my Kali-Linux virtual machine.



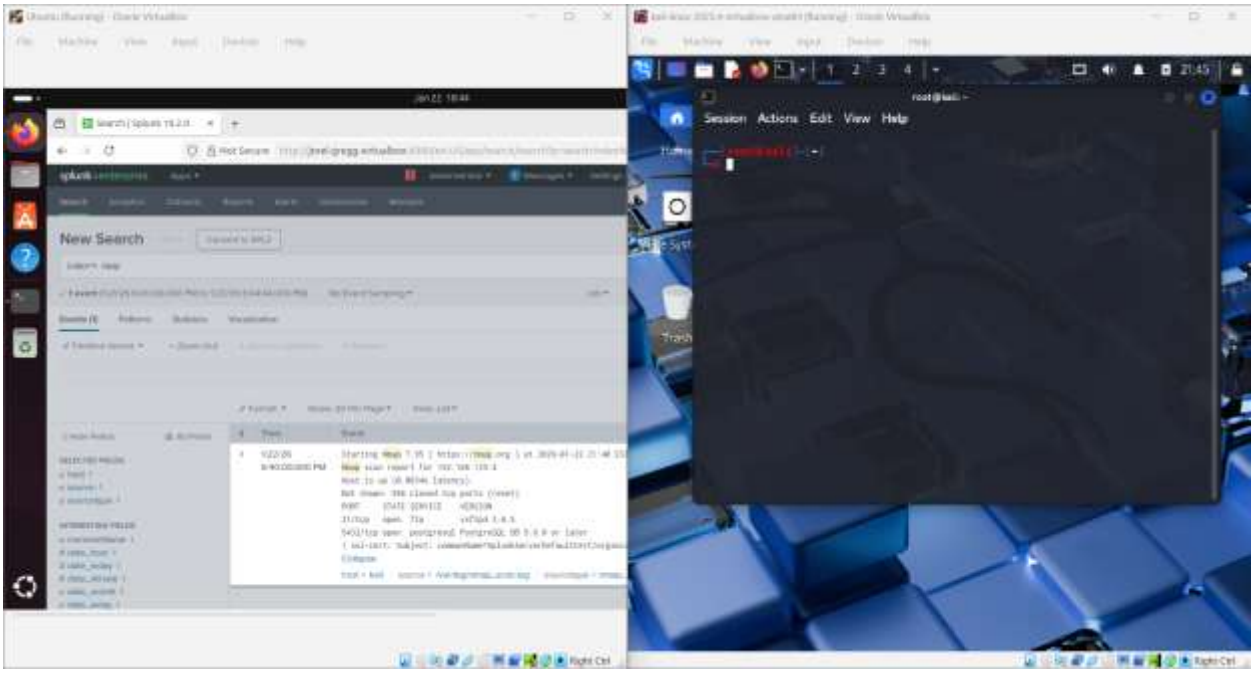
6. The next step was to ensure that I set up the Splunk receiving end on my Ubuntu machine to listen to port 9997.



7. Then I added my journal log in the Kali VM to my forwarder and restarted the forwarder. I couldn't find the journal log in the searches of Splunk so I had to set up a fake log file and create some events to ensure Splunk was receiving data.

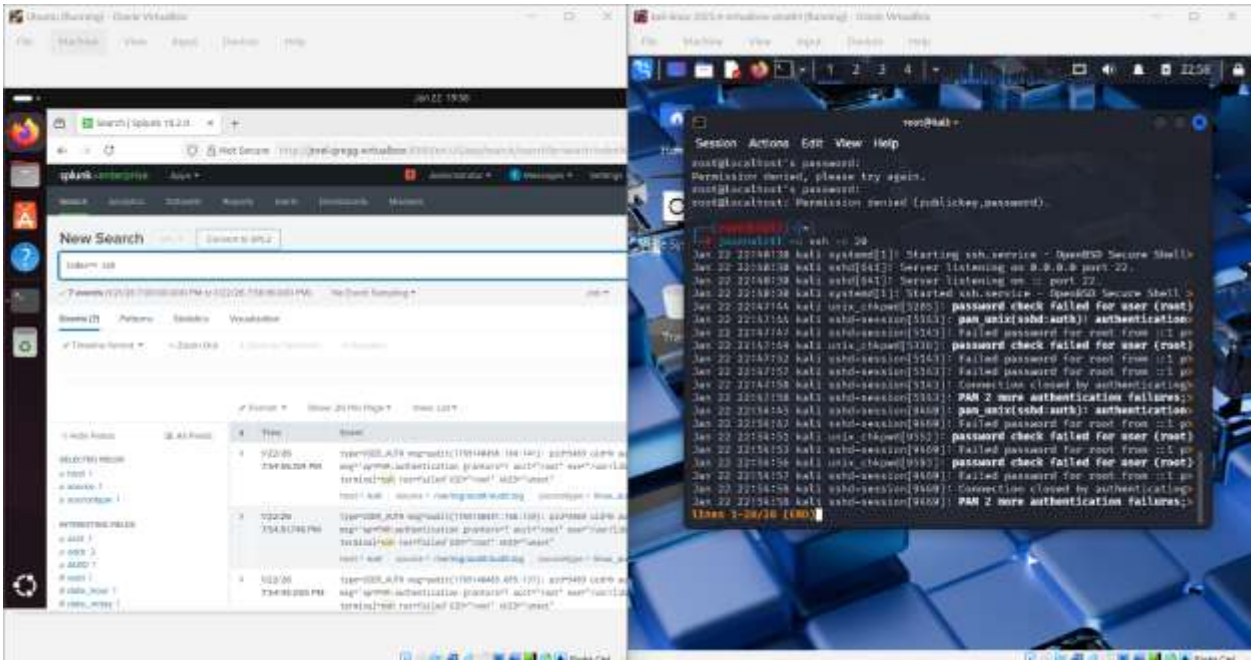


8. I began some with some basic threat actor actions like scanning with NMAP but I couldn't figure out why I couldn't' find any logs on Splunk. After doing some research I discovered that NMAP is not really "logged" and had to create a log file and add it to the monitors. Then when I scanned, I saved it to the log file to generate logs to find.

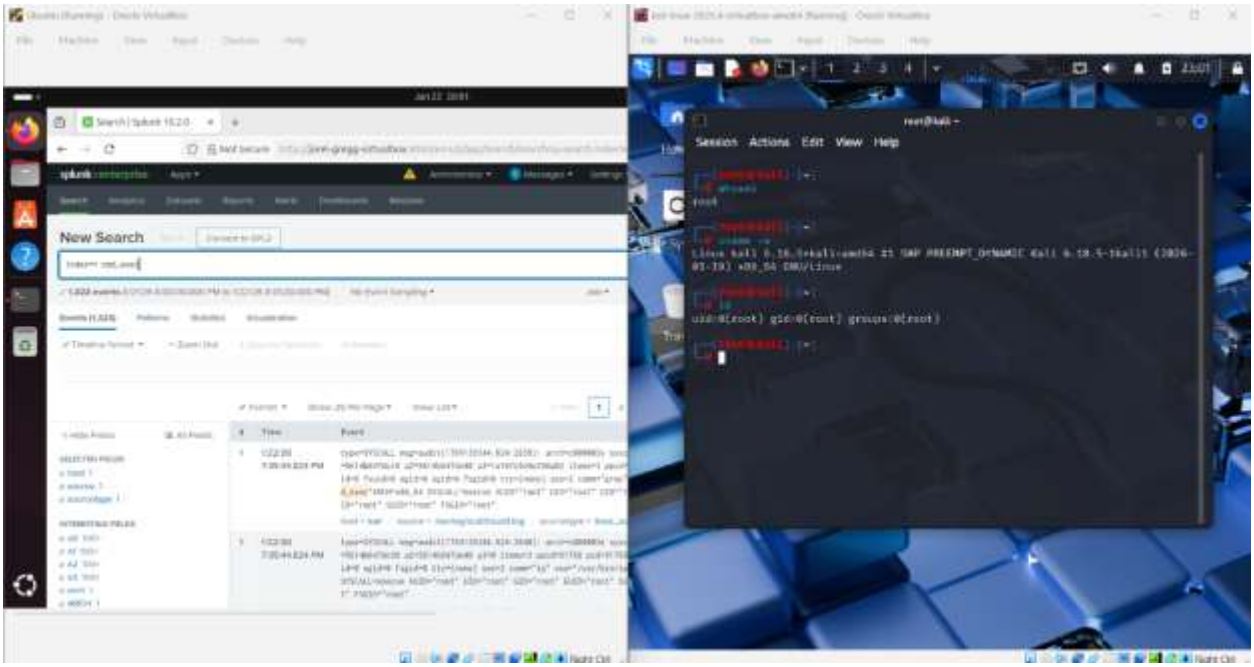


9. As I dug deeper into learning how SPLUNK works and finding what logs are NOT created in Kali, I researched and found that common commands needed to be set up in logs by an enterprise tool Audtid. I downloaded this onto Kali and configured it. While I was connected to the internet with my Kali VM I went ahead and grabbed ssh server as well so I could practice identifying that log data. I then turned the second network adapter off, so the machines were only on my local host network again.

10. First thing I attempted was to capture failed password attempts through SSH by just using ssh localhost and then the incorrect password three times. Then I went to my Splunk search and report and searched for index=* ssh which yielded results.



11. Last, I wanted to ensure that my Auditd was functioning, so I ran some simple commands such as whoami and id, then searched Splunk for index=* cmd_exec which showed that it was receiving the logs for the Auditd program.



This lab not only continued my education in learning Linux but allowed me to begin getting used to running the SIEM tool Splunk and identifying how to find log information that could potentially be a threat actor. My next goal is to continue learning what's capable with Splunk and begin setting up scheduled alerts based on the searches I completed in this lab.