




## 2. Network Lab , Shared Folder and Splunk Installation Settings

Change Network Settings to NAT NETWORK



Host-only Networks NAT Networks Cloud Networks

Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NatNetwork	10.0.2.0/24		Enabled

General Options Port Forwarding

Name: AD LAB

IPv4 Prefix: 192.168.10.0/24

☒ Enable DHCP











☐ Enable IPv6

IPv6 Prefix:

☐ Advertise Default IPv6 Route

ApplyReset

Apply the newly created network to the Splunk server :

 General
  System
  Display
  Storage
  Audio
  **Network**
 Serial Ports
  USB
  Shared Folders
  User Interface

## Network

Adapter 1
 Adapter 2
 Adapter 3
 Adapter 4

☒ Enable Network Adapter
 

Attached to: NAT Network

Name: AD LAB

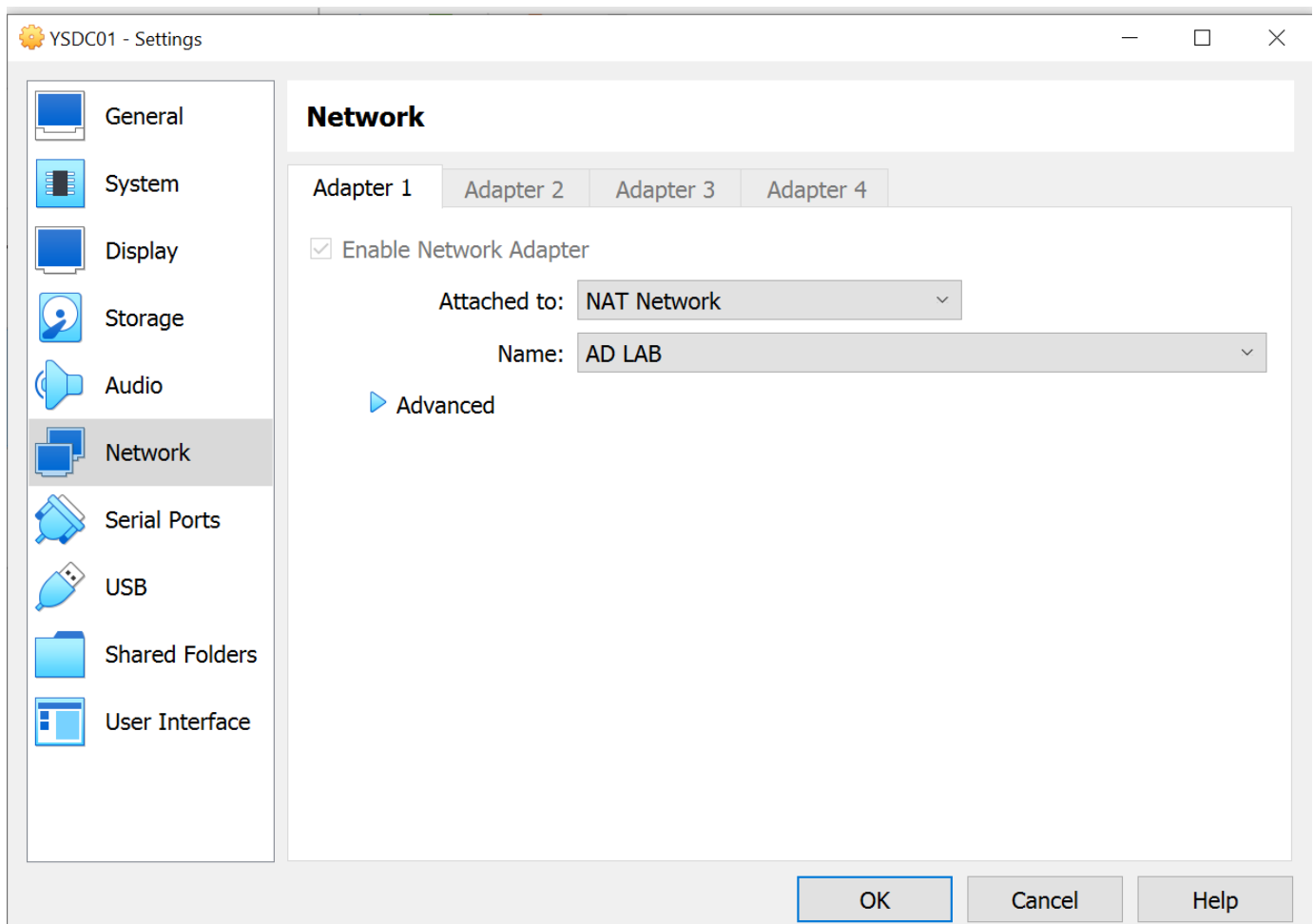
▶ Advanced

OK

Cancel

Help

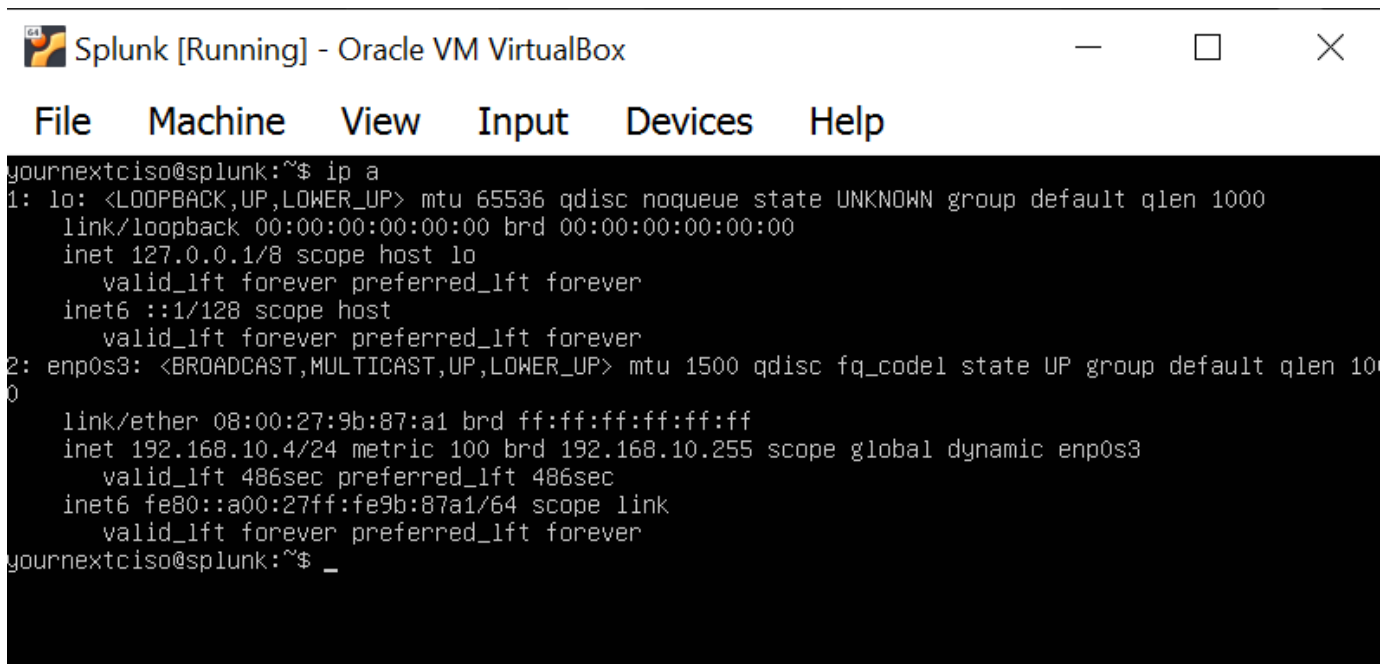
Do the same to the AD server, windows client and kali machine :



And that should set it.

## Setting up Static IP for the Splunk server


Note the ip address currently assigned through dhcp . Use ip a :



Change into the /etc/netplan directory to edit the network config file : Modify this initial setup

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: true
  version: 2
```

To this :

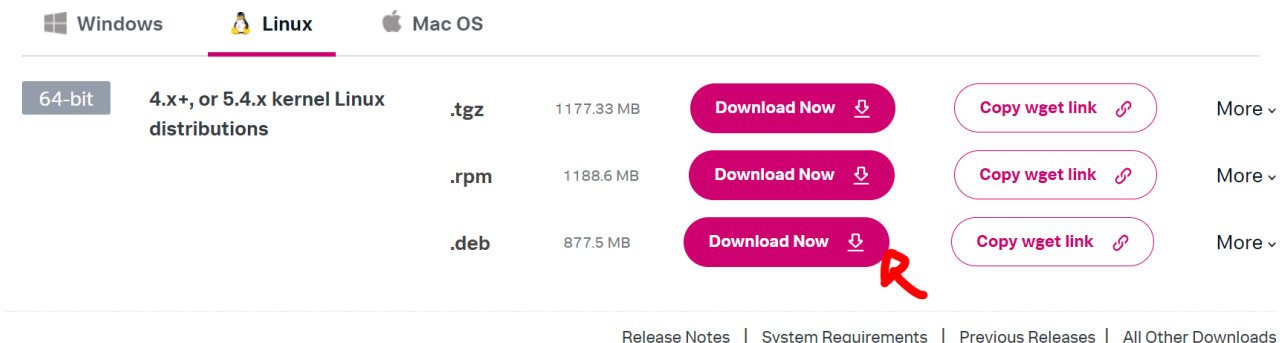


The screenshot shows a virtual machine window titled "Splunk [Running] - Oracle VM VirtualBox". The window has a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". The main area displays a terminal window running "GNU nano 6.2" editing a file named "00-installer-config.yaml". The terminal shows the same network configuration as the previous block, but with modifications: "dhcp4: no", "addresses: [192.168.10.4/24]", "nameservers: [8.8.8.8]", and "routes: - to: default, via: 192.168.10.1". The cursor is at the end of the "nameservers" line.

Save the config and apply it . Use sudo netplan apply:

## Downloading Splunk

1. Head over to Splunk.com and download the setup file [here](#)  
Choose Your Installation Package



The screenshot shows the "Choose Your Installation Package" section of the Splunk download page. It has tabs for "Windows", "Linux", and "Mac OS", with "Linux" selected. Under the "Linux" tab, there are three rows of download links for different Linux distributions: "4.x+, or 5.4.x kernel Linux distributions". Each row has a "Download Now" button with a download icon, a "Copy wget link" button with a link icon, and a "More" dropdown menu. A red arrow points to the "Download Now" button for the ".deb" package.

Package Type	Size	Download Now	Copy wget link	More
64-bit .tgz	1177.33 MB	Download Now	Copy wget link	More
64-bit .rpm	1188.6 MB	Download Now	Copy wget link	More
64-bit .deb	877.5 MB	Download Now	Copy wget link	More

Release Notes | System Requirements | Previous Releases | All Other Downloads

2. Install the virtualbox guess addon file on the splunk vm :

```
yournextciso@splunk:/$ sudo apt-get install virtualbox
virtualbox                                virtualbox-guest-utils                    virtualbox-qt
virtualbox-dkms                          virtualbox-guest-utils-hwe                virtualbox-source
virtualbox-ext-pack                      virtualbox-guest-x11
virtualbox-guest-additions-iso          virtualbox-guest-x11-hwe
yournextciso@splunk:/$ sudo apt-get install virtualbox-guest-additions-iso _
```

Install the virtualbox-guest-utils (sudo apt-get install virtualbox-guest-utils):

```
(Reading database ... 97619 files and directories currently installed.)
Preparing to unpack .../virtualbox-guest-utils_6.1.50-dfsg-1~ubuntu1.22.04.3_am
Unpacking virtualbox-guest-utils (6.1.50-dfsg-1~ubuntu1.22.04.3) ...
Setting up virtualbox-guest-utils (6.1.50-dfsg-1~ubuntu1.22.04.3) ...
Created symlink /etc/systemd/system/multi-user.target.wants/virtualbox-guest-ut
stemd/system/virtualbox-guest-utils.service.
[ 233.233249] vboxsf: Unknown parameter 'tag'
Processing triggers for man-db (2.10.2-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

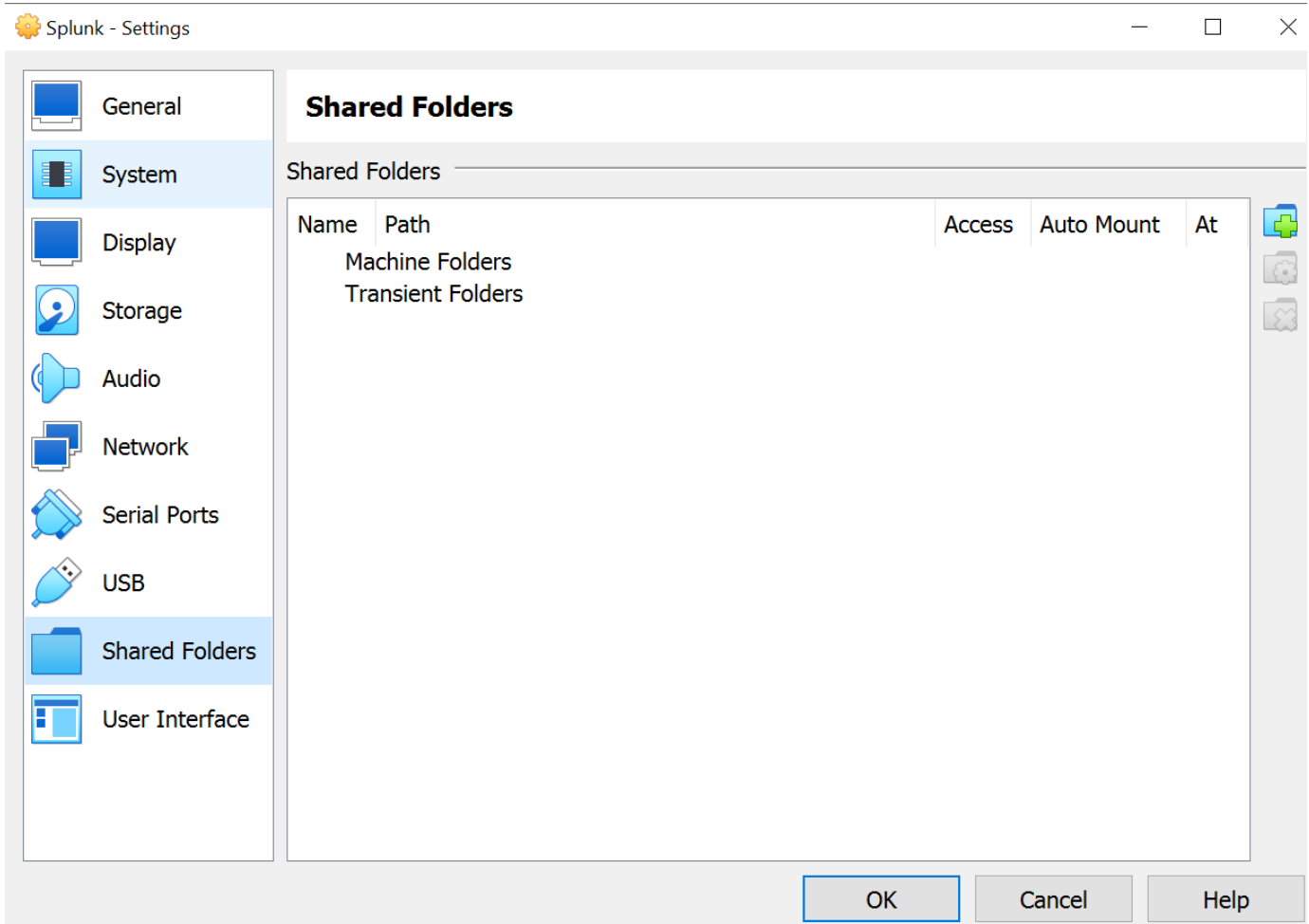
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
yournextciso@splunk:~$ _
```

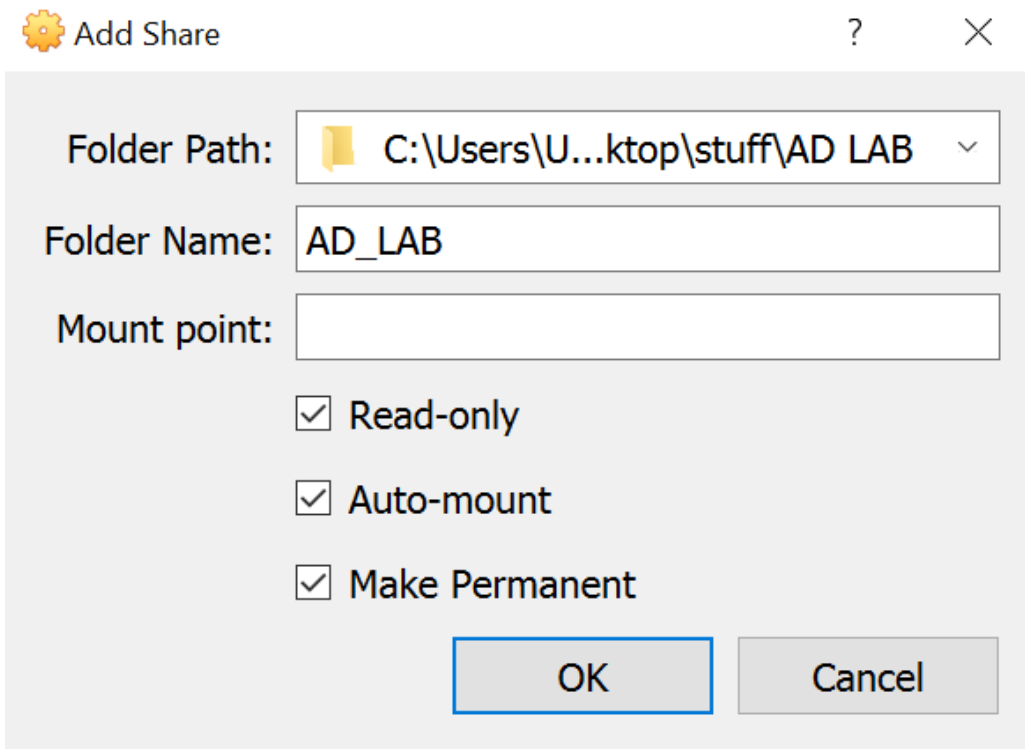
## Share Folder creation

Since we will be downloading the splunk package on our host machine it is better if we create a shared folder accessible to the splunk VM. Choose a directory and create a folder(name it anything you want).

Then head over to the splunk VM, and in the top menu click on devices --> Shared folders --> Shared folder settings :



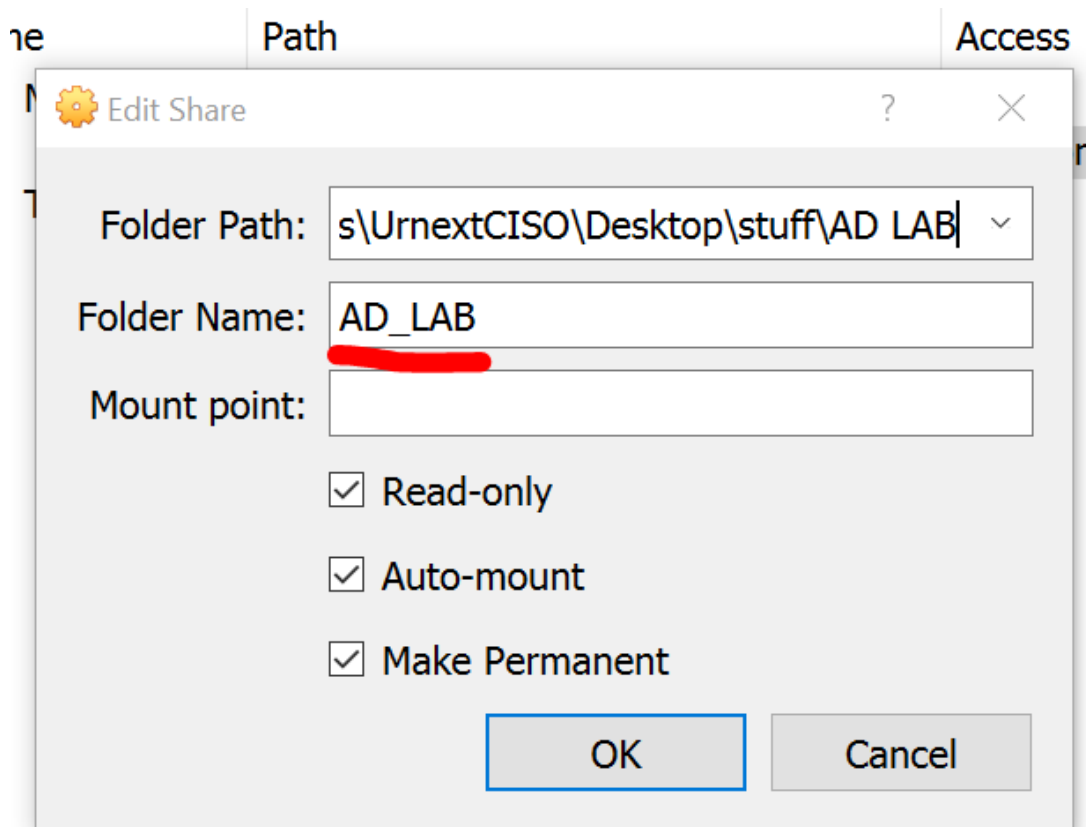
Add the folder you just created and assign various permission settings :



Now move the downloaded .deb file into the folder you just created and reboot the Splunk Now add the share user : `sudo adduser "username" vboxsf`:

```
yournextciso@splunk:~$ sudo adduser yournextciso vboxsf
Adding user `yournextciso' to group `vboxsf' ...
Adding user yournextciso to group vboxsf
Done.
yournextciso@splunk:~$ _
```

Make a directory called share and mount the directory created earlier onto our share folder:



```
yournextciso@splunk:~$ sudo adduser yournextciso vboxsf
Adding user `yournextciso' to group `vboxsf' ...
Adding user yournextciso to group vboxsf
Done.
yournextciso@splunk:~$ mkdir share
yournextciso@splunk:~$ ls
share
yournextciso@splunk:~$ sudo mount -t vboxsf -o uid=1000,gid=1000 AD_LAB share/
yournextciso@splunk:~$
```

Now log out and then login let the settings take effect :

```

yournextciso@splunk:~$ cd share/
yournextciso@splunk:~/share$ ls -la
total 898560
drwxrwxrwx 1 yournextciso yournextciso      0 Jan  9 12:02 .
drwxr-x--- 5 yournextciso yournextciso    4096 Jan  9 12:31 ..
-rwxrwxrwx 1 yournextciso yournextciso 920120936 Jan  9 11:38 splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb
yournextciso@splunk:~/share$

```

Now install splunk sudo dpkg -i "splunk file" :

```

yournextciso@splunk:~/share$ sudo dpkg -i splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb
[sudo] password for yournextciso:
Selecting previously unselected package splunk.
(Reading database ... 97633 files and directories currently installed.)
Preparing to unpack splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb ...
no need to run the pre-install check
Unpacking splunk (9.4.0) ...
Setting up splunk (9.4.0) ...
complete
yournextciso@splunk:~/share$

```

Cd into the directory where splunk is installed. cd /opt/splunk and then change into the splunk user by executing sudo -u splunk bash :

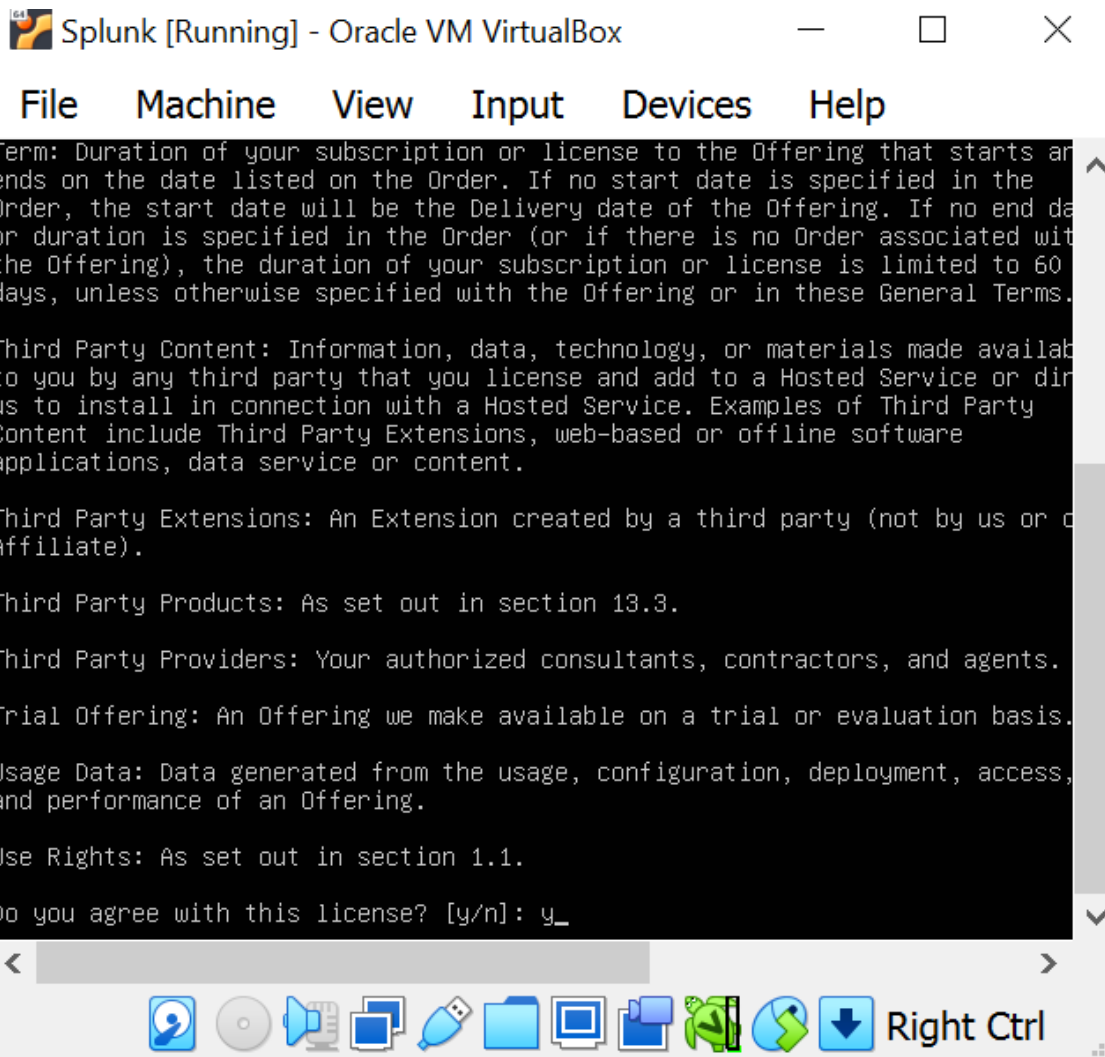
```

yournextciso@splunk:/opt/splunk$ sudo -u splunk bash
[sudo] password for yournextciso:
splunk@splunk:~$

```

Go into the splunk binary directory cd bin , and run the installer (./splunk start) , press q and the y to accept the agreement :





Set the username and password and wait for the setup to be completed.

```
Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=splunk/O=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib
and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased
security
Done

Waiting for web server at http://127.0.0.1:8000 to be available..... Done
ne

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

The Splunk web interface is at http://splunk:8000

yournextciso@splunk:~$
```

You can now access the splunk GUI by booting up your kali vm and navigating to the <http://<>:8000>: