SIEM: Log Monitoring Lab Setup with Splunk

hackingarticles.in/siem-log-monitoring-lab-setup-with-splunk

Raj August 26, 2020

Splunk Inc. is an American public **multinational corporation** based in San Francisco, California, that produces software for searching, monitoring, and analyzing machine-generated big data via a Web-style interface.

Splunk (the product) captures, indexes, and correlates real-time data in a searchable repository from which it can generate graphs, reports, alerts, dashboards, and visualizations.

Table of Content

What is Splunk

Splunk is a software that is used to search, and analyze machine data generated by various CPU running on web or local servers, IoT devices, mobile apps, sensors, or data created by the user. It completes the needs of IT infrastructure by analyzing the logs generated by systems in various processes in a structured or semi-structured format with proper data modelling and then it allows users to create Reports, Alerts, Tags, and Dashboards on these data.

Splunk Features

Data searching: – searching in Splunk involves the pattern of creating metrics or indexes on Dashboards.

Data ingestion: – Splunk ingest data in various formats like XML, JSON, and unstructured machine data such as logs of CPU running on web servers.

Data Indexing: – Splunk auto index the ingested data of various machines for the faster searching on various conditions

Alerts: – Splunk alert used for triggering emails or other feeds when some unusual suspicious activity found in data is being analysed**.**

Dashboards: – it shows the search results in the form of pivots, area mapping, pie charts, reports, etc**.**

Splunk Architecture

There are three main components of Splunk: –

- Splunk Forwarder
- Splunk Indexer
- Splunk Head

Prerequisites

To configure Splunk in your Ubuntu platform, there are some prerequisites required for installation.

- Ubuntu 20.04.1 with minimum 4GB RAM and 2 CPU
- SSH Access with Root Privileges
- Firewall Port: – 8000

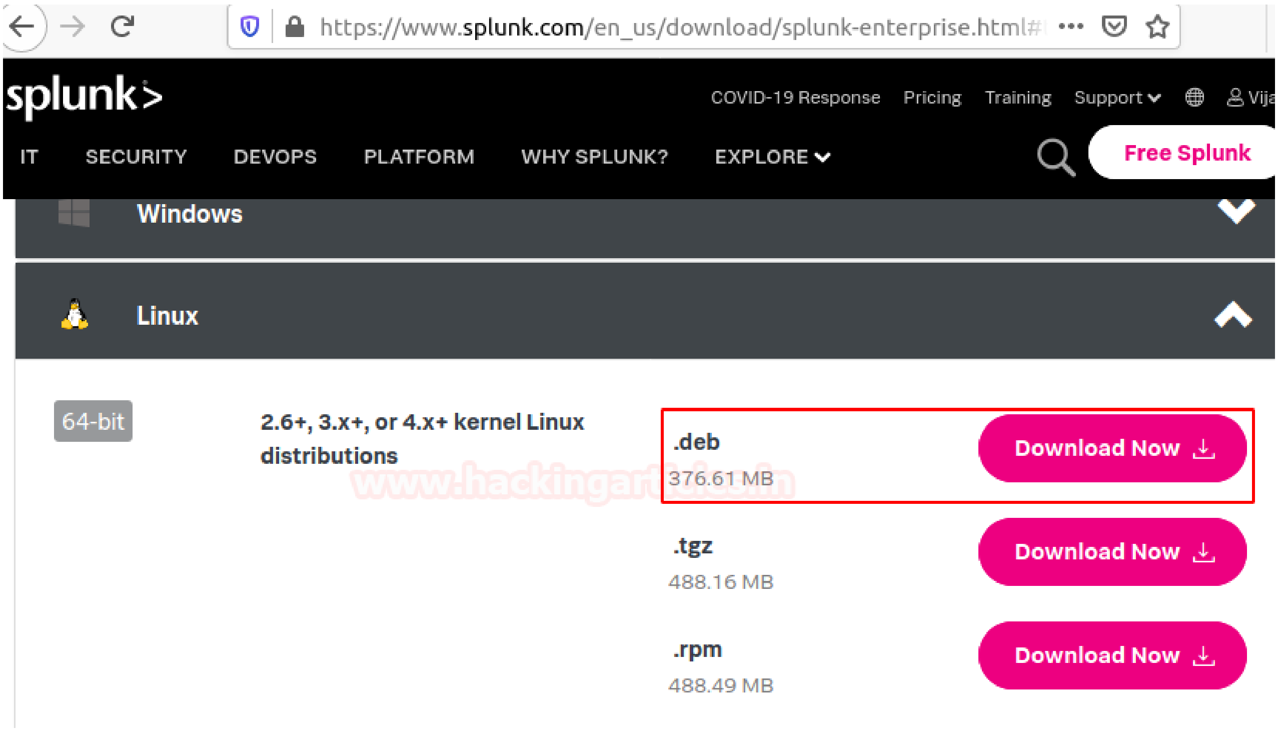
Splunk Environment

In this blog, we will target to install an enterprise version that is available free for 60 days with all features enabled. You can download Splunk by following the below link.

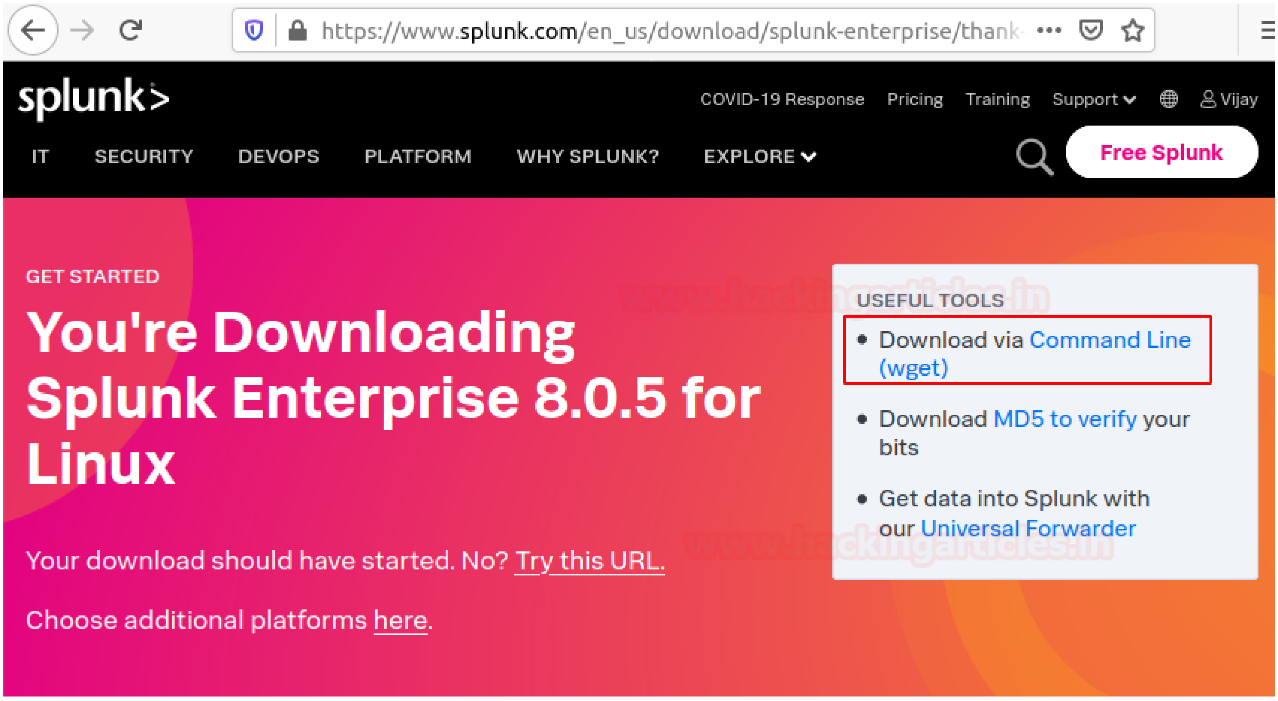
```
https://www.splunk.com/en_us/download/splunk-enterprise.html
```

Linux version

Create a Splunk Account and download Splunk for Linux version by the given above link. We choose **.deb** Package for the installation in Ubuntu.



We can directly install it via terminal by copying **wget** snippet



GET STARTED

You're Downloading Splunk Enterprise 8.0.5 for Linux

Your download should have started. No? Try this URL.

Choose additional platforms here.

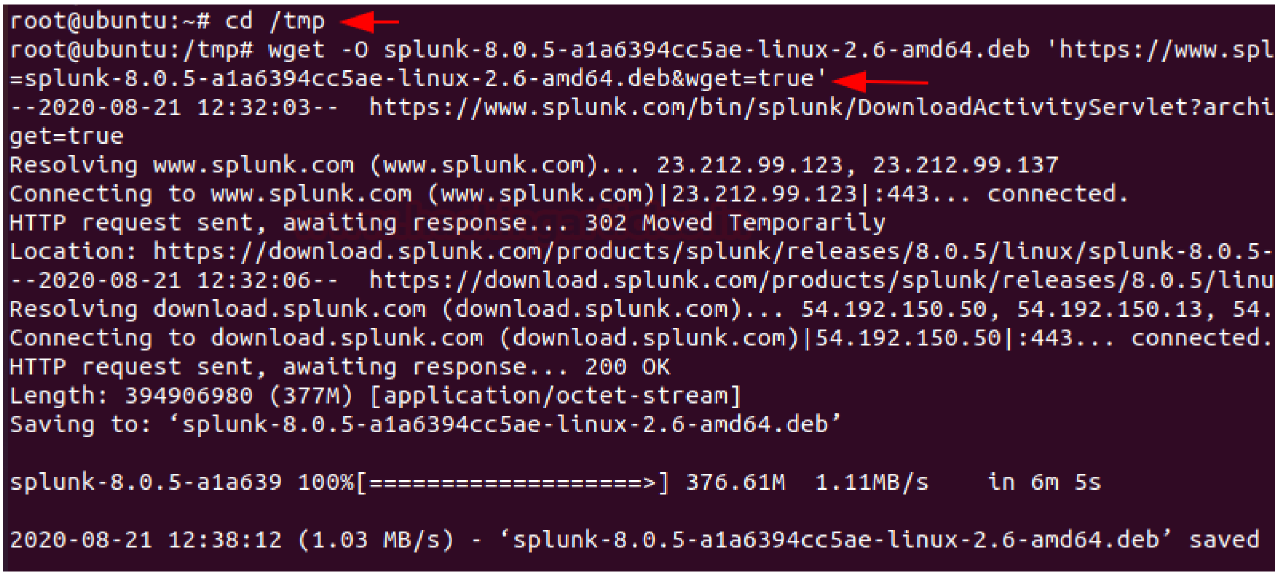
USEFUL TOOLS

- Download via Command Line (wget)
- Download MD5 to verify your bits
- Get data into Splunk with our Universal Forwarder

Download and install Splunk

Now, Hit the terminal and download the Splunk into the tmp directory by entering the following command.

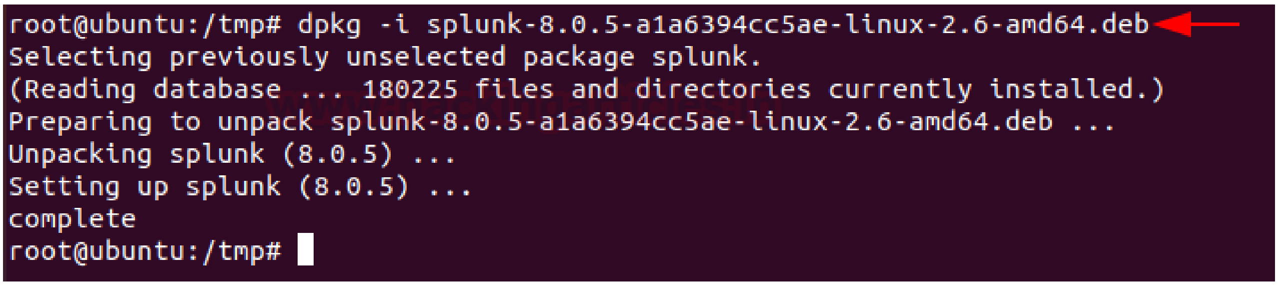
```
cd /tmp
wget -O splunk-8.0.5-a1a6394cc5ae-linux-2.6-amd64.deb
'https://www.splunk.com/bin/splunk/DownloadActivityServlet?
architecture=x86_64&platform=linux&version=8.0.5&product=splunk&filename=splunk-
8.0.5-a1a6394cc5ae-linux-2.6-amd64.deb&wget=true'
```



```
root@ubuntu:~# cd /tmp
root@ubuntu:/tmp# wget -O splunk-8.0.5-a1a6394cc5ae-linux-2.6-amd64.deb 'https://www.spl
=splunk-8.0.5-a1a6394cc5ae-linux-2.6-amd64.deb&wget=true'
--2020-08-21 12:32:03--  https://www.splunk.com/bin/splunk/DownloadActivityServlet?archi
get=true
Resolving www.splunk.com (www.splunk.com)... 23.212.99.123, 23.212.99.137
Connecting to www.splunk.com (www.splunk.com)|23.212.99.123|:443... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: https://download.splunk.com/products/splunk/releases/8.0.5/linux/splunk-8.0.5-
--2020-08-21 12:32:06--  https://download.splunk.com/products/splunk/releases/8.0.5/linu
Resolving download.splunk.com (download.splunk.com)... 54.192.150.50, 54.192.150.13, 54.
Connecting to download.splunk.com (download.splunk.com)|54.192.150.50|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 394906980 (377M) [application/octet-stream]
Saving to: ‘splunk-8.0.5-a1a6394cc5ae-linux-2.6-amd64.deb’

splunk-8.0.5-a1a639 100%[===================>] 376.61M  1.11MB/s    in 6m 5s

2020-08-21 12:38:12 (1.03 MB/s) - ‘splunk-8.0.5-a1a6394cc5ae-linux-2.6-amd64.deb’ saved
```

Next, we run the dpkg command to extract and install the Splunk server. To extract .deb package enter the following command

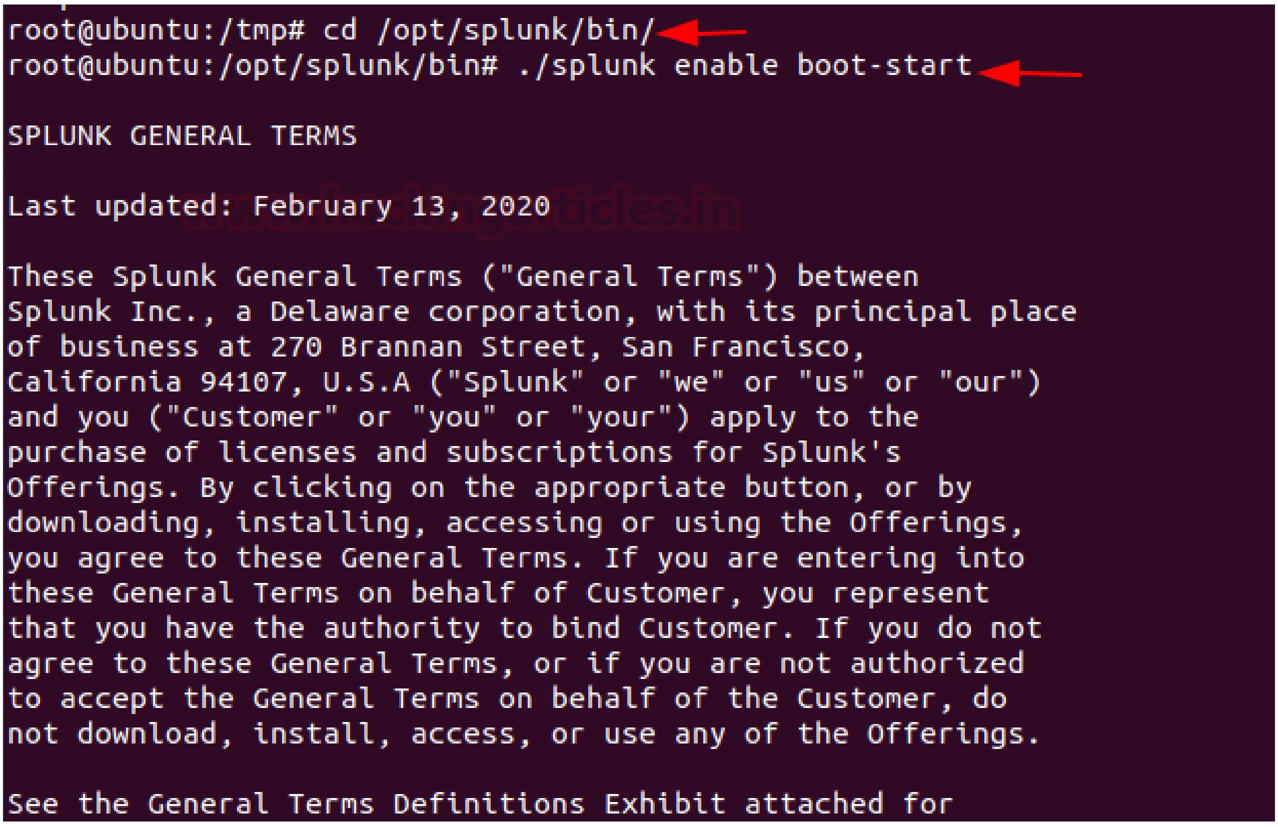
```
dpkg -i splunk-8.0.5-a1a6394cc5ae-linux-2.6-amd64.deb
```



```
root@ubuntu:/tmp# dpkg -i splunk-8.0.5-a1a6394cc5ae-linux-2.6-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 180225 files and directories currently installed.)
Preparing to unpack splunk-8.0.5-a1a6394cc5ae-linux-2.6-amd64.deb ...
Unpacking splunk (8.0.5) ...
Setting up splunk (8.0.5) ...
complete
root@ubuntu:/tmp# 
```

Secondly, we need to create the init.d script so we can easily start or stop Splunk service. Change your binary directory at /opt/splunk/bin/ and run the following command to start the Splunk with system boot.

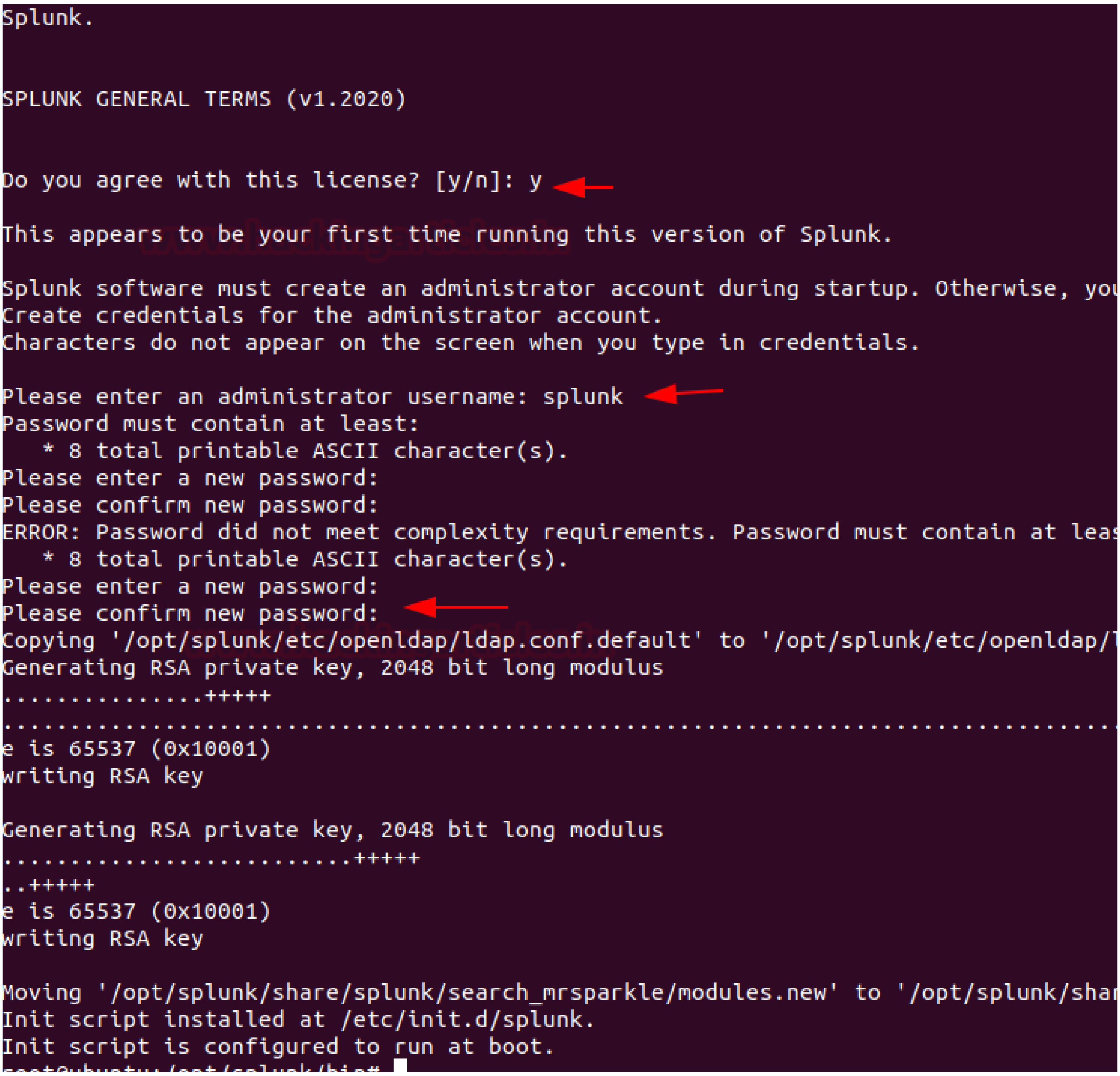
```
cd /opt/splunk/bin/
./splunk enable boot-start
```



```
root@ubuntu:/tmp# cd /opt/splunk/bin/
root@ubuntu:/opt/splunk/bin# ./splunk enable boot-start

SPLUNK GENERAL TERMS

Last updated: February 13, 2020

These Splunk General Terms ("General Terms") between
Splunk Inc., a Delaware corporation, with its principal place
of business at 270 Brannan Street, San Francisco,
California 94107, U.S.A ("Splunk" or "we" or "us" or "our")
and you ("Customer" or "you" or "your") apply to the
purchase of licenses and subscriptions for Splunk's
Offerings. By clicking on the appropriate button, or by
downloading, installing, accessing or using the Offerings,
you agree to these General Terms. If you are entering into
these General Terms on behalf of Customer, you represent
that you have the authority to bind Customer. If you do not
agree to these General Terms, or if you are not authorized
to accept the General Terms on behalf of the Customer, do
not download, install, access, or use any of the Offerings.

See the General Terms Definitions Exhibit attached for
```

During this process press the spacebar to go through the license agreement and then type **"Y"** to accept it and then provide the username and password that you created on the official website of Splunk. Finally, we can start Splunk service with the below argument.

```
service splunk start
```

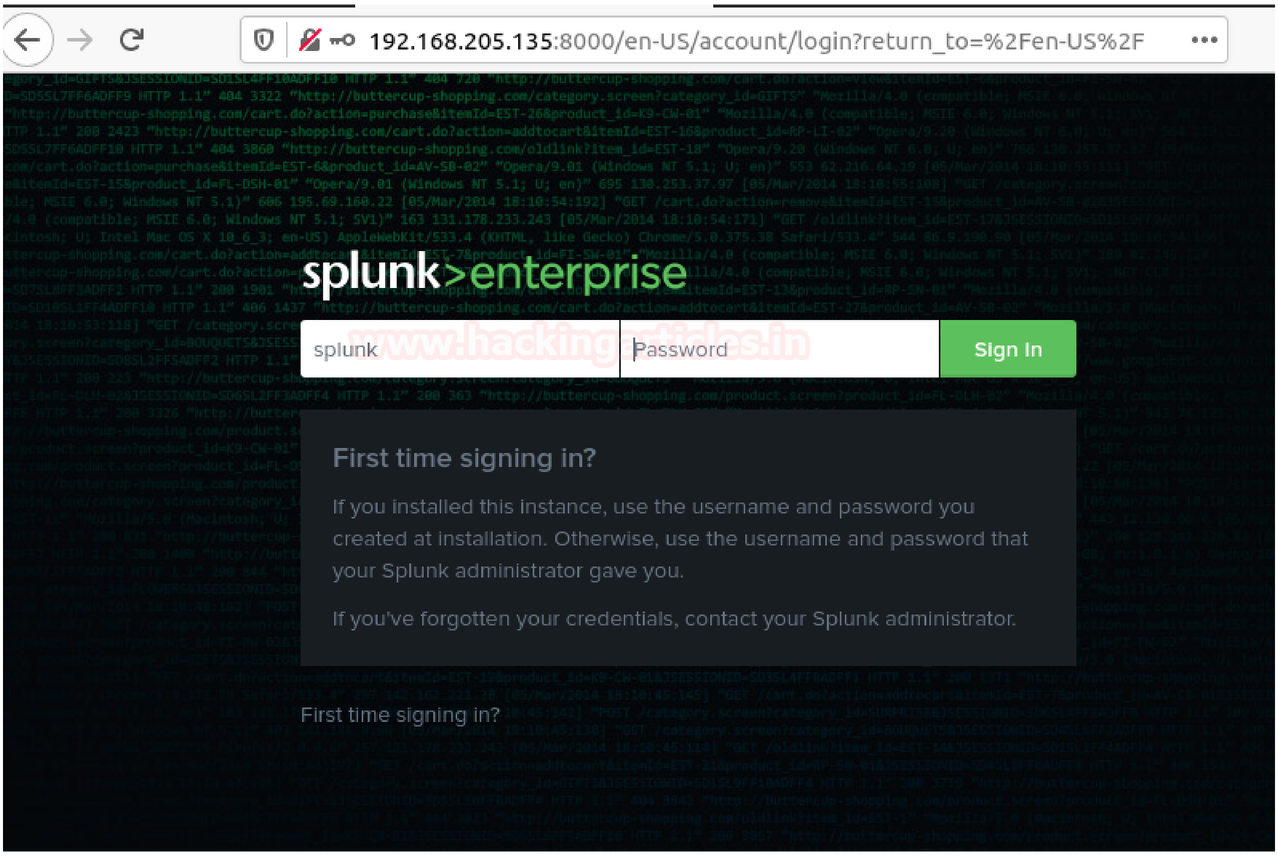


```
Splunk.


SPLUNK GENERAL TERMS (v1.2020)


Do you agree with this license? [y/n]: y

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: splunk
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
ERROR: Password did not meet complexity requirements. Password must contain at leas
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Copying '/opt/splunk/etc/openldap/ldap.conf.default' to '/opt/splunk/etc/openldap/l
Generating RSA private key, 2048 bit long modulus
...............+++++
.............................................................................
e is 65537 (0x10001)
writing RSA key

Generating RSA private key, 2048 bit long modulus
..........................+++++
..+++++
e is 65537 (0x10001)
writing RSA key

Moving '/opt/splunk/share/splunk/search_mrsparkle/modules.new' to '/opt/splunk/shar
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
root@ubuntu:/opt/splunk/bin#
```

Now, you need to make sure port 8000 is open on your server firewall and then you can access Splunk on web interface at

```
http://server-Ip:8000/
http://server-hostname:8000
```

And then, enter the login credentials that you created during the installation process to access the GUI interface. Once you logged in then you will have your Splunk Dashboard ready to set fire on the logs .



192.168.205.135:8000/en-US/account/login?return_to=%2Fen-US%2F

splunk>enterprise

First time signing in?

If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you.

If you've forgotten your credentials, contact your Splunk administrator.

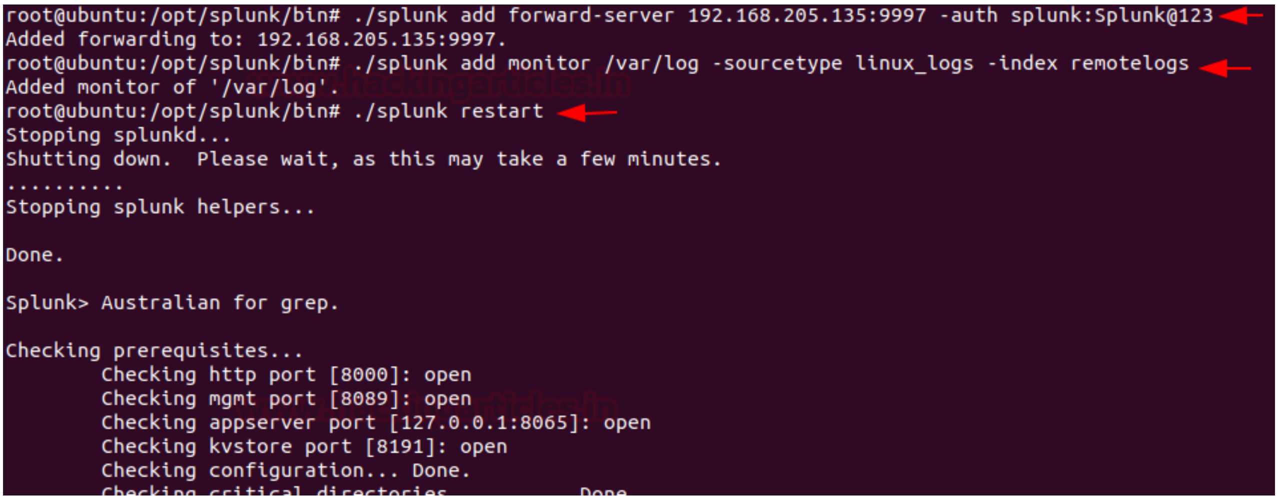
First time signing in?

Adding a task

On the Splunk web interface, there are various categories listed over on the homepage you can choose your own to start Splunking. I'm adding an example for a task which is been added to the Splunk system. My task is to add or forward system logs to Splunk dashboard.

To forward logs to Splunk monitoring console just open the terminal and hit the following commands in the Splunk installed directory with the below arguments.

```
cd /opt/splunk/bin
./splunk add forward-server 192.168.205.135:9997 -auth splunk:Splunk@123
./splunk add monitor /var/log -sourcetype linux_logs -index remotelogs
./splunk restart
```



```
root@ubuntu:/opt/splunk/bin# ./splunk add forward-server 192.168.205.135:9997 -auth splunk:Splunk@123
Added forwarding to: 192.168.205.135:9997.
root@ubuntu:/opt/splunk/bin# ./splunk add monitor /var/log -sourcetype linux_logs -index remotelogs
Added monitor of '/var/log'.
root@ubuntu:/opt/splunk/bin# ./splunk restart
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
..........
Stopping splunk helpers...

Done.

Splunk> Australian for grep.

Checking prerequisites...
        Checking http port [8000]: open
        Checking mgmt port [8089]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration... Done.
        Checking critical directories...          Done
```

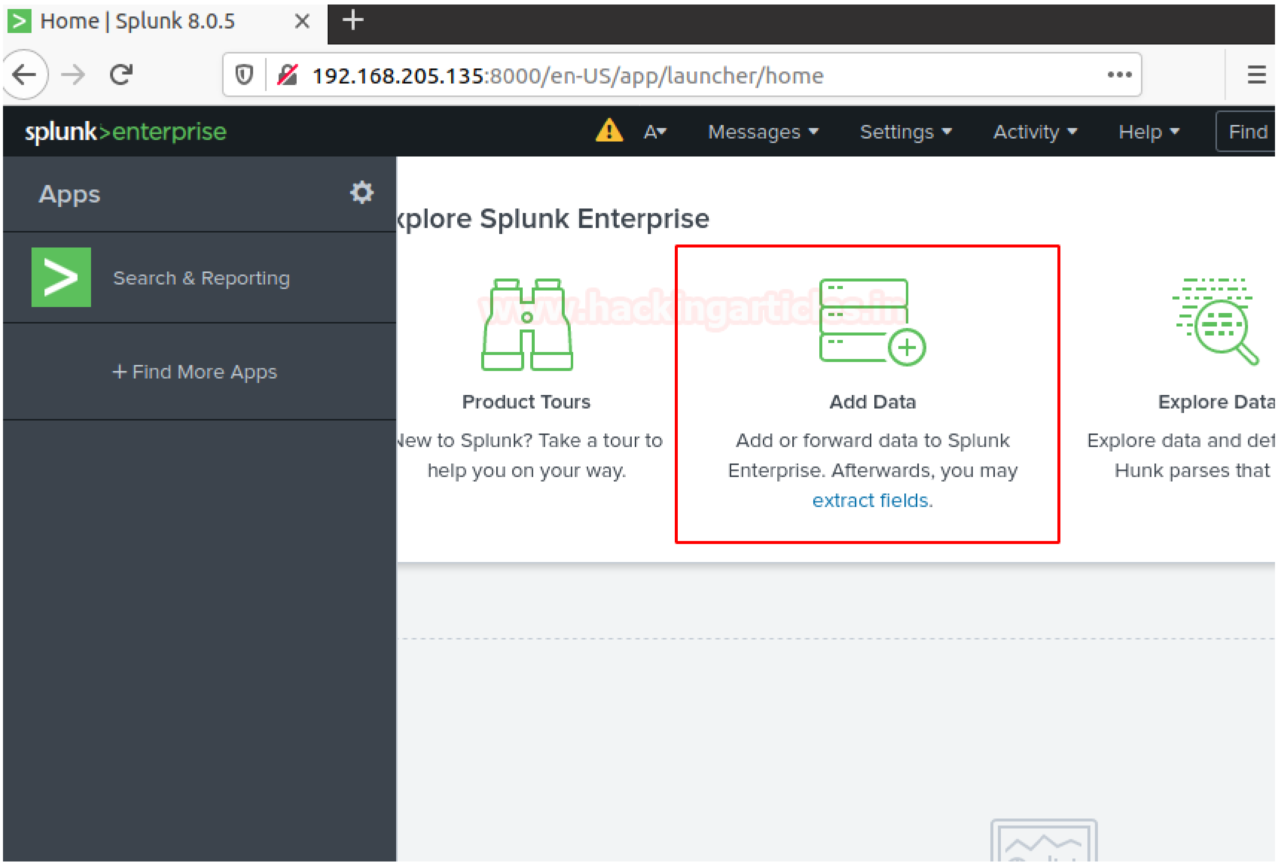
And then open Splunk search and reporting console and then run a query in the search bar.

```
index=remotelogs * host-ubuntu
```

You can also directly add this task by your Splunk Dashboard by following the below steps.

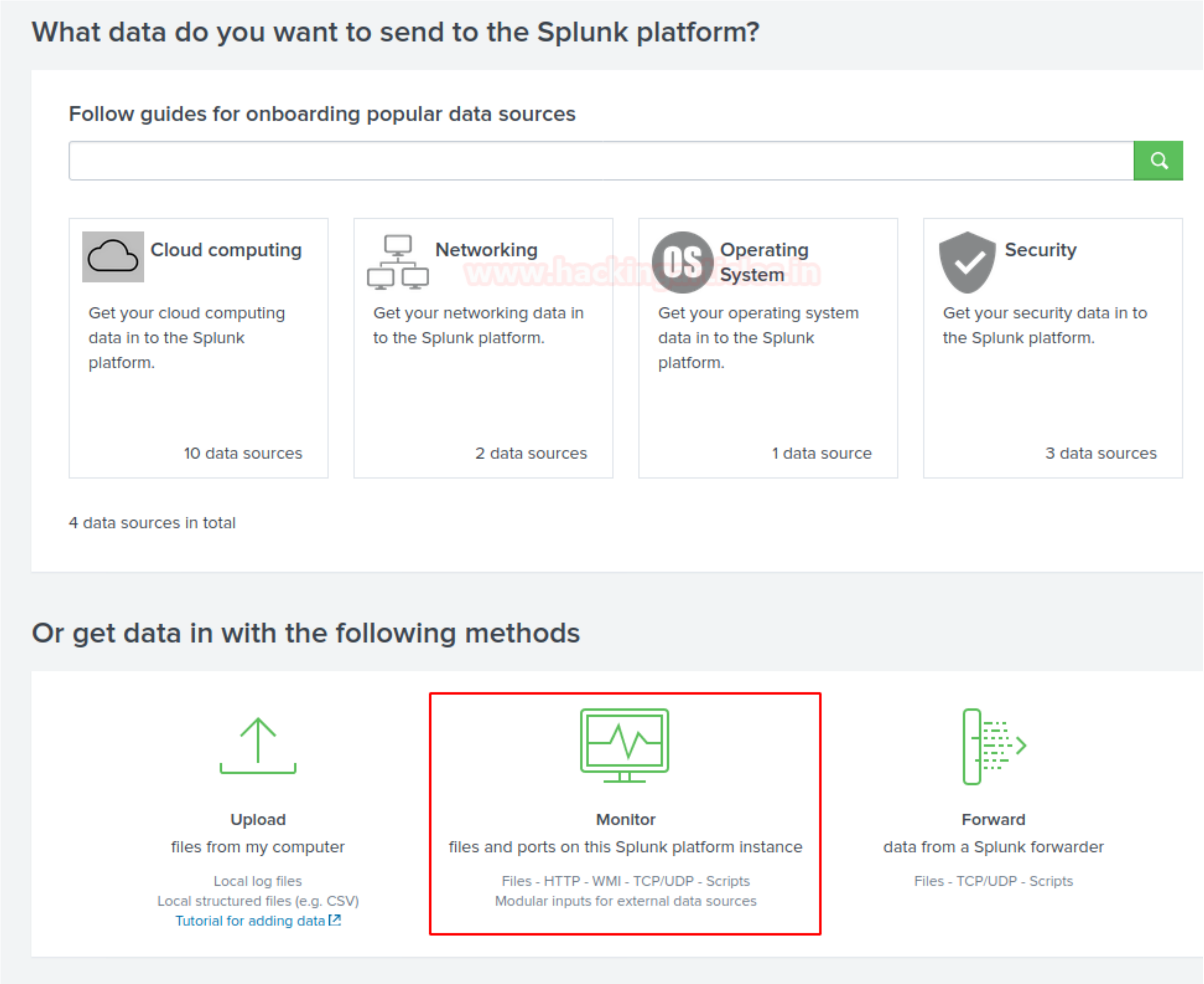
Step 1.

Fire up the Splunk web interface on your favourite browser and choose the **“Add Data”** option to start with.



Step 2.

The **“Add Data”** opens up with three options: Upload, Monitor, and Forward each option have self-explanatory with a short description. Our task is to monitor system logs we go with the option of **“Monitor”.**



What data do you want to send to the Splunk platform?

Follow guides for onboarding popular data sources

Cloud computing	Networking	Operating System	Security
Get your cloud computing data in to the Splunk platform.	Get your networking data in to the Splunk platform.	Get your operating system data in to the Splunk platform.	Get your security data in to the Splunk platform.
10 data sources	2 data sources	1 data source	3 data sources

4 data sources in total

Or get data in with the following methods

Upload
files from my computer
Local log files
Local structured files (e.g. CSV)
Tutorial for adding data

Monitor
files and ports on this Splunk platform instance
Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

Forward
data from a Splunk forwarder
Files - TCP/UDP - Scripts

In the monitor option, there are four categories as shown below

Files & Directories: To monitor files and folders

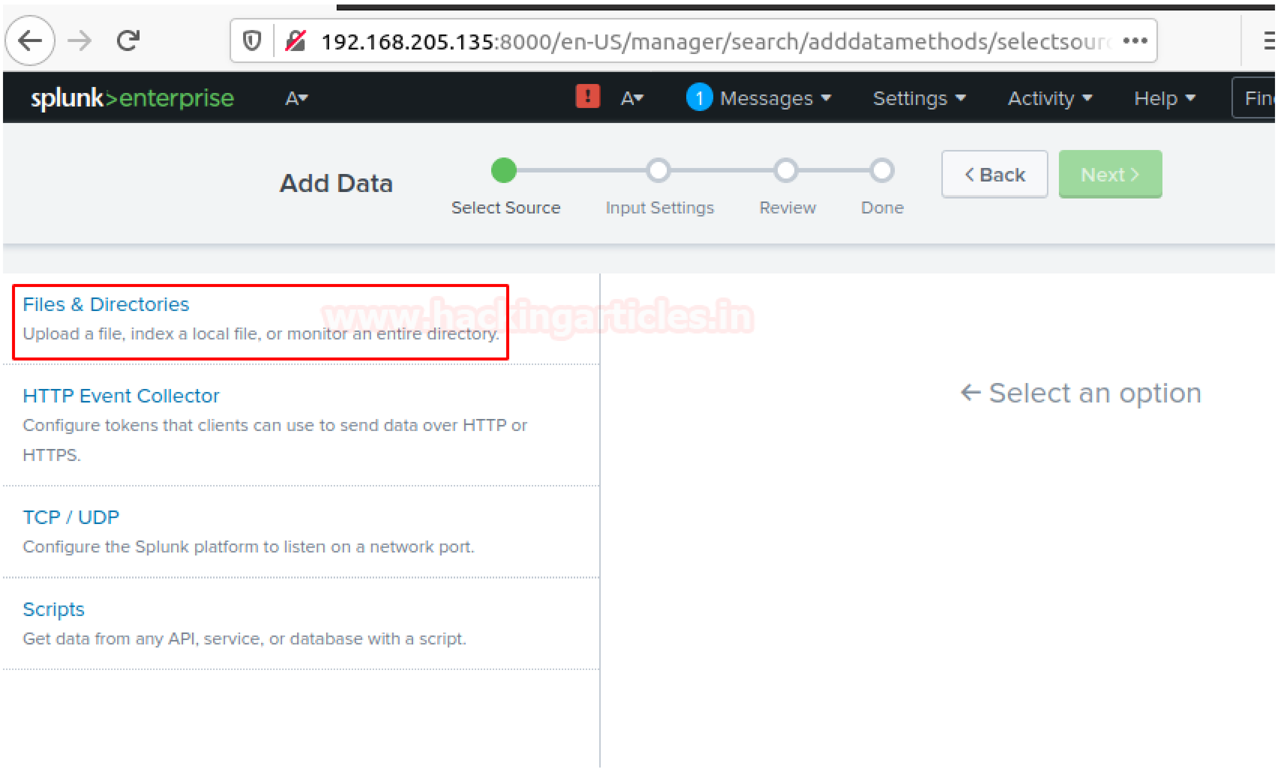
HTTP Event Collector: To Monitor Data streaming over HTTP

TCP/UDP: To monitor network Traffic over TCP/UDP ports

Scripts: To monitor Scripts and commands

Step 3.

As per our purpose we choose and go with the “**Files & Directories”** option.



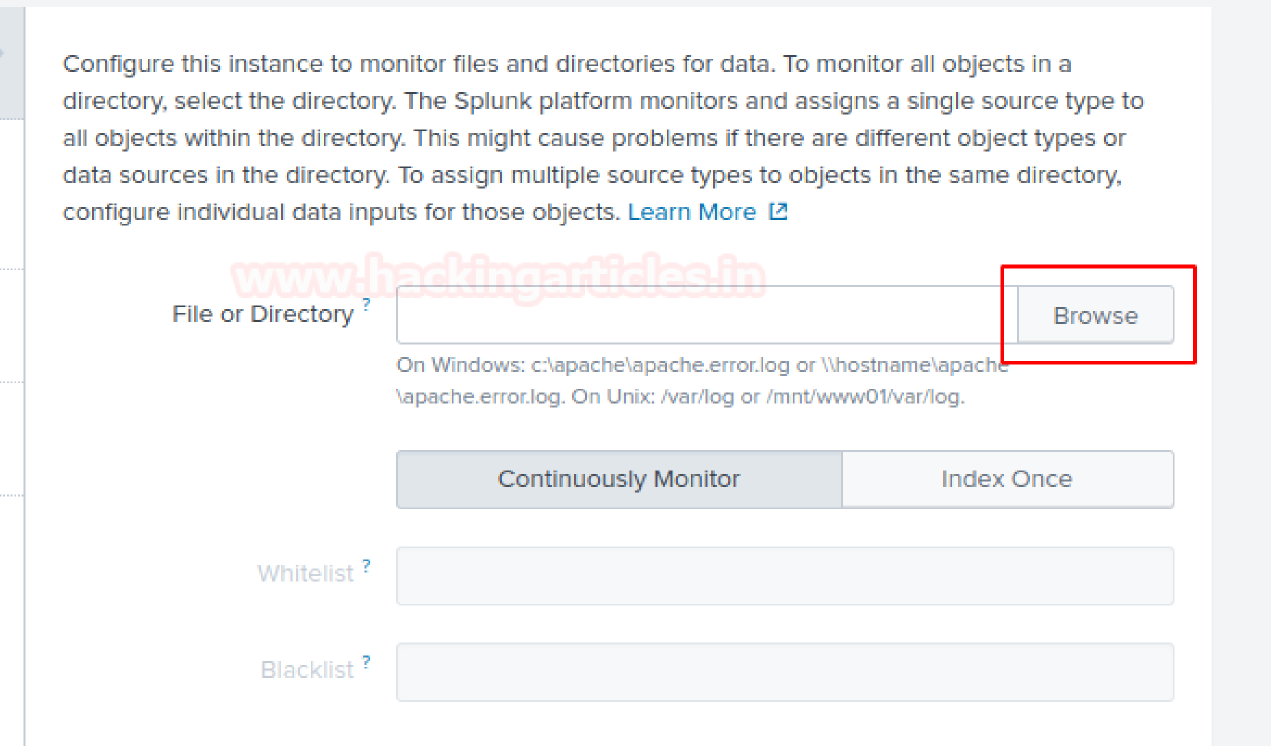
Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

And then we are going to browse the path where system logs are stored.



Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. Learn More

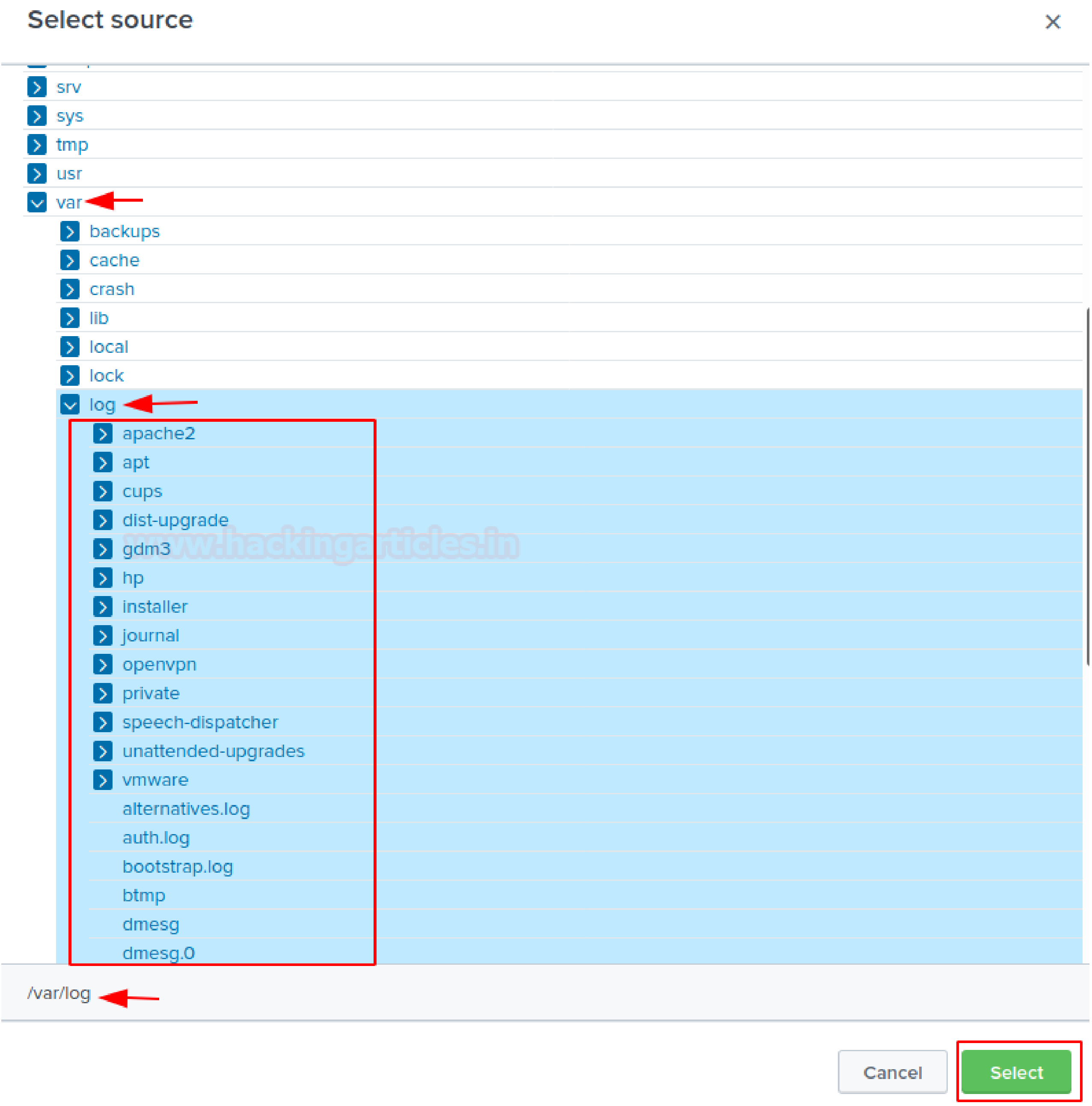
File or Directory ?

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

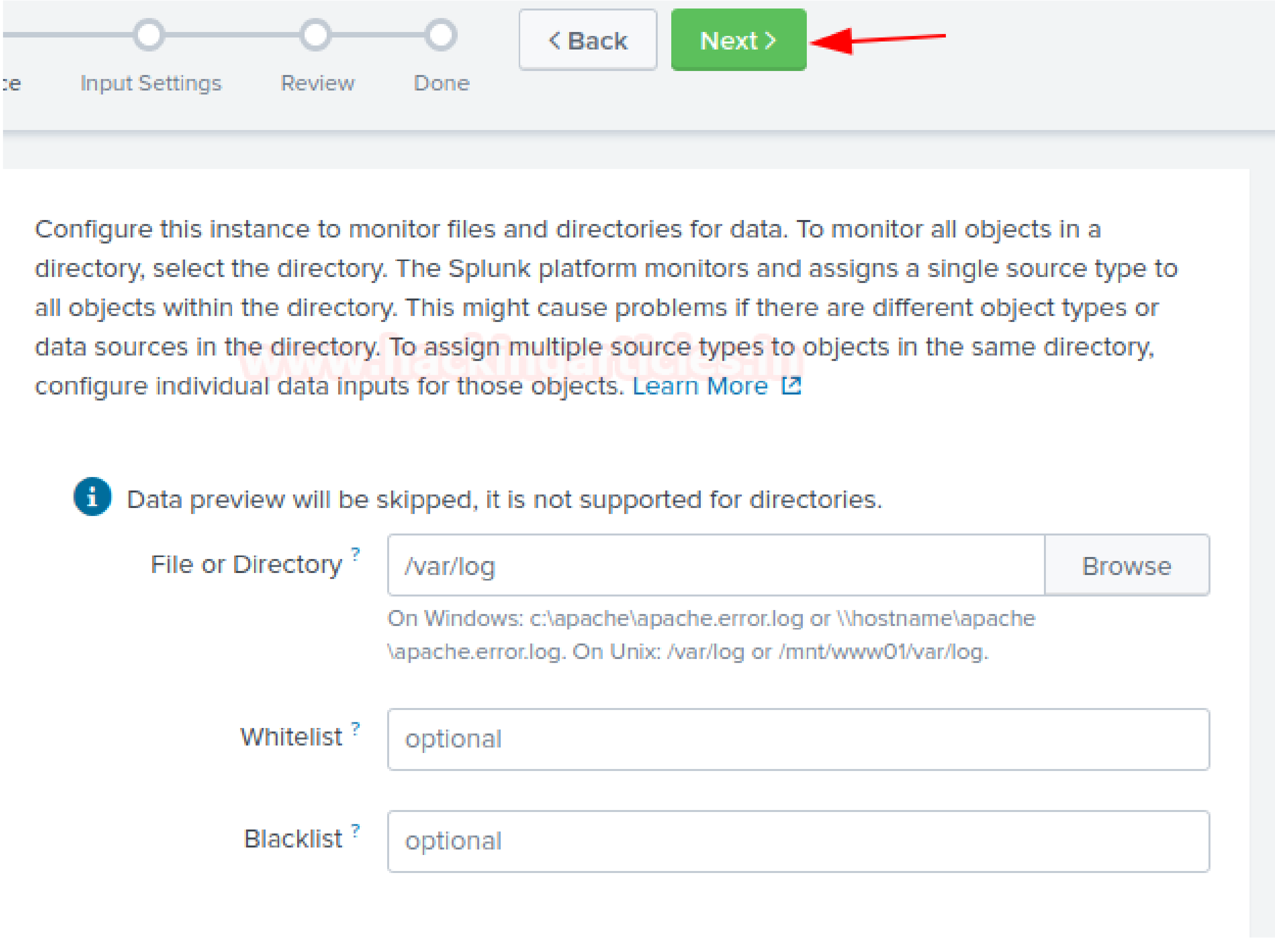
Whitelist ?

Blacklist ?

Now, we’re going to browse the exact path **/var/log** that’s from the server to monitor. Once you had done then select the next option.



After selecting the system files to monitor select the next option.



Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. Learn More

Data preview will be skipped, it is not supported for directories.

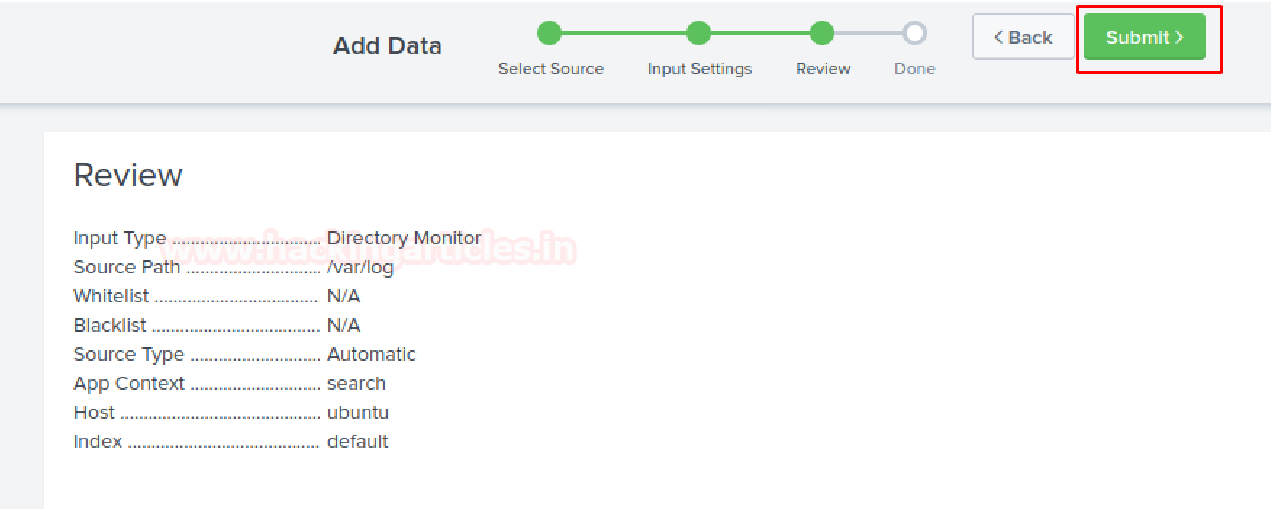
File or Directory ? /var/log Browse

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Whitelist ? optional

Blacklist ? optional

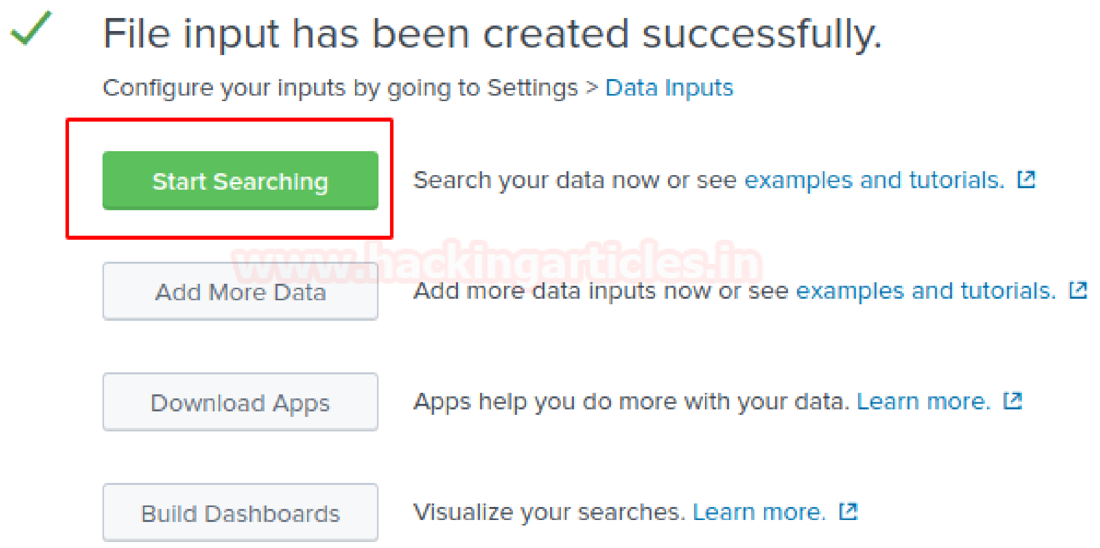
Also, you can whitelist or blacklist specific directories that you don't want to monitor on a given dialogue box and then review your settings and hit submit button.



Review

```
Input Type .............................. Directory Monitor
Source Path ............................ /var/log
Whitelist ................................. N/A
Blacklist ................................. N/A
Source Type ............................ Automatic
App Context ............................ search
Host ........................................ ubuntu
Index ....................................... default
```

Congrats! Finally, you have successfully added the task to the **Search & Reporting** console now **Start Searching**.



File input has been created successfully.

Configure your inputs by going to Settings > Data Inputs

Search your data now or see examples and tutorials.

Add more data inputs now or see examples and tutorials.

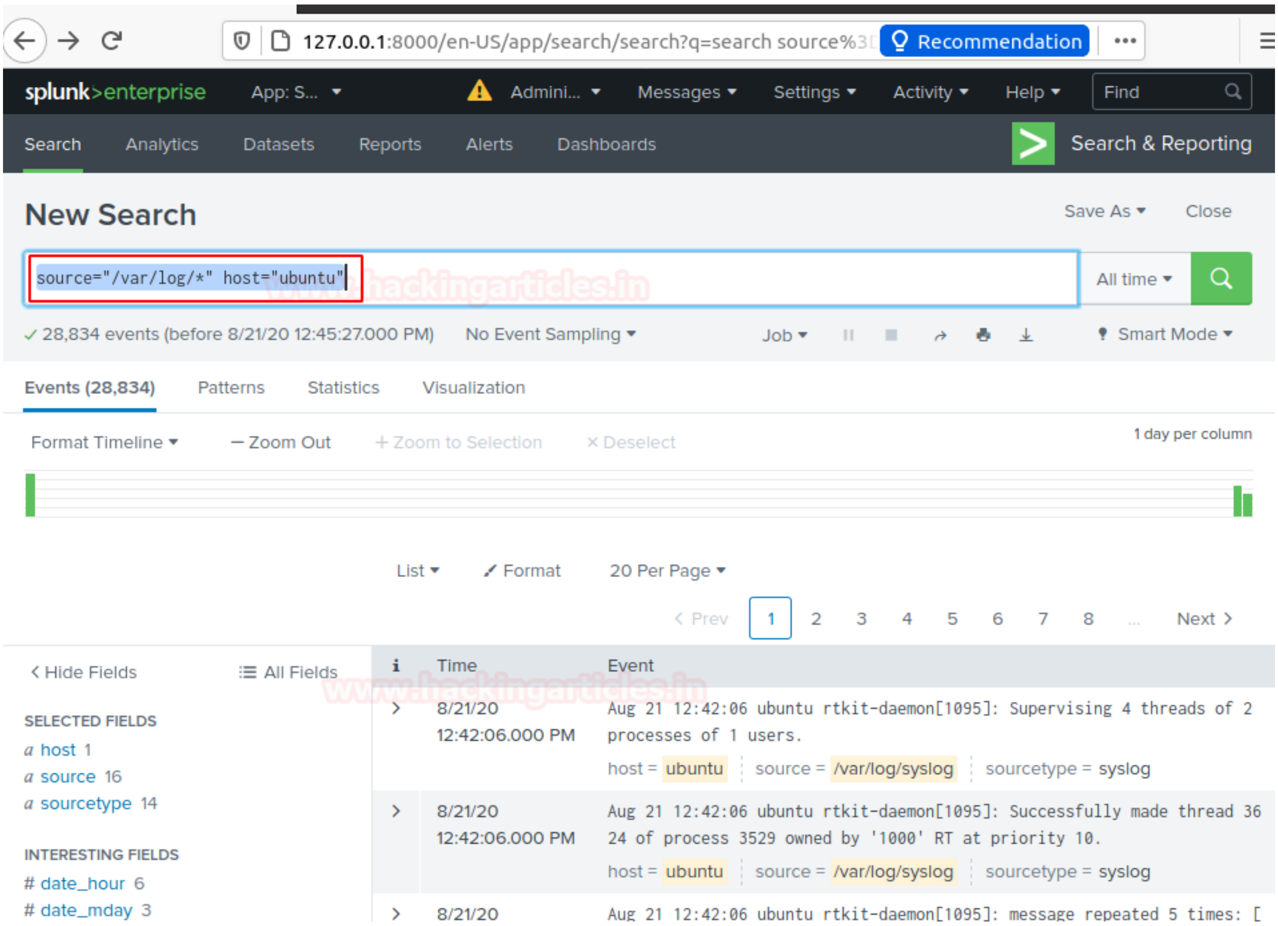
Apps help you do more with your data. Learn more.

Visualize your searches. Learn more.

Step 4.

Now you've successfully added data source to Splunk for monitoring. You can search and monitor logs file as required just run the search query

```
source="/var/log/*" host="ubuntu"
```



```
source="/var/log/*" host="ubuntu"
```

i	Time	Event
›	8/21/20 12:42:06.000 PM	Aug 21 12:42:06 ubuntu rtkit-daemon[1095]: Supervising 4 threads of 2 processes of 1 users. host = ubuntu source = /var/log/syslog sourcetype = syslog
›	8/21/20 12:42:06.000 PM	Aug 21 12:42:06 ubuntu rtkit-daemon[1095]: Successfully made thread 36 24 of process 3529 owned by '1000' RT at priority 10. host = ubuntu source = /var/log/syslog sourcetype = syslog
›	8/21/20	Aug 21 12:42:06 ubuntu rtkit-daemon[1095]: message repeated 5 times: [

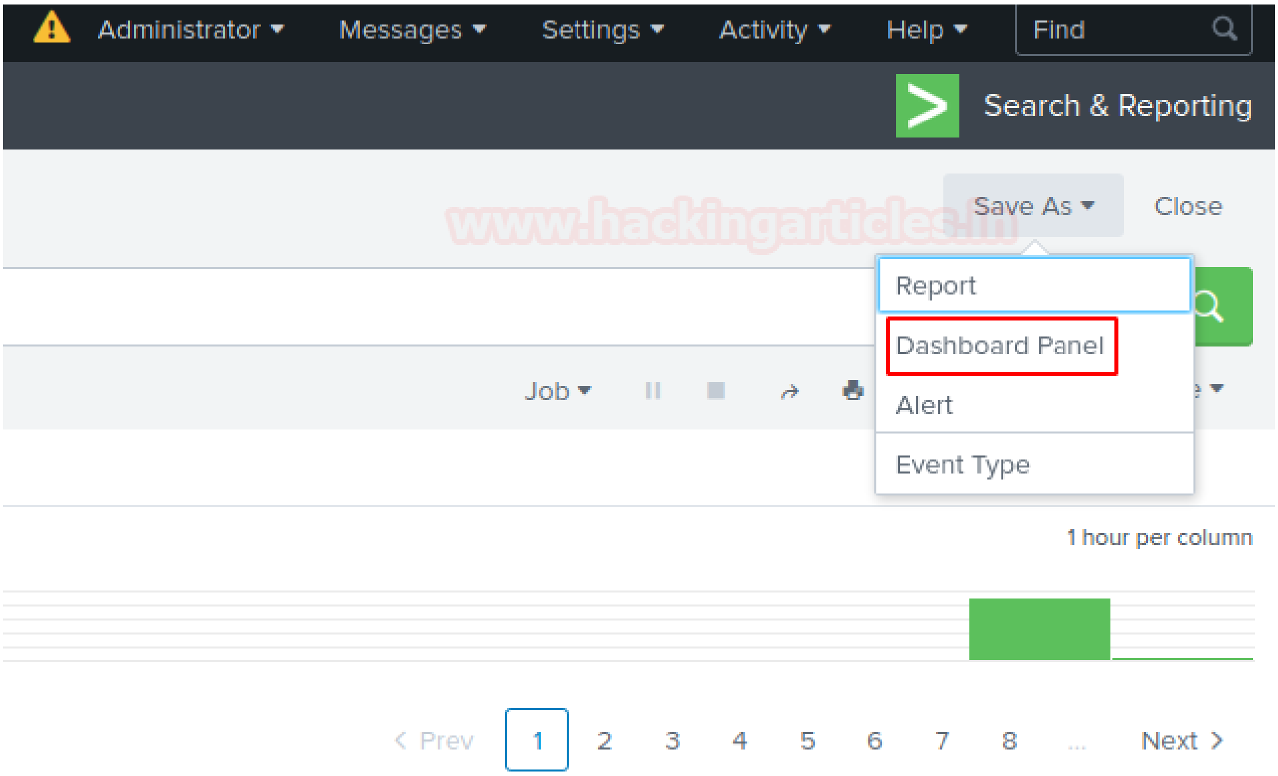
Creating a Dashboard

And then now you can save these logs directory on your dashboard or also you can create an alert that is used for triggering emails or other feeds when some unusual suspicious activity found in data is being analysed.

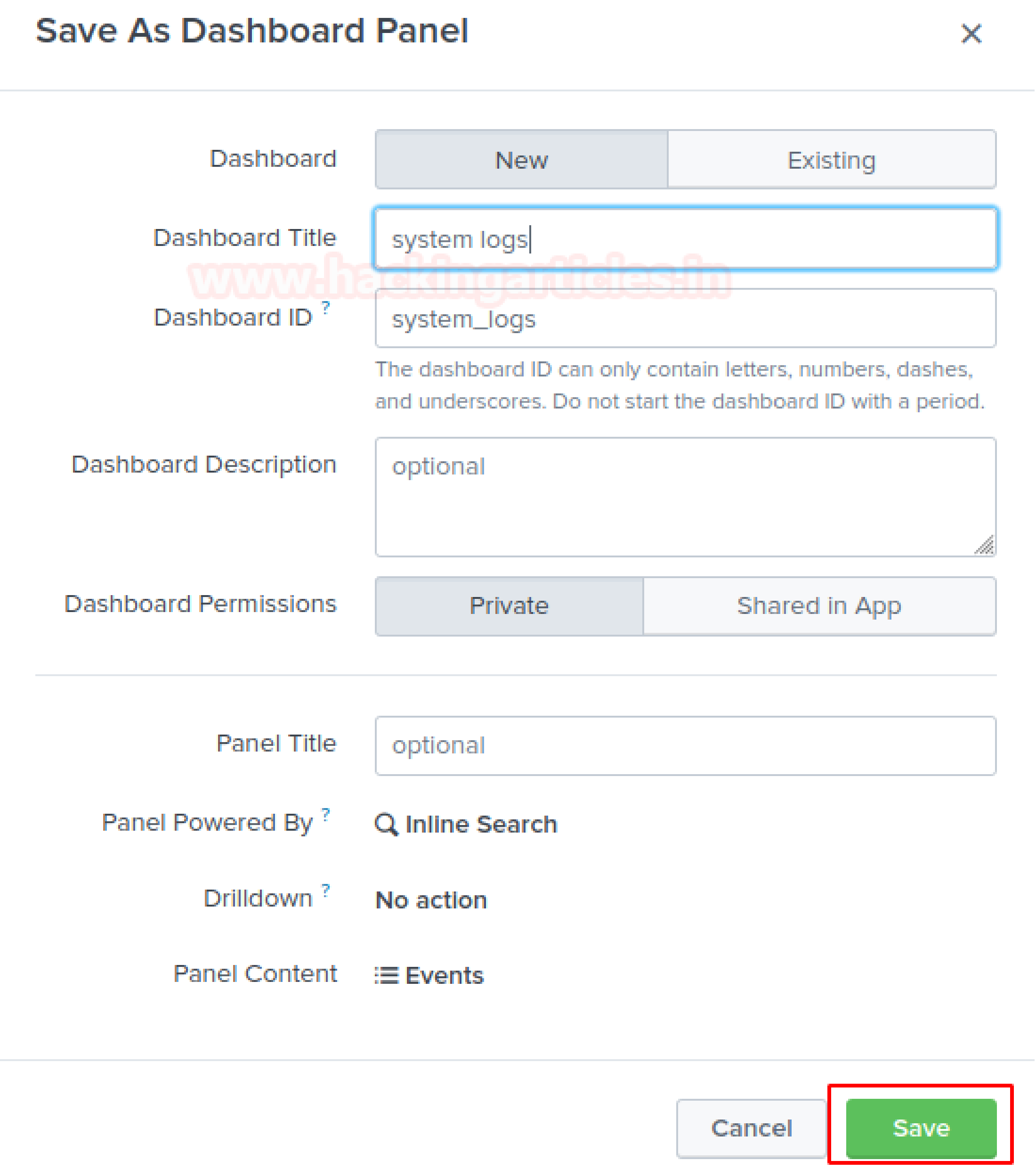
To add this search and reporting console on your Dashboard simply follow the steps as described below.

Step 5.

Just locate **"Save As"** option on above of the Search & Reporting console and select **"Dashboard Panel"**



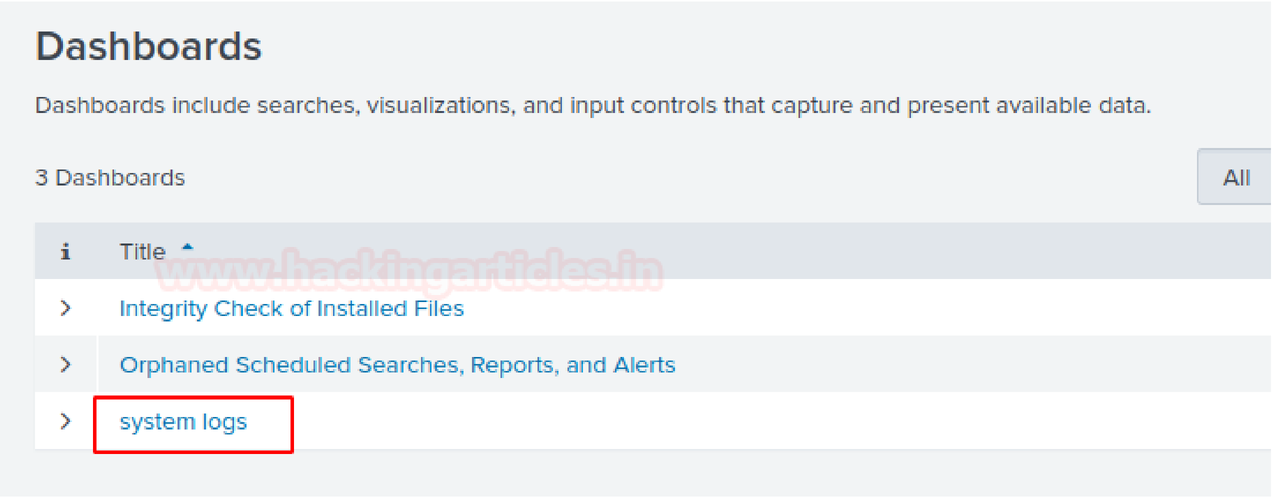
By selecting option Dashboard panel, it will prompt a Save As panel. Enter the Title of Dashboard panel and descriptions then save it.



Save As Dashboard Panel

Dashboard	New / Existing
Dashboard Title	system logs
Dashboard ID ?	system_logs
	The dashboard ID can only contain letters, numbers, dashes, and underscores. Do not start the dashboard ID with a period.
Dashboard Description	optional
Dashboard Permissions	Private / Shared in App
Panel Title	optional
Panel Powered By ?	Inline Search
Drilldown ?	No action
Panel Content	Events

Great! You have successfully created your dashboard panel. Now you can directly monitor your system logs by heading system logs under Dashboards panel.



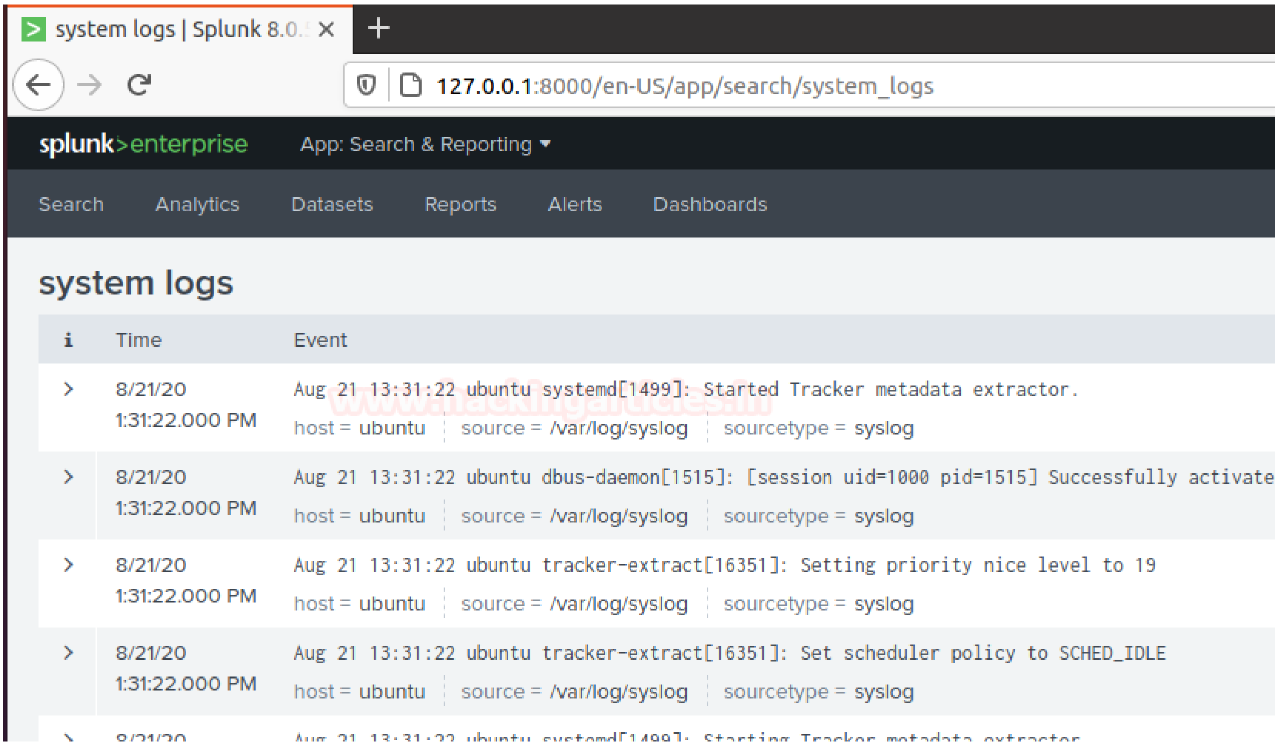
Dashboards

Dashboards include searches, visualizations, and input controls that capture and present available data.

3 Dashboards

i	Title
>	Integrity Check of Installed Files
>	Orphaned Scheduled Searches, Reports, and Alerts
>	system logs

Just select options available on your dashboard that you want to monitor in my case I'm watching the server logs that I saved in my dashboard. Now You can watch as many files of your server by simply adding it into the dashboard panel.



i	Time	Event
>	8/21/20 1:31:22.000 PM	Aug 21 13:31:22 ubuntu systemd[1499]: Started Tracker metadata extractor. host = ubuntu source = /var/log/syslog sourcetype = syslog
>	8/21/20 1:31:22.000 PM	Aug 21 13:31:22 ubuntu dbus-daemon[1515]: [session uid=1000 pid=1515] Successfully activate host = ubuntu source = /var/log/syslog sourcetype = syslog
>	8/21/20 1:31:22.000 PM	Aug 21 13:31:22 ubuntu tracker-extract[16351]: Setting priority nice level to 19 host = ubuntu source = /var/log/syslog sourcetype = syslog
>	8/21/20 1:31:22.000 PM	Aug 21 13:31:22 ubuntu tracker-extract[16351]: Set scheduler policy to SCHED_IDLE host = ubuntu source = /var/log/syslog sourcetype = syslog
>	8/21/20	Aug 21 13:31:22 ubuntu systemd[1499]: Starting Tracker metadata extractor

Log Monitoring

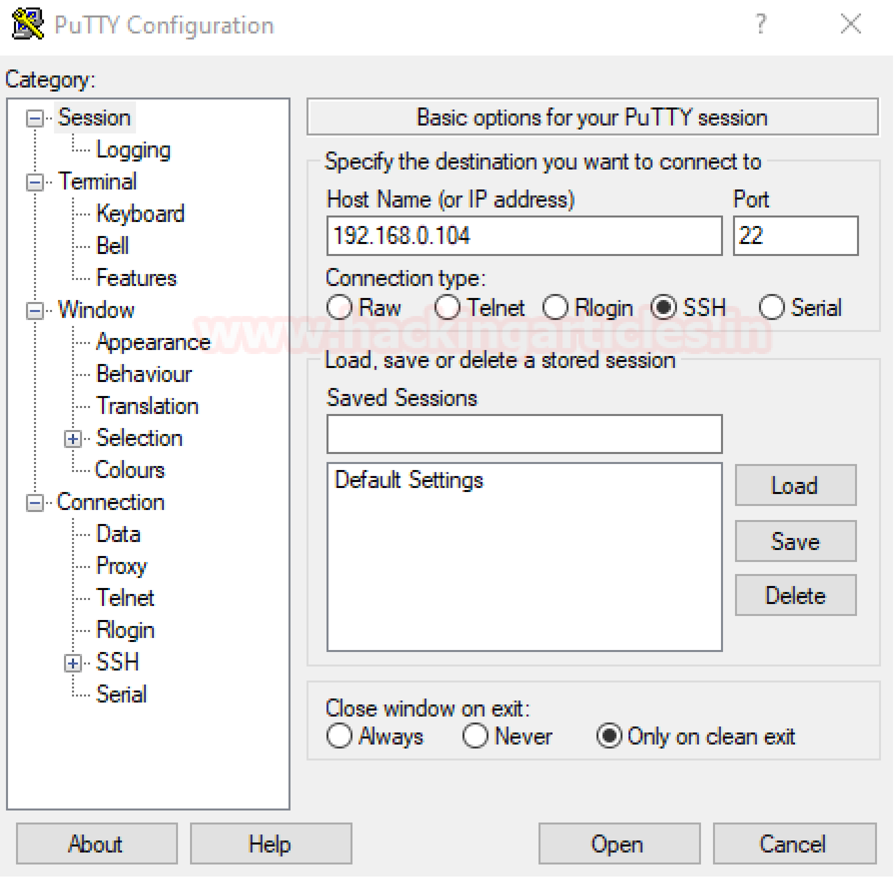
This one is a little bit special, as we can go into the **"Dashboard"** tab select the options that you want to monitor

For example, I'm going to take access to my server by different protocol's as described below

- SSH
- Telnet
- Vsftpd

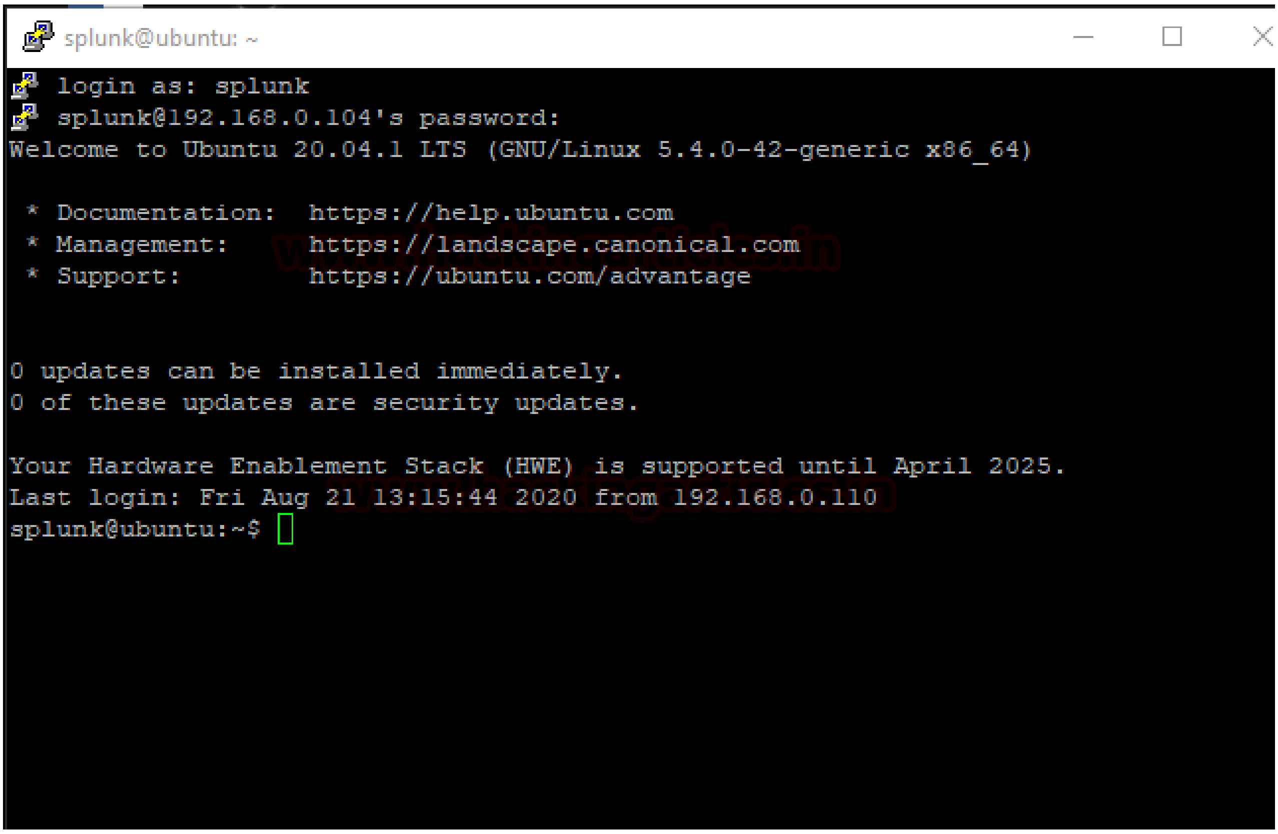
SSh

I use putty to take SSH access to my server machine



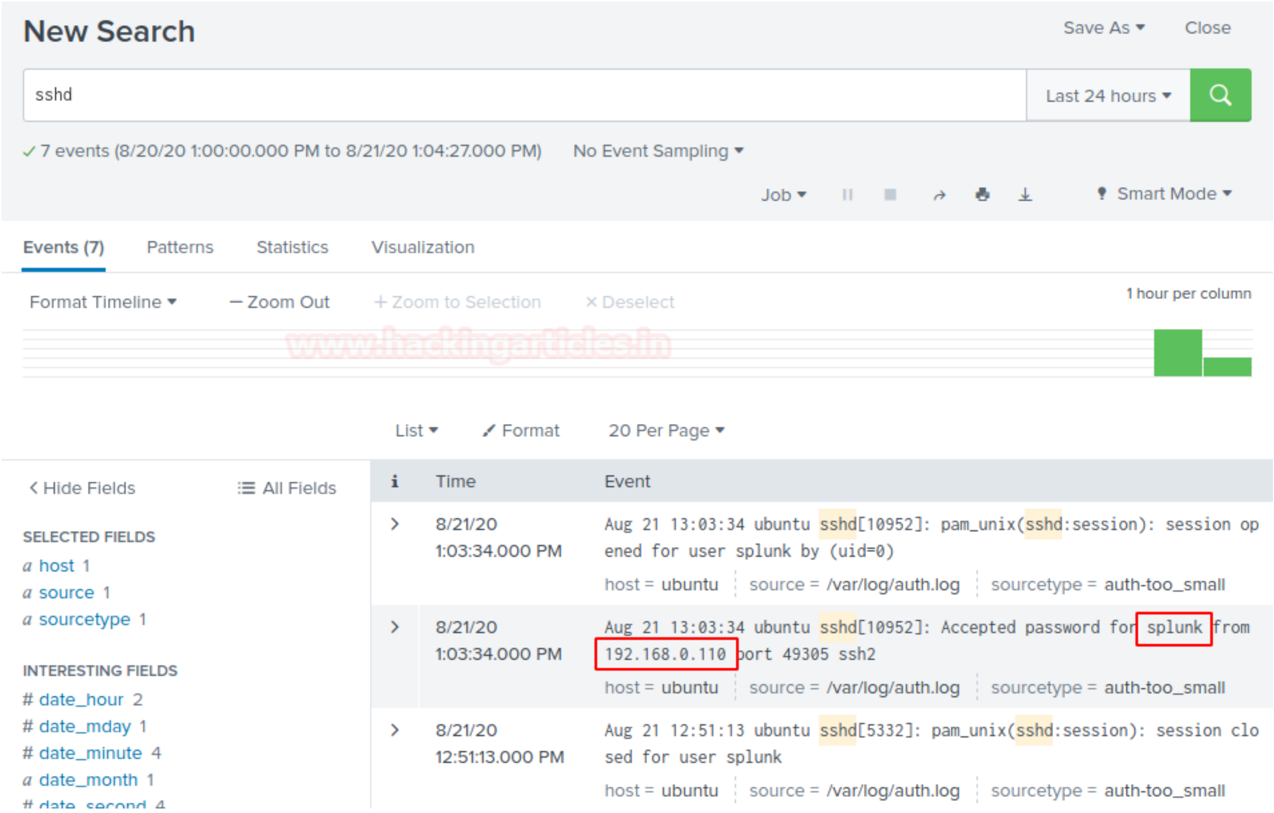
Host Name (or IP address): 192.168.0.104
Port: 22
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial
Close window on exit: ○ Always ○ Never ● Only on clean exit

After setting host or port open the SSH prompt login into the server



```
login as: splunk
splunk@192.168.0.104's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-42-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


0 updates can be installed immediately.
0 of these updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Fri Aug 21 13:15:44 2020 from 192.168.0.110
splunk@ubuntu:~$
```

After getting the access of the server get back to your dashboard and narrow down the logs to SSH on the server by running a query sshd.



sshd

✓ 7 events (8/20/20 1:00:00.000 PM to 8/21/20 1:04:27.000 PM)

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

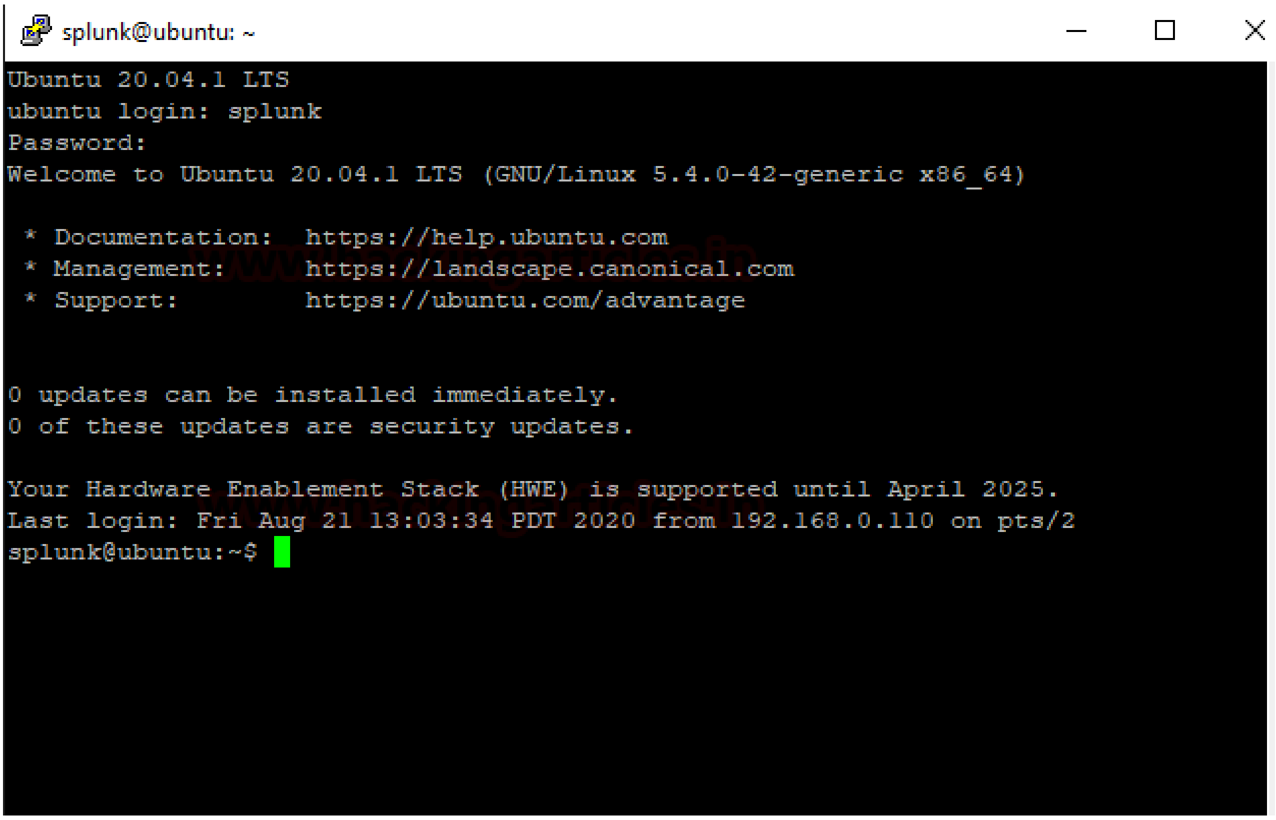
INTERESTING FIELDS
- # date_hour 2
- # date_mday 1
- # date_minute 4
- a date_month 1
- # date_second 4

Time	Event
8/21/20 1:03:34.000 PM	Aug 21 13:03:34 ubuntu sshd[10952]: pam_unix(sshd:session): session opened for user splunk by (uid=0) host = ubuntu source = /var/log/auth.log sourcetype = auth-too_small
8/21/20 1:03:34.000 PM	Aug 21 13:03:34 ubuntu sshd[10952]: Accepted password for splunk from 192.168.0.110 port 49305 ssh2 host = ubuntu source = /var/log/auth.log sourcetype = auth-too_small
8/21/20 12:51:13.000 PM	Aug 21 12:51:13 ubuntu sshd[5332]: pam_unix(sshd:session): session closed for user splunk host = ubuntu source = /var/log/auth.log sourcetype = auth-too_small

Now, we can see SSH access of the server machine in Dashboard under saved panel named system logs.

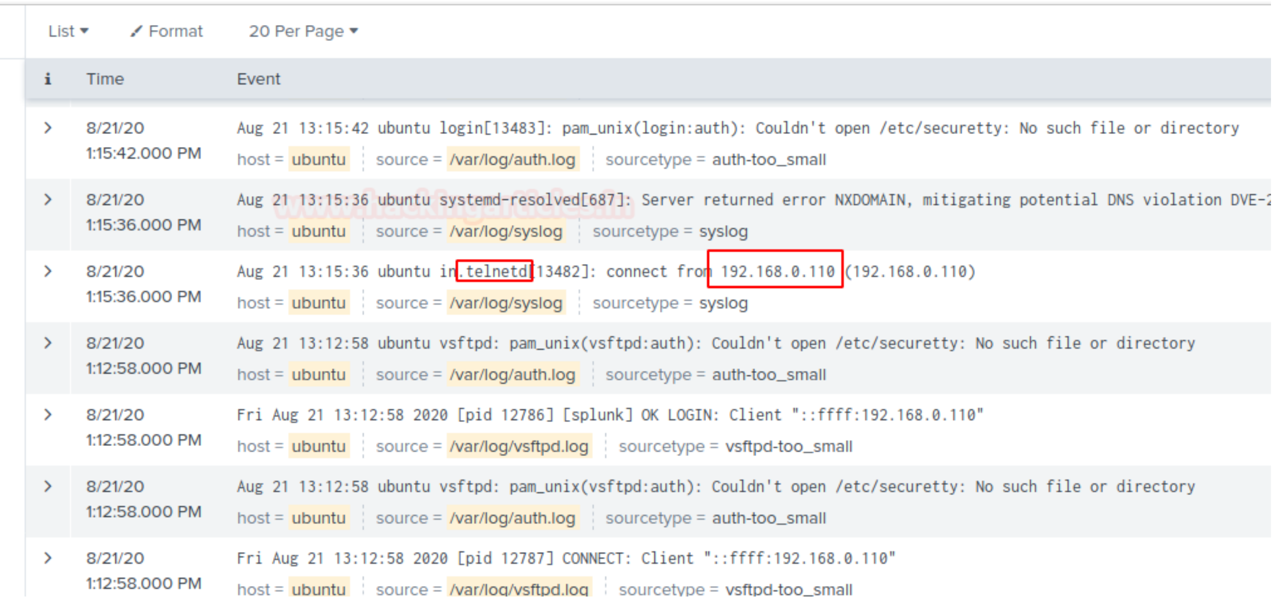
Telnet

I used the same puttygen to take telnet access of my server machine use your credentials to log in to your server.



```
Ubuntu 20.04.1 LTS
ubuntu login: splunk
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-42-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


0 updates can be installed immediately.
0 of these updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Fri Aug 21 13:03:34 PDT 2020 from 192.168.0.110 on pts/2
splunk@ubuntu:~$
```

Let’s check what happened to the Splunk dashboard. After getting the access of the server get back to your dashboard and narrow down the logs to telnet on the server by running query **telnet**.



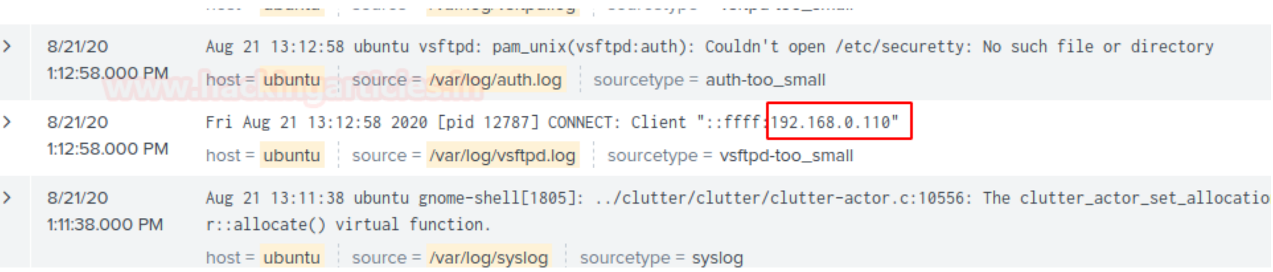
```
8/21/20 1:15:42.000 PM  Aug 21 13:15:42 ubuntu login[13483]: pam_unix(login:auth): Couldn't open /etc/securetty: No such file or directory
                        host = ubuntu   source = /var/log/auth.log   sourcetype = auth-too_small
8/21/20 1:15:36.000 PM  Aug 21 13:15:36 ubuntu systemd-resolved[687]: Server returned error NXDOMAIN, mitigating potential DNS violation DVE-2
                        host = ubuntu   source = /var/log/syslog   sourcetype = syslog
8/21/20 1:15:36.000 PM  Aug 21 13:15:36 ubuntu in.telnetd[13482]: connect from 192.168.0.110 (192.168.0.110)
                        host = ubuntu   source = /var/log/syslog   sourcetype = syslog
8/21/20 1:12:58.000 PM  Aug 21 13:12:58 ubuntu vsftpd: pam_unix(vsftpd:auth): Couldn't open /etc/securetty: No such file or directory
                        host = ubuntu   source = /var/log/auth.log   sourcetype = auth-too_small
8/21/20 1:12:58.000 PM  Fri Aug 21 13:12:58 2020 [pid 12786] [splunk] OK LOGIN: Client "::ffff:192.168.0.110"
                        host = ubuntu   source = /var/log/vsftpd.log   sourcetype = vsftpd-too_small
8/21/20 1:12:58.000 PM  Aug 21 13:12:58 ubuntu vsftpd: pam_unix(vsftpd:auth): Couldn't open /etc/securetty: No such file or directory
                        host = ubuntu   source = /var/log/auth.log   sourcetype = auth-too_small
8/21/20 1:12:58.000 PM  Fri Aug 21 13:12:58 2020 [pid 12787] CONNECT: Client "::ffff:192.168.0.110"
                        host = ubuntu   source = /var/log/vsftpd.log   sourcetype = vsftpd-too_small
```

Now, we can see Telnet access logs of the server machine in Dashboard under the same panel.

Hang on! This is not enough.

Vsftpd

I took the vsftpd access of my server machine by using **winscp** or you can use your desired applications.



```
8/21/20 1:12:58.000 PM  Aug 21 13:12:58 ubuntu vsftpd: pam_unix(vsftpd:auth): Couldn't open /etc/securetty: No such file or directory
                        host = ubuntu   source = /var/log/auth.log   sourcetype = auth-too_small
8/21/20 1:12:58.000 PM  Fri Aug 21 13:12:58 2020 [pid 12787] CONNECT: Client "::ffff:192.168.0.110"
                        host = ubuntu   source = /var/log/vsftpd.log   sourcetype = vsftpd-too_small
8/21/20 1:11:38.000 PM  Aug 21 13:11:38 ubuntu gnome-shell[1805]: ../clutter/clutter-actor.c:10556: The clutter_actor_set_allocatio
                        r::allocate() virtual function.
                        host = ubuntu   source = /var/log/syslog   sourcetype = syslog
```

Narrow down your search by running a query vsftpd and then successfully you will be able to see your server vsftpd logs. You can run more search queries to drill down it deeper.

The more will be discussed in part 2.

Coming soon!

Author – Vijay is a Certified Ethical Hacker, Technical writer and Penetration Tester at Hacking Articles. Technology and Gadget freak. Contact **Here**