

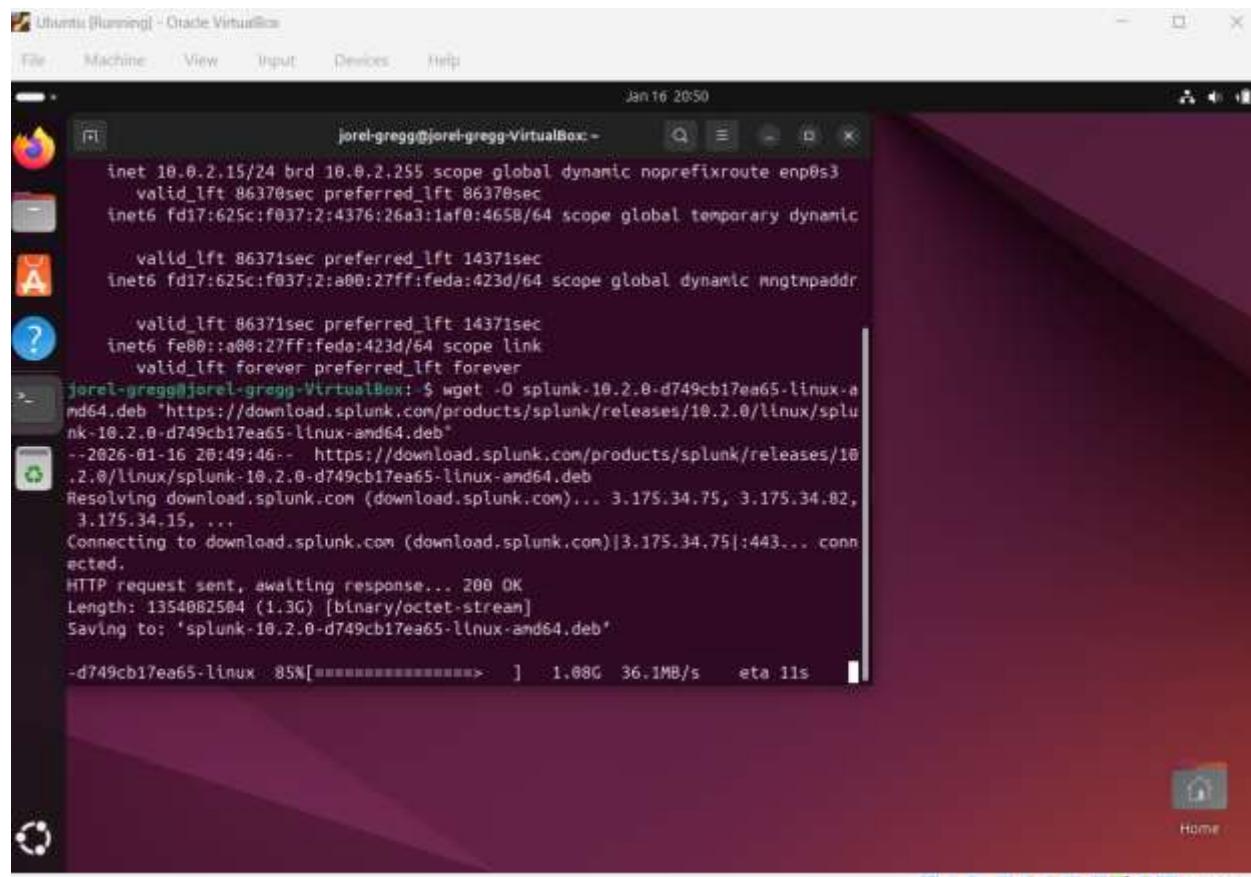
Jorel Gregg

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.



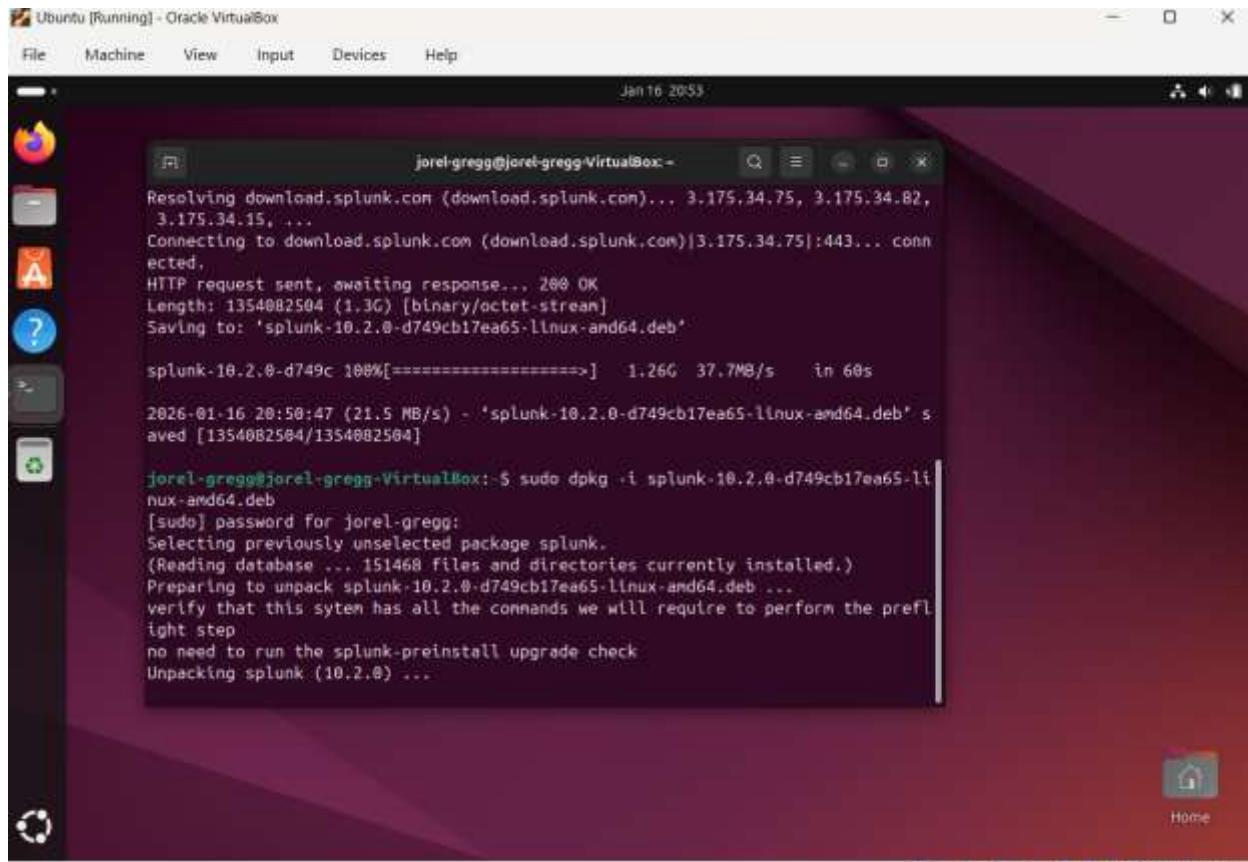
The screenshot shows a terminal window on an Ubuntu desktop. The terminal output is as follows:

```
inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
  valid_lft 86370sec preferred_lft 86370sec
inet6 fd17:625c:f037:2:4376:26a3:1af0:4658/64 scope global temporary dynamic
  valid_lft 86371sec preferred_lft 14371sec
inet6 fd17:625c:f037:2:a00:27ff:fed:423d/64 scope global dynamic mngtmpaddr
  valid_lft 86371sec preferred_lft 14371sec
inet6 fe80::a00:27ff:fed:423d/64 scope link
  valid_lft forever preferred_lft forever
jorel-gregg@jorel-gregg-VirtualBox: ~ wget -O splunk-10.2.0-d749cb17ea65-linux-amd64.deb 'https://download.splunk.com/products/splunk/releases/10.2.0/linux/splunk-10.2.0-d749cb17ea65-linux-amd64.deb'
--2026-01-16 28:49:46-- https://download.splunk.com/products/splunk/releases/10.2.0/linux/splunk-10.2.0-d749cb17ea65-linux-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 3.175.34.75, 3.175.34.82, 3.175.34.15, ...
Connecting to download.splunk.com (download.splunk.com)|3.175.34.75|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1354082504 (1.3G) [binary/octet-stream]
Saving to: 'splunk-10.2.0-d749cb17ea65-linux-amd64.deb'

-d749cb17ea65-linux 85%[=====>] 1.08G 36.1MB/s eta 11s
```

2. I then used the following command to install Splunk on the Ubuntu machine.

a. sudo dpkg -i splunk-xxx.deb



The screenshot shows a terminal window titled "Ubuntu [Running] - Oracle VirtualBox" with the command "sudo dpkg -i splunk-xxx.deb" being run. The terminal output shows the download of the Splunk package from download.splunk.com, the extraction of the package, and the successful installation of the "splunk-10.2.0-d749cb17ea65-linux-amd64.deb" package. The terminal window is part of a desktop environment with icons for a browser, file manager, terminal, and help.

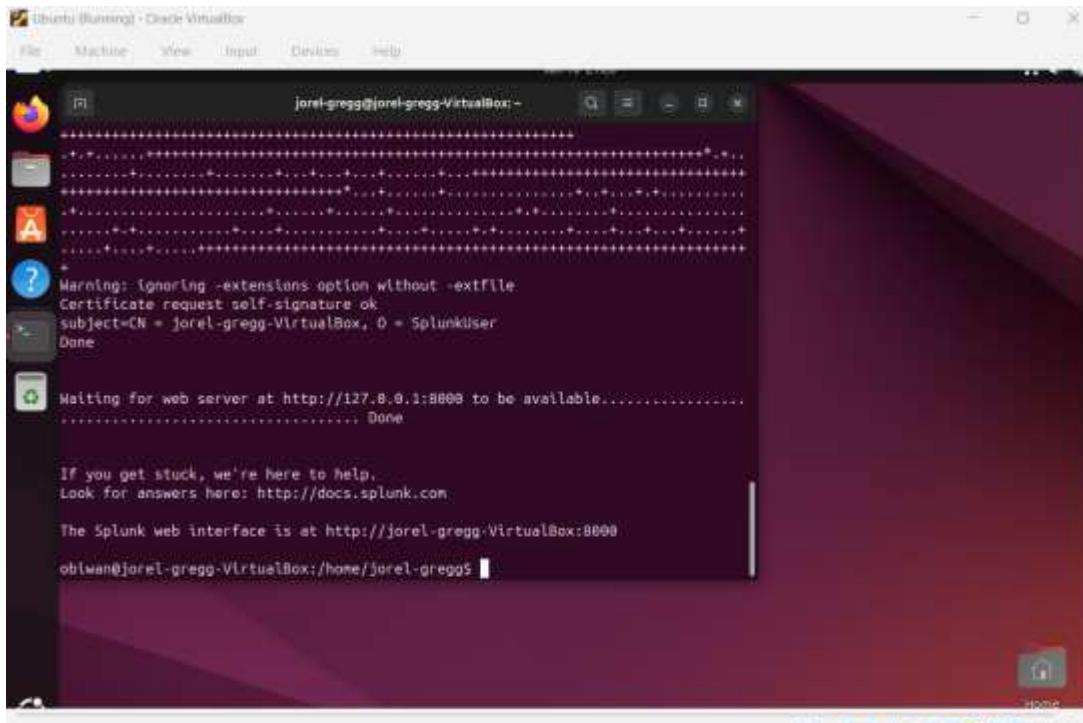
```
Resolving download.splunk.com (download.splunk.com)... 3.175.34.75, 3.175.34.82, 3.175.34.15, ...
Connecting to download.splunk.com (download.splunk.com)|3.175.34.75|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1354082504 (1.3G) [binary/octet-stream]
Saving to: 'splunk-10.2.0-d749cb17ea65-linux-amd64.deb'

splunk-10.2.0-d749c 100%[=====] 1.26G 37.7MB/s in 60s

2026-01-16 20:50:47 (21.5 MB/s) - 'splunk-10.2.0-d749cb17ea65-linux-amd64.deb' saved [1354082504/1354082504]

jorel-gregg@jorel-gregg-VirtualBox:~$ sudo dpkg -i splunk-10.2.0-d749cb17ea65-li
nux-amd64.deb
[sudo] password for jorel-gregg:
Selecting previously unselected package splunk.
(Reading database ... 151468 files and directories currently installed.)
Preparing to unpack splunk-10.2.0-d749cb17ea65-linux-amd64.deb ...
verify that this system has all the commands we will require to perform the preflight step
no need to run the splunk-preinstall upgrade check
Unpacking splunk (10.2.0) ...
```

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.



jorel-gregg@jorel-gregg-VirtualBox:~

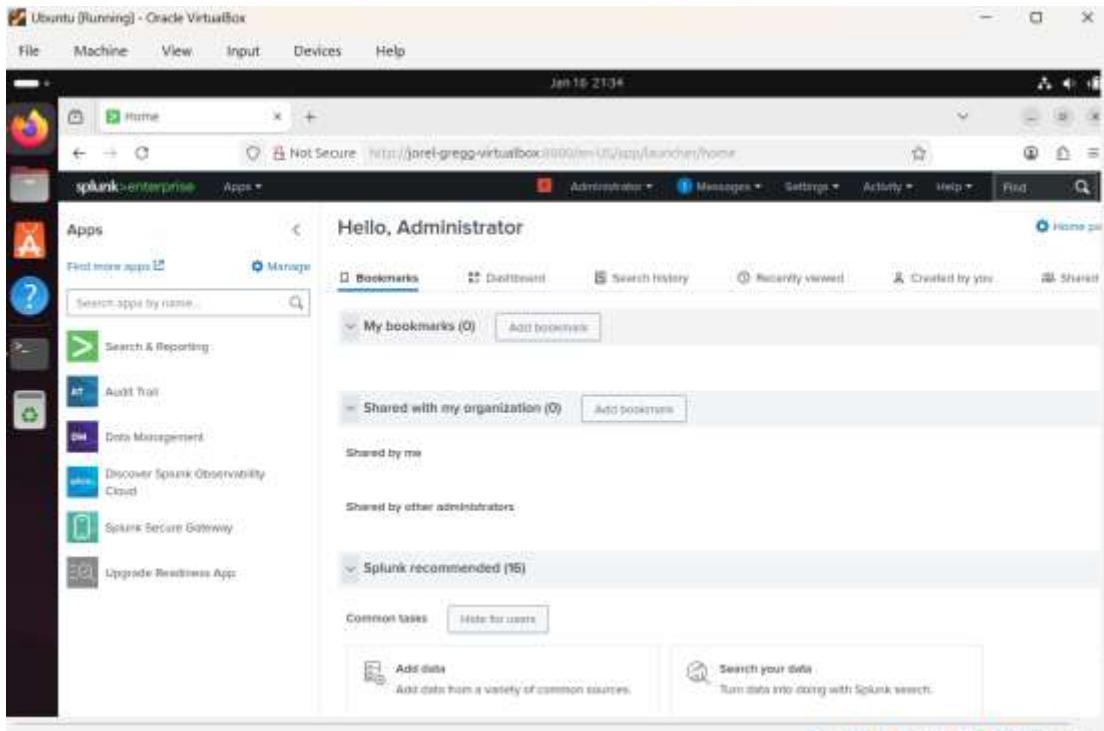
```
Warning: ignoring -extensions option without -extfile
Certificate request self-signature ok
subject=CN = jorel-gregg-VirtualBox, O = SplunkUser
Done

Waiting for web server at http://127.8.0.1:8000 to be available.....
Done

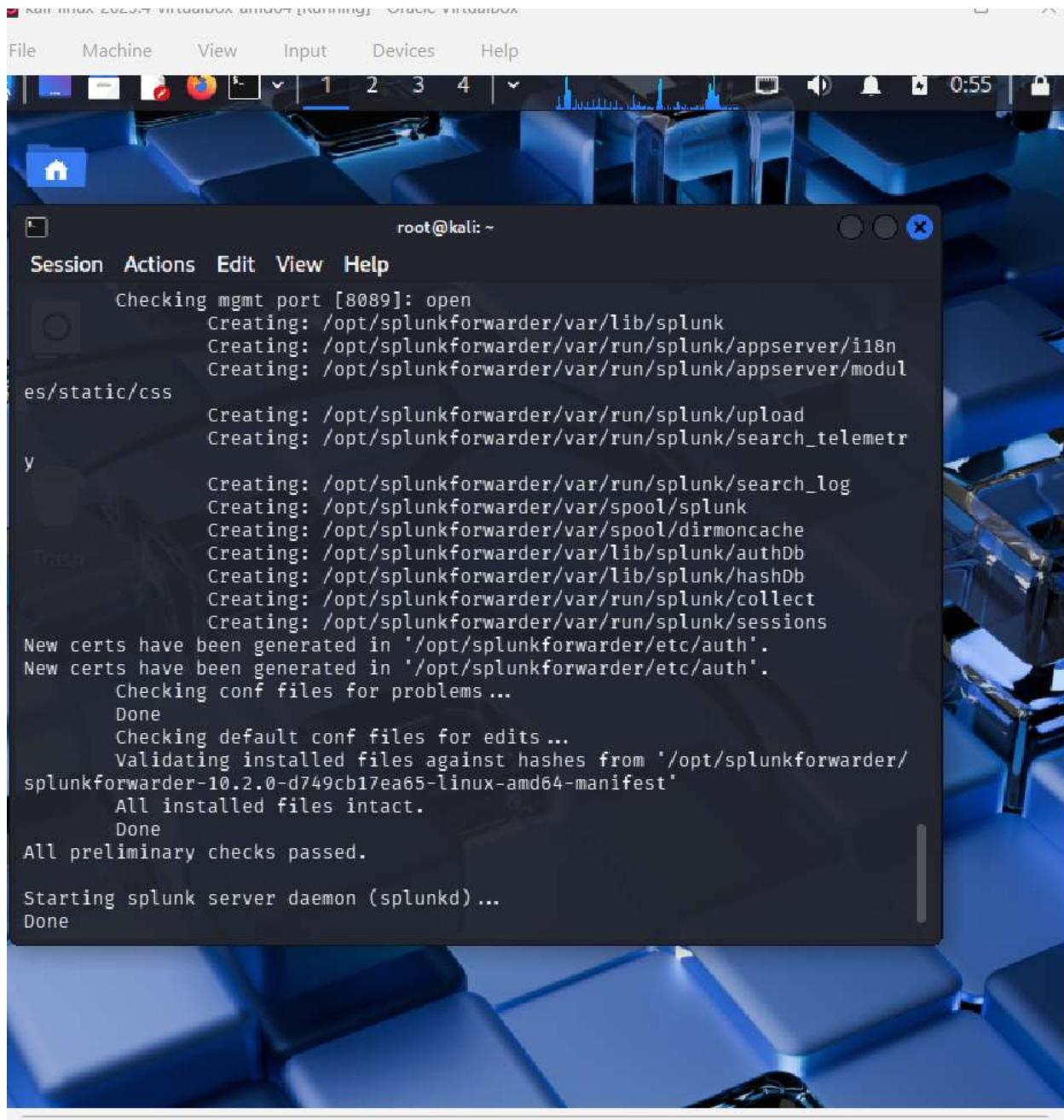
If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk Web interface is at http://jorel-gregg-VirtualBox:8000
oblwan@jorel-gregg-VirtualBox:/home/jorel-gregg$
```

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.

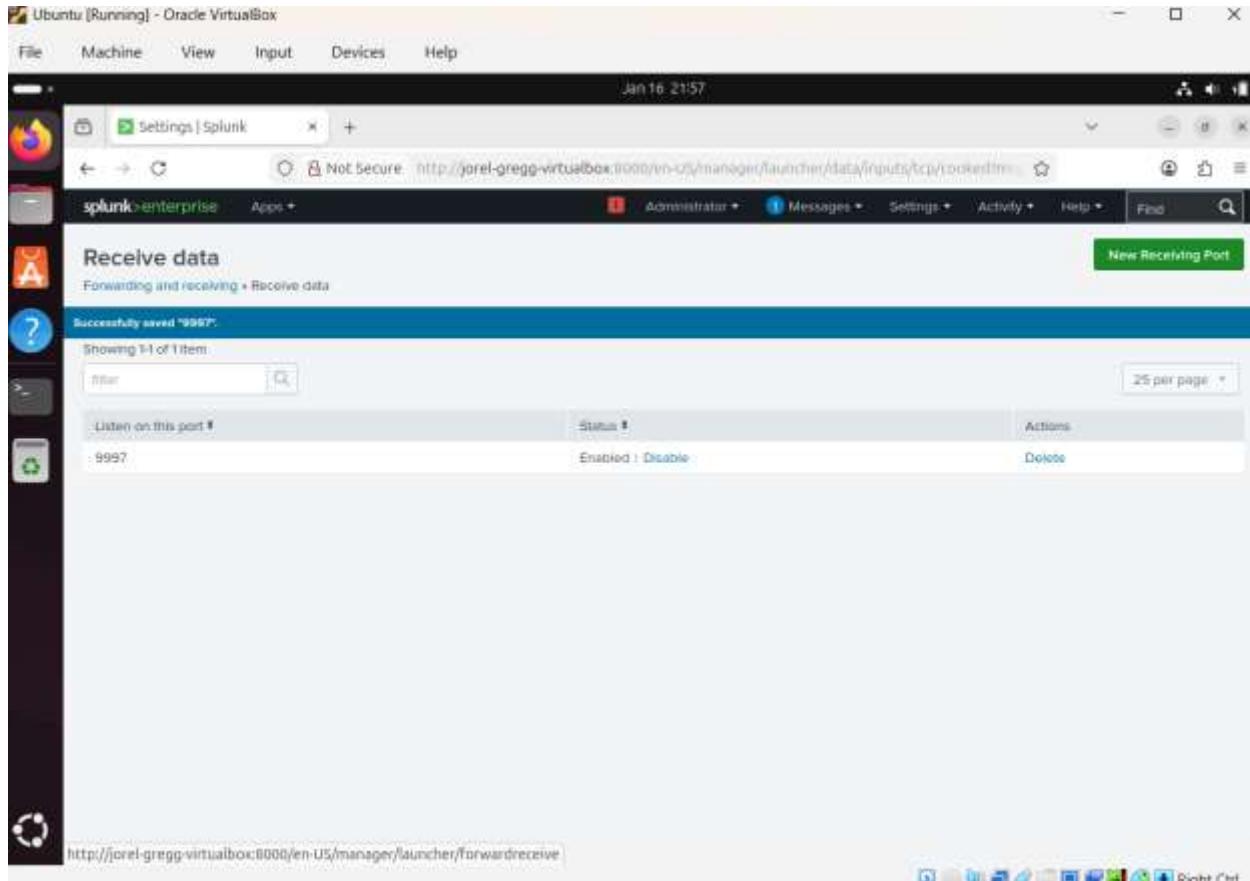


root@kali:~

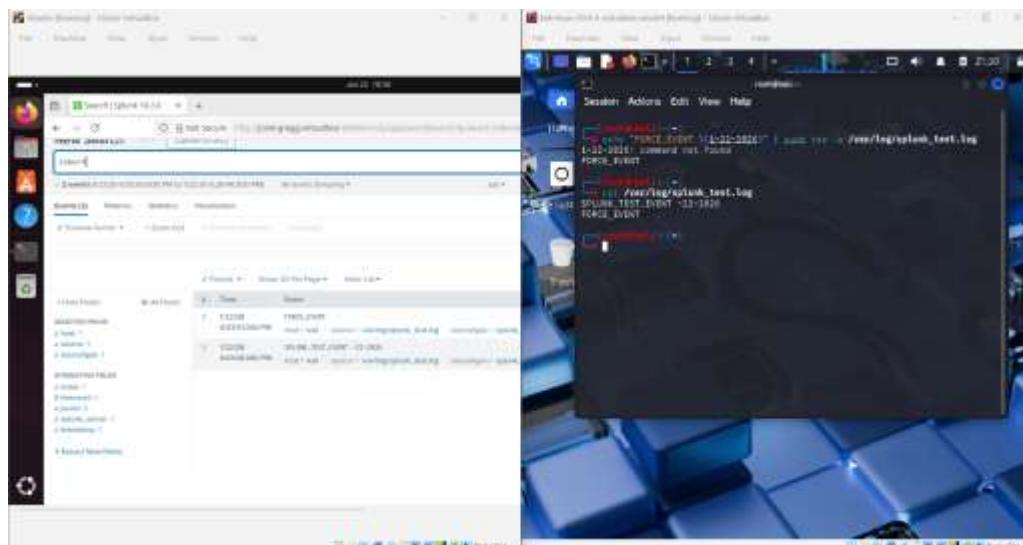
```
Session Actions Edit View Help
Checking mgmt port [8089]: open
Creating: /opt/splunkforwarder/var/lib/splunk
Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
Creating: /opt/splunkforwarder/var/run/splunk/upload
Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
Creating: /opt/splunkforwarder/var/run/splunk/search_log
Creating: /opt/splunkforwarder/var/spool/splunk
Creating: /opt/splunkforwarder/var/spool/dirmoncache
Creating: /opt/splunkforwarder/var/lib/splunk/authDb
Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
Creating: /opt/splunkforwarder/var/run/splunk/collectors
Creating: /opt/splunkforwarder/var/run/splunk/sessions
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
    Checking conf files for problems ...
    Done
    Checking default conf files for edits ...
    Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-10.2.0-d749cb17ea65-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd) ...
Done
```

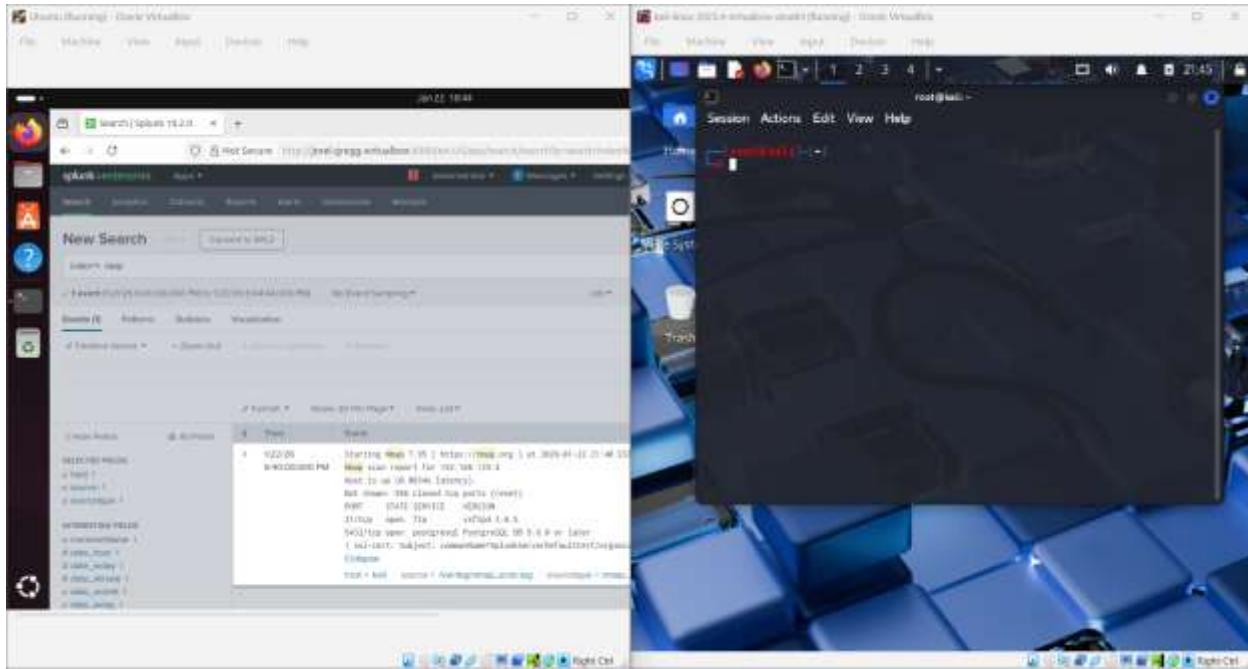
6. The next step was to ensure that I set up the Splunk receiving end on my Ubuntu machine to listen to port 9997.



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.

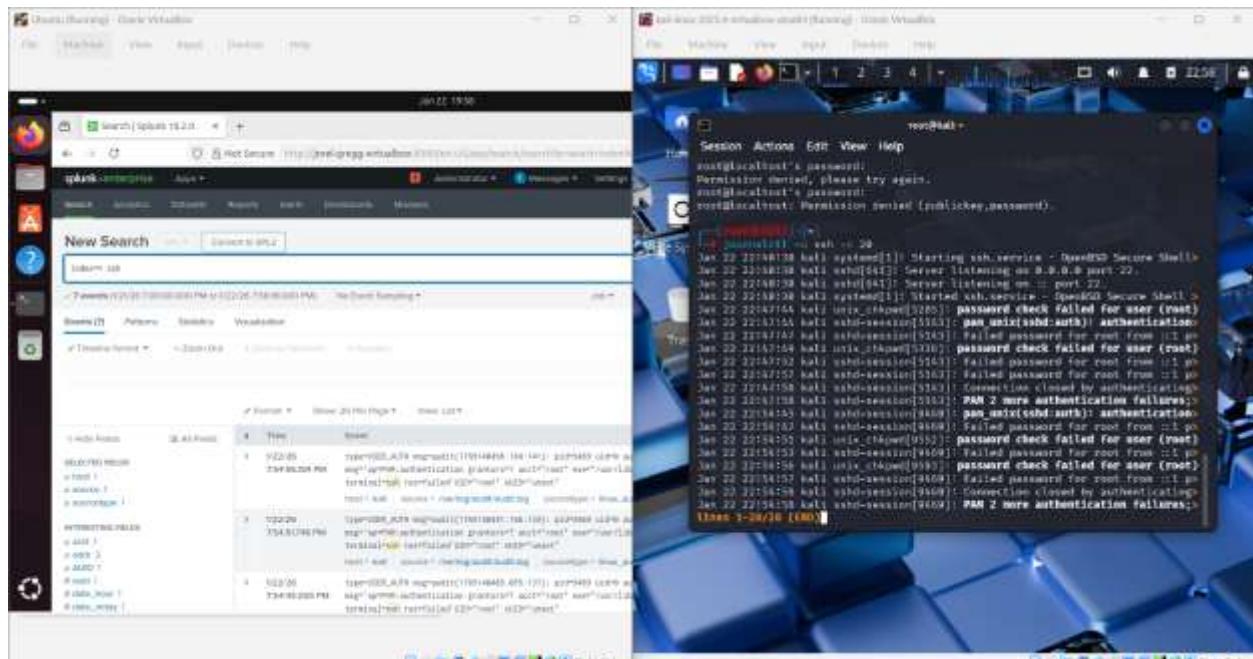


8. I began some with some basic threat actor actions like scanning with NMAP but I couldn't figure out why I couldn't find any logs on Splunk. After doing some research I discovered that NMAP is not really "logged" and had to create a log file and add it to the monitors. Then when I scanned, I saved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

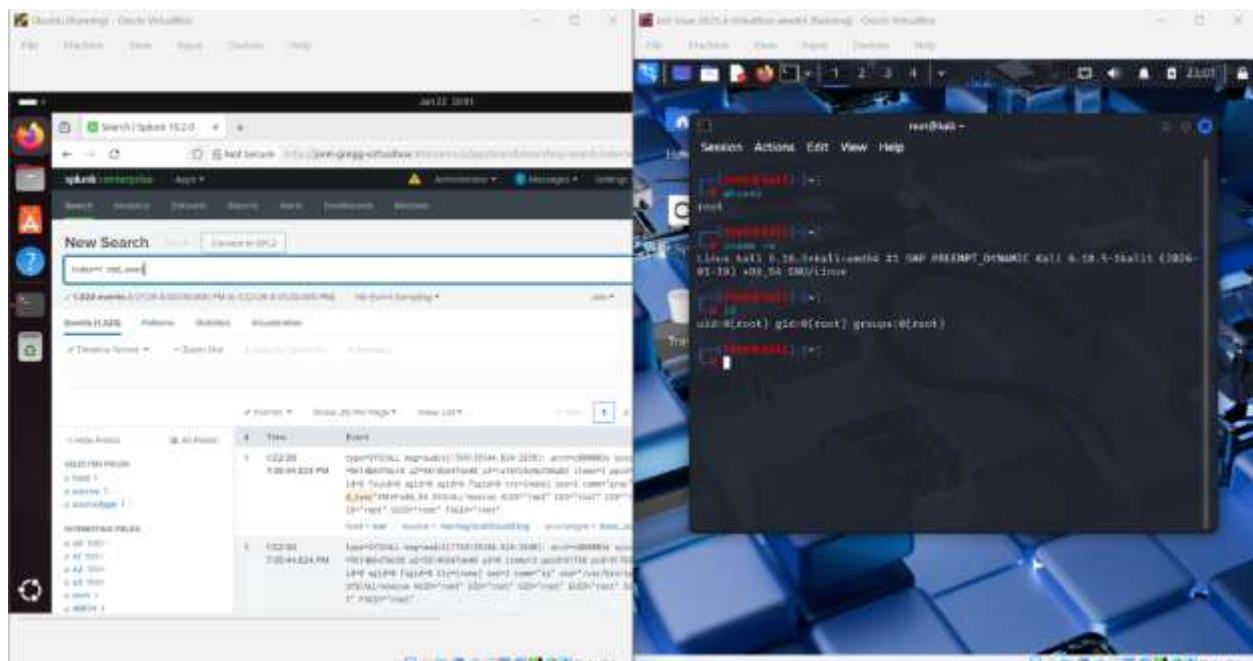


9. As I dug deeper into learning how SPLUNK works and finding what logs are NOT created in Kali, I researched and found that common commands needed to be set up in logs by an enterprise tool Audited. I downloaded this onto Kali and configured it. While I was connected to the internet with my Kali VM 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 Audited 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 Audited 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.