## **Installation of Splunk SIEM and Log Forwarding**

## **Introduction to the Lab**

Splunk is an innovative technology which searches and indexes log files and helps organizations derive insights from the data. A main benefit of Splunk is that it uses indexes to store data, and so does not require a separate database to store its information. Splunk is used for monitoring and searching through big data. It indexes and correlates information in a container that makes it searchable, and makes it possible to generate alerts, reports, and visualizations. It can recognize data patterns, create metrics, and help diagnose problems, for business challenges like IT management, security, and compliance.

Splunk forwarders consume data and send it to an indexer. Forwarders require minimal resources and have little impact on performance, so they can usually reside on the machines where the data originates. There are two kinds of forwarders in Splunk.

1. The **universal forwarder** contains only the components that are necessary to forward data. The universal forwarder is designed to run on production servers, having minimal CPU and memory usage and the least impact possible on mission-critical software.
2. A **heavy forwarder is a full Splunk Enterprise instance** that can index, search, and change data as well as forward it. Splunk forwarder in our Splunk server ubuntu machine acts as an agent for log collection from remote machines. Splunk forwarder collects logs from remote machines and forwards them to the indexer (Splunk database) for further processing and storage.

**Note:** Universal forwarders do not have a web or application interface. Once installed, you must make configuration changes at the command line in both Windows and Unix- or Linux-based systems.

**Best practices:**

* + Use the universal forwarder when possible as a data collection method.
  + Stop and start the universal forwarder from the command line.

## **Pre-requisites of the lab**

The pre-requisites (recommended system requirement) for configuring Universal Forwarder and Splunk Server for log collection are:

* VMware Fusion or Workstation (It must be registered; trials will not work)
* Install two Ubuntu Virtual machines
* RAM 2+GB
  + 2 GHz dual core processor or higher
  + 4 GB system memory
  + 20 GB of free hard drive space
  + Internet access
* Make sure both virtual machines are on the same network, Preferably NAT

## **Steps of the lab:**

To get our VM up and running, we will need to execute the following steps:

**Step 1:** Preparing the first Ubuntu VM for Splunk Installation

**Step 2**: Configuring receiving port at Ubuntu Splunk Server

**Step 3:** Download and install Splunk Universal Forwarder on second ubuntu machine

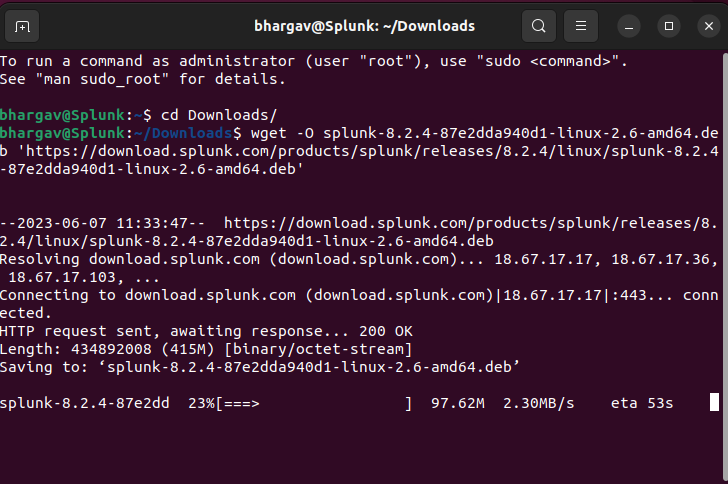
**Step 4:** Searching and Reporting App – Capture the logs in Splunk Ubuntu Server

## **Execution of the lab**

**Step 1: Preparing the first Ubuntu VM for Splunk Installation**

**Open the command terminal and run the following commands**

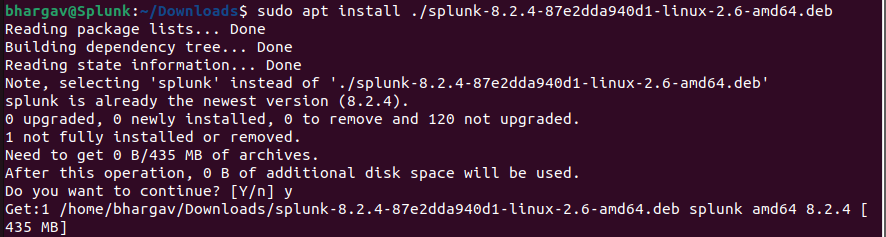
1. Change to the Downloads directory using the command cd Downloads/
2. Run the command below to download Splunk.



wget -O splunk-8.2.4-87e2dda940d1-linux-2.6-amd64.deb 'https://download.splunk.com/products/splunk/releases/8.2.4/linux/splunk-8.2.4-87e2dda940d1-linux-2.6-amd64.deb'

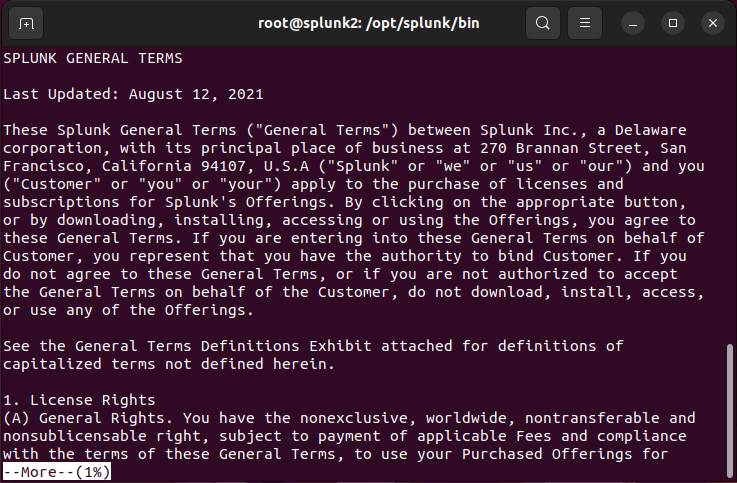
1. Run the command below to install the downloaded Splunk package

sudo apt install ./splunk-8.2.4-87e2dda940d1-linux-2.6-amd64.deb

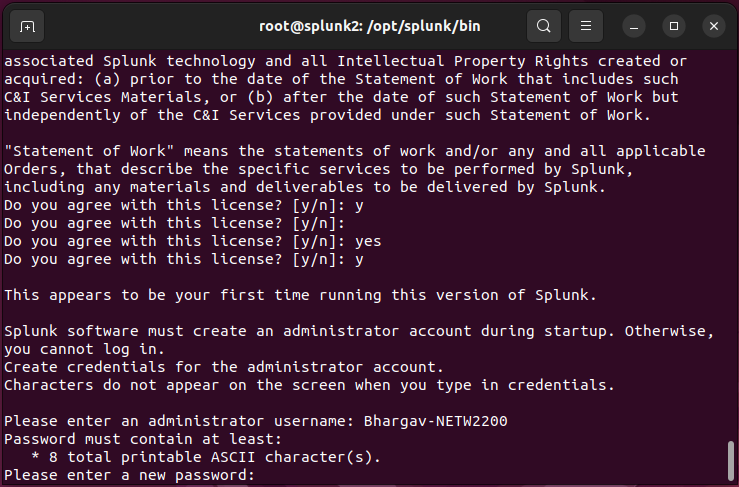


1. Switch to root using the command sudo su and input your password
2. Switch to the Splunk directory using the command cd /opt/splunk/bin
3. Run the command to accept Splunk license and

./splunk start --accept-licence/



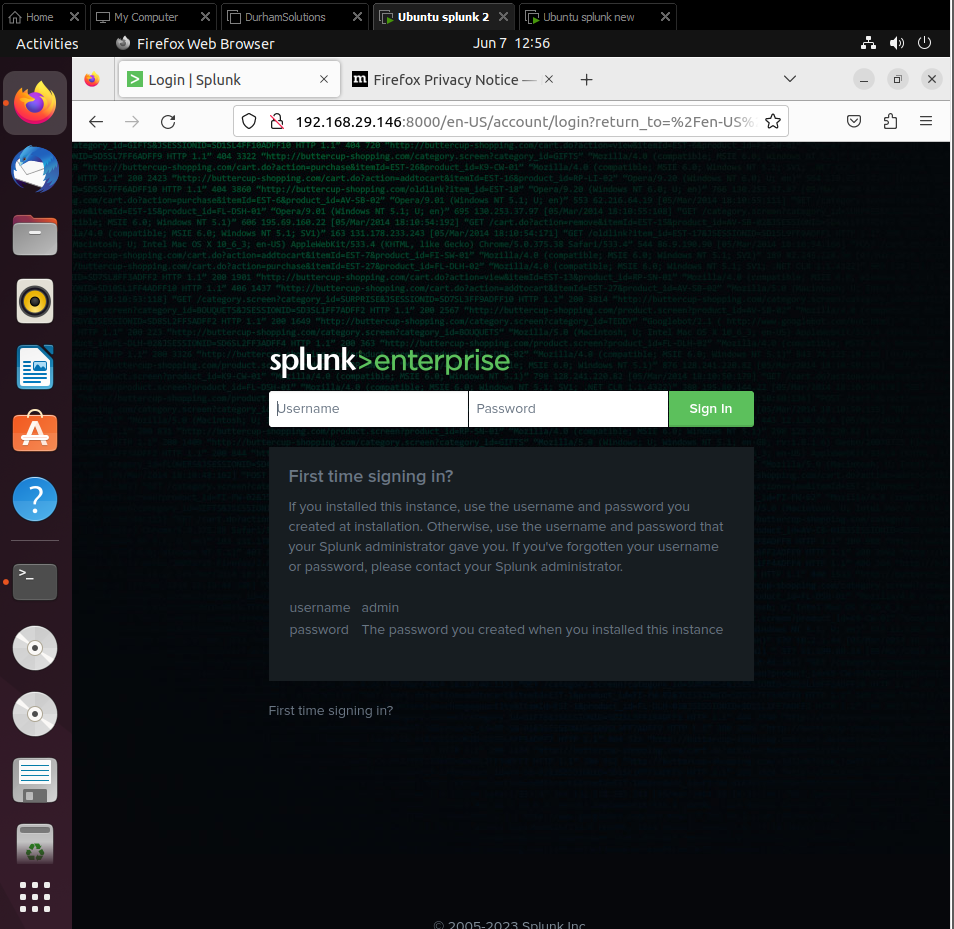
1. Press enter to get to the end of the License agreement and type y (yes) to accept the license
2. Input an administrator username with the format Firstname-NETW2200 and a password you can remember as you won’t be able to access Splunk without this.



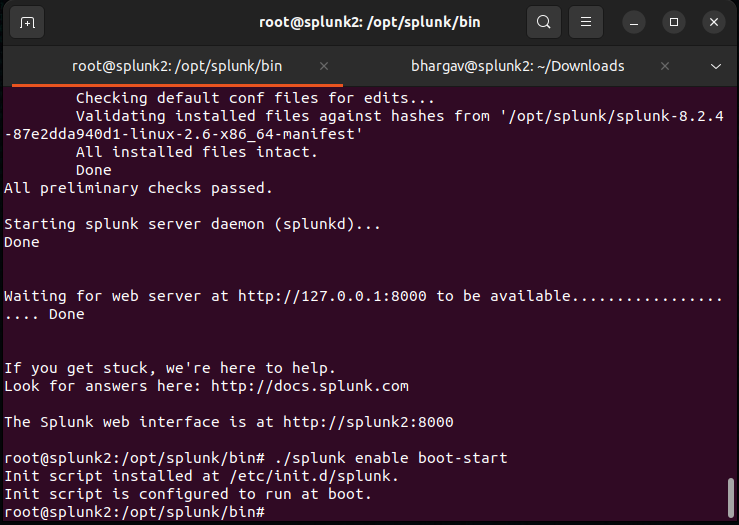
And wait for some time till it’s done installing (Sometimes may work right away and some time may get errors)

1. Splunk should be ready and the web url would be in your command line. Copy the web url and paste on your browser to access Splunk.

Alternatively, Splunk can also be accessed in the browser using the ubuntu Virtual machines IP address routed through port 8000 i.e., 192.168.80.130:8000.

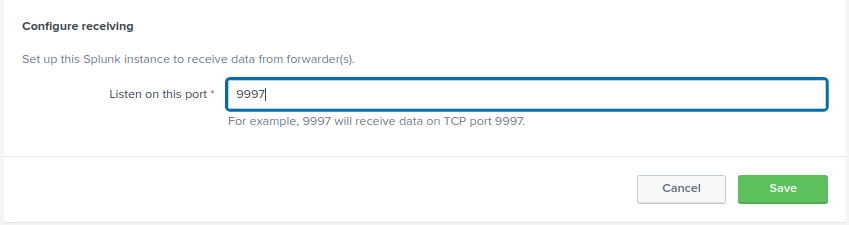


1. Go back to the command line and type the command below to ensure Splunk services starts at any reboot of our virtual machine ./splunk enable boot-start

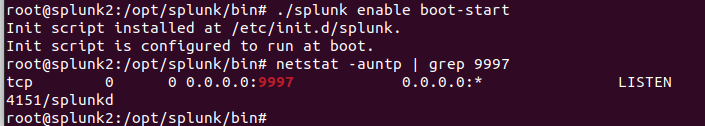


**Step 2: Configuring receiving port at Ubuntu Splunk Server**

1. Go to web interface of Splunk enterprise by using ipaddress:8000. It will ask your administrator username and password for Splunk. Go to settings tab above and click on forwarding and receiving
2. Click on Configure receiving under the Receive data column. Click on new receiving ports
3. Input the default receiving port on TCP port 9997

****

1. Go back to your command line and run the **command netstat -auntp | grep 9997.** This would allow us to see the new configured receiving port we added in previous step.

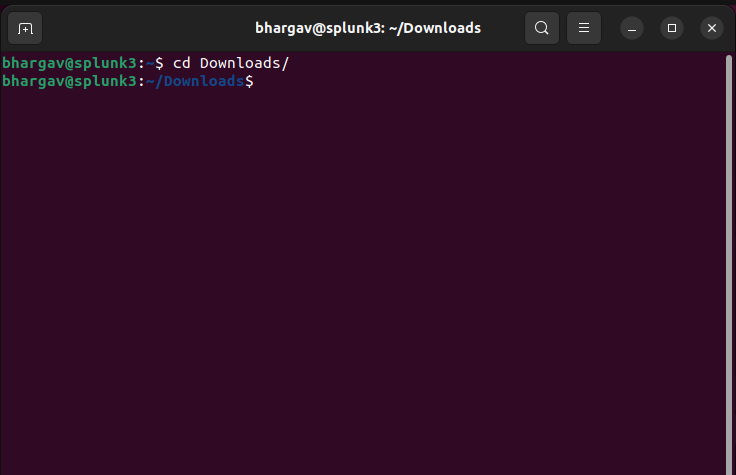


Now our Splunk is listening on the port 9997 for any logs from our universal forwarder. **Congratulations, you have just configured Splunk Ubuntu Server to receive logs now.**

That’s the end of installing Splunk. Next, would be to install our Splunk universal forwarder to forward logs to Splunk.

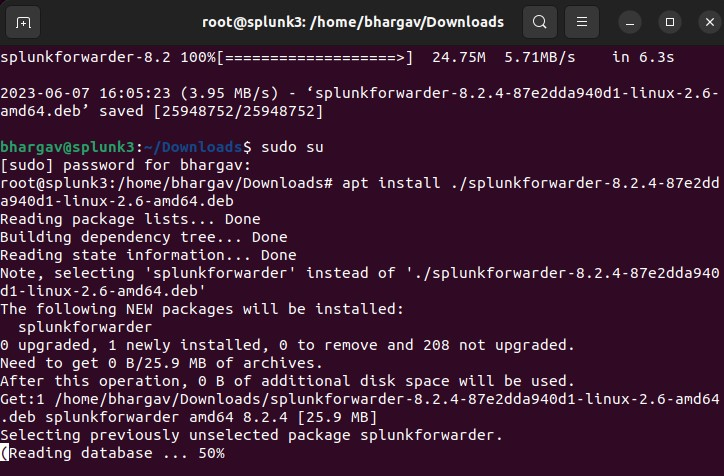
**Step 3: Download and install Splunk Universal Forwarder on second ubuntu machine**

1. Go to your second ubuntu machine you installed, open the terminal window and change to the downloads directory using the command cd Downloads to run the command (I believe you all should know by now what cd (change directory) command means)



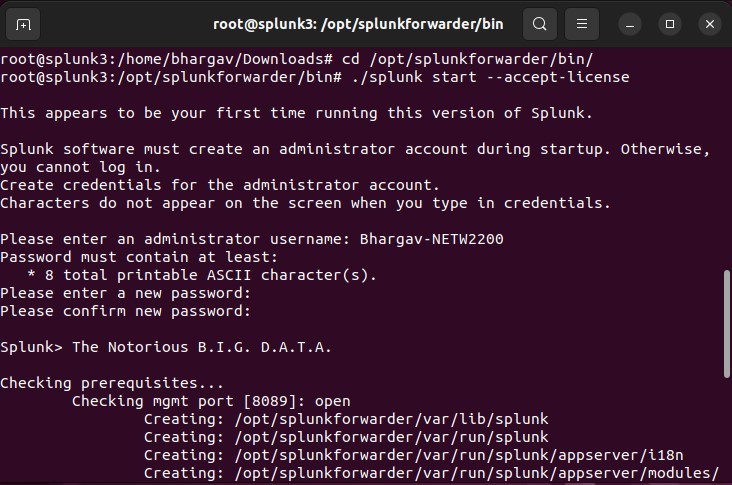
wget -O splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-amd64.deb 'https://download.splunk.com/products/universalforwarder/releases/8.2.4/linux/splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-amd64.deb'

1. Run the command sudo su and input password to change to root user.
2. Install the universal forwarder using the command.

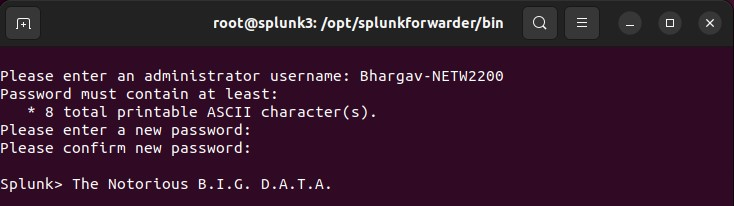


apt install ./splunkforwarder-8.2.4-87e2dda940d1-linux-2.6-amd64.deb

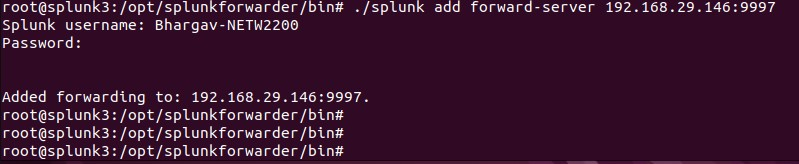
1. Run the command cd /opt/splunkforwarder/bin/ to change to the Splunk forwarder bin directory and start the license using the command ./splunk start --accept-license to accept the license agreement



1. set your forwarders username to firtstname-NETW2200 and input password



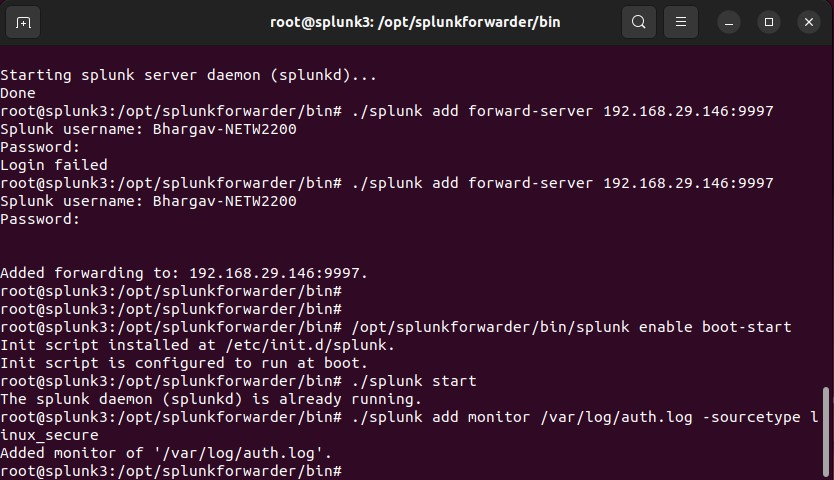
1. Next step would be to add our Splunk’s IP address to our forwarder to forward logs using the command ./splunk add forward-server (your splunk IP-address:port added to splunk to receive logs)   
   e.g. ./splunk add forward-server 192.168.80.130:9997



1. Run the command to enable boot at start

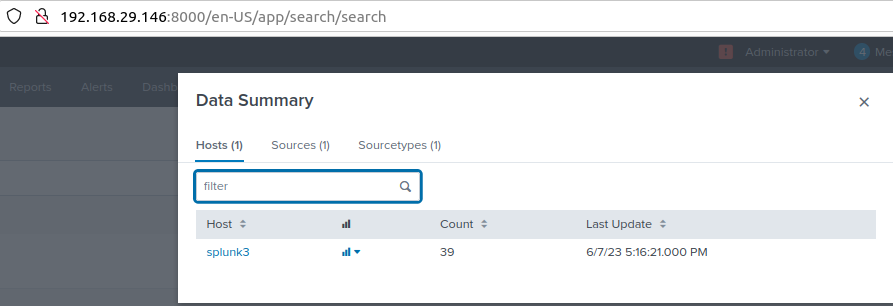
/opt/splunkforwarder/bin/splunk enable boot-start

1. Next would be to run the command ./splunk start on the universal forwarder to make sure we start the service.
2. Next step would be to run the command ./splunk add monitor /var/log/auth.log -sourcetype linux\_secure to send our authentication logs to Splunk (**Note:** This may ask for your Splunk username and password to authenticate

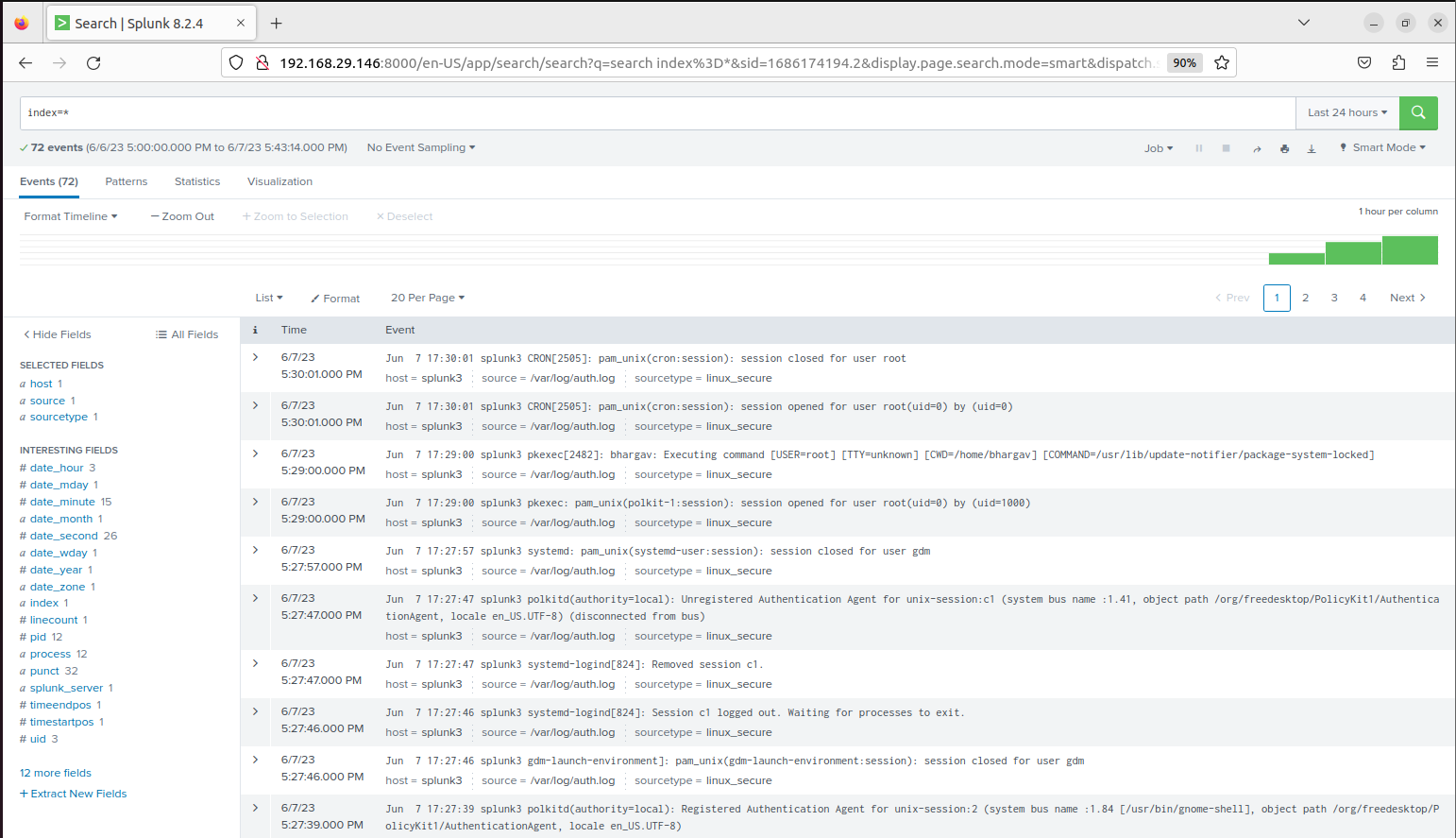


**Step 4: Searching and Reporting App – Capture the logs in Splunk Ubuntu Server**

1. Once we run add-monitor command in previous, the next thing we would do is to wait for few minutes for this to take effect. After few minutes, click on Data summary on the search page of Ubuntu Splunk Server and you would see your authentication logs data has started ingesting into Splunk as seen below. Keep time picker as 24 hours.



1. Now we run the command index=\*, this way we would be able to see some data in our Splunk (To make the most of our free Splunk license in this lab, we'll send only our authentication logs to Splunk for the time being, and we'll explore with more log forwarding in future Labs if we need more detections.)

****

Congratulations, you've just set up Splunk and the Splunk universal forwarder to forward your authentication logs from Ubuntu Linux to the SIEM (Splunk)

Part 2:

We will install openssh-server on our Splunk Forwarder Virtual Machine. After installing this, we would attempt logging in using ssh from a Kali machine using invalid and valid credentials. This Kali attack will be captured by our Splunk Ubuntu Server and would be captured as logs in it.

**Pre-requisites of the lab**

The pre-requisites (recommended system requirement) are:

* Splunk and Splunk forwarder installed
* Kali Virtual Machine (Attacker machine) with following specifications:
  + 4 GHz dual core processor or better
  + 4 GB system memory
  + 80 GB of free hard drive space
  + Internet access is helpful

**Steps of the lab:**

To get our VM up and running, we will need to execute the following steps:

**Step 1:** Download a Kali Image and launch the VM.

**Step 2:** Install openssh-server on second Ubuntu Universal Forwarder machine.

**Step 3:** Login to Kali and Password Spray our Ubuntu Universal Forwarder machine (Victim Machine)- invalid Credentials (RED TEAM)

**Step 4:** Check the attack captured in first Ubuntu Splunk Server Machine.

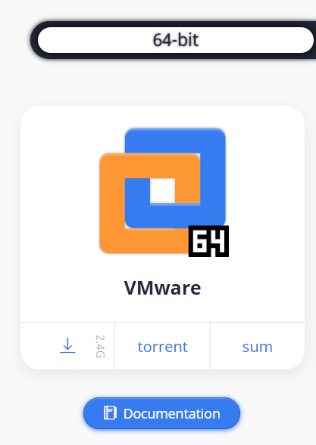
**Step 5:** Brute force attack on second Ubuntu Universal Forwarder machine by Kali machine by using Hydra tool in Kali Linux- Successful attack

**Step** **6:** Check the successful attack logs in your first Ubuntu Splunk server machine

**Execution of the lab**

**Step 1: Download a Kali Image and launch the VM.**

1. Let us download a kali image from kali.org, Use the link below to download kali - <https://kali.download/virtual-images/kali-2021.4a/kali-linux-2021.4a-vmware-amd64.7z>

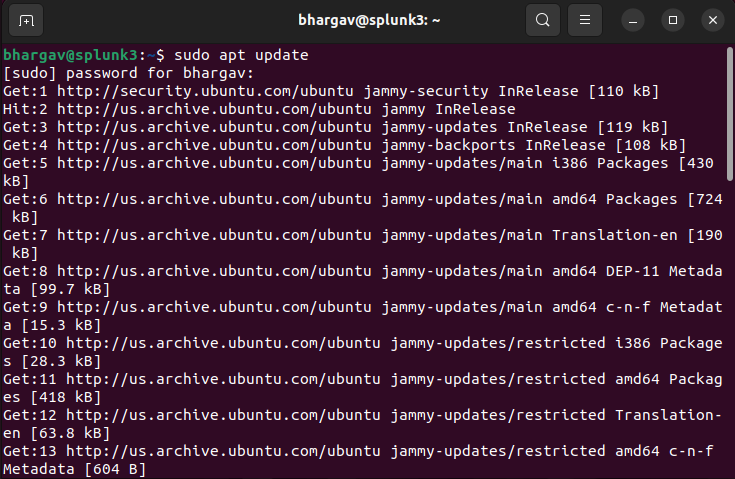
****

1. Unzip your downloaded kali image using 7zip or any other unzipping tool. Go to VMware and click on file -> open. Navigate to your downloaded and unzipped kali to open it and your Kali VM would be created.
2. Power it on, username:kali, password: kali

****

**Step 2: Install openssh-server on Splunk Forwarder Virtual machine.**

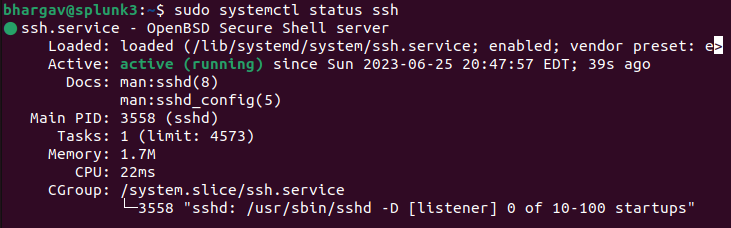
We would download and **enable ssh** on our Splunk Forwarder virtual machine using the following commands

1. First, we would run command to update our vm using **sudo apt update **
2. Next, we run the command to install a ssh server on our ubuntu machine **sudo apt install openssh-server**

**A screenshot of a computer

AI-generated content may be incorrect.**

1. Run the command **sudo systemctl status ssh** to check the status of our ssh server. The status should be green showing running

****

1. To make sure we enable ssh on ubuntu OS firewall just if the vm has one, execute the command **sudo ufw allow ssh**

**A purple background with white text

AI-generated content may be incorrect.**

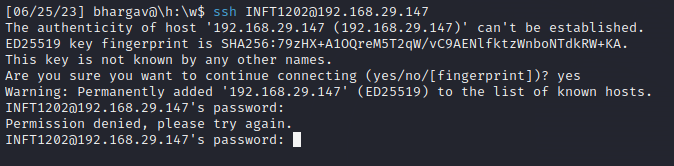
1. Check the IP address of your Ubuntu Universal Forwarder using ifconfig
2. Use the command who to check and confirm your username on your Ubuntu Splunk forwarder.

**Step 3: Login to Kali and Password Spray our Ubuntu Universal Forwarder machine (Victim Machine)- invalid Credentials (RED TEAM)**

Let’s have some fun. Let’s play the attacker here.

1. Try to ssh with a wrong username as seen below using the username INFT1202 and command would be

ssh INFT1202@your\_ubuntu\_UniversalForwarderIP.



1. As the Blue Team, on your Kali machine, run the command ifconfig. This is to confirm our Kali IP, as we would use this IP to check the logs in our first Ubuntu Splunk Server.

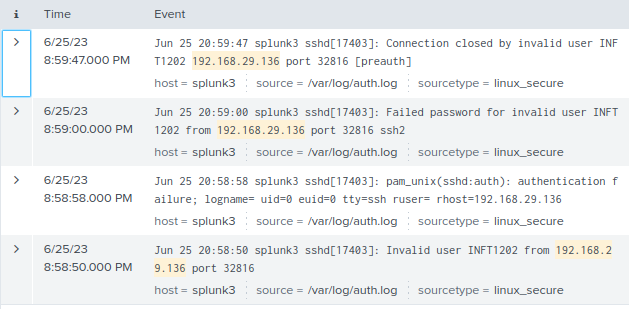
A screen shot of a computer

AI-generated content may be incorrect.

Step 4: Check the attack captured in first Ubuntu Splunk Server Machine.

Next, let us detect the attempted potential access to our Ubuntu machine using a wrong username.

1. Go to the Search and Reporting in Splunk and run the following command: index=\* YourKaliIP e.g., index=\* 192.168.29.136 (my Kali VM). We would see that Splunk shows an invalid user is trying to access our Ubuntu virtual machine using ssh on port 22.



1. You can see, everything got captured in Ubuntu Splunk Server from your kali machine in /var/log/auth.log

Good Job, now as the blue team member, we have detected an attacker is trying to log into our Ubuntu Universal Forwarder using an unidentified credential.

Step 5: Brute force attack on second Ubuntu Universal Forwarder machine by Kali machine by using Hydra tool in Kali Linux- Successful attack

1. Go back to your Kali machine to play the attacker one more time and assume we do not know the password of the Ubuntu Universal Forwarder machine but know the username after doing some Open-Source Intelligence.
2. Let’s create a wordlist using random passwords and **add your Ubuntu Universal Forwarder VM password** to the list (see password list below), in this demo, my ubuntu password was very weak password which was “**Password**”. To create password list, run the command on the terminal of your kali machine.

nano password.txt (This would open a **nano editor** named password.txt)

1. Create a custom Password list by copying and pasting this password list to the opened editor and save it as password.txt.

**Note**: Make sure you add your ubuntu password to the list. This is to make our brute force faster.

PXyFaFexFxopg5k5

wfSTXaZyUTTfVrM9

YYh6nuqDJKgqSPtQ

E8XTUWQo9SMAJ7q6

GBLxJgQRgQiJ4DWC

iY1d1mcFM2KgZ7vr

MRfeALJUiUkAwWwp

nobCWwnNWcuKuzhz

9JmqVSq1V3jtJHxT

Password

Vagrant

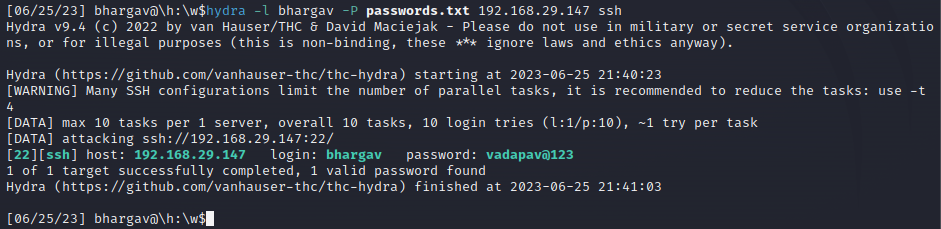
1. When the nano editor opens in your command line, copy the password list, and paste it to the editor and don’t forget to include your correct ubuntu password to the editor (this would make our password spray faster) A computer screen with a white line

   AI-generated content may be incorrect.
2. For nano editor, press ctrl + x and the editor would ask if you wanted to save. Type y(yes) to save our password list.
3. Hope you guys are having some fun, there is still more fun playing the attacker here. Playing as the attacker and as stated earlier, we assume we already know the username of the Ubuntu machine so make sure you check the right username of your ubuntu machine by logging into your Ubuntu Universal forwarder VM. Open the command terminal and execute the command - who

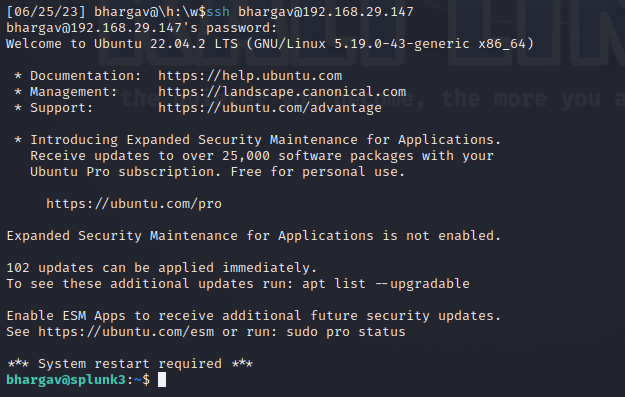
A black background with white text

AI-generated content may be incorrect.

1. After confirming the username of the Ubuntu Universal Forwarder VM, let’s use hydra to password spray the ssh port of our Ubuntu machine using a brute force method and the custom password list. Execute the hydra command: hydra -l [username] -P [password list] [victim machine IP] ssh



Good Job, now we have gotten the victim’s password (our Ubuntu Universal Forwarder VM) using the tool hydra to run a password spray.

1. Playing the attacker, from our Kali VM, we would use the credentials to login to our Ubuntu Universal Forwarder VM through SSH.

# ssh YourUsername@[UbuntuServerVMIP]

# ssh fuadnetw2200@192.168.80.140

Good Job, playing the attacker, you have successfully gained access to the Ubuntu Universal Forwarder VM.

Step 6: Check the successful attack logs in your first Ubuntu Splunk server machine

1. Check the successful attempt logs captured by Ubuntu Splunk Server

A screenshot of a computer

AI-generated content may be incorrect.

1. Screenshot confirming our Ubuntu username and we would see Splunk detected the successful login from the attacker machine