



# Splunk

## SIEM: Log Monitoring

**Original Author:** *Vijay*



## Table of Contents

Abstract.....	3
SIEM: Log Monitoring Lab Setup with Splunk .....	4
<b>What is Splunk</b> .....	4
<b>Splunk Features</b> .....	4
<b>Prerequisites</b> .....	5
<b>Splunk Environment</b> .....	5
<b>Download and install Splunk</b> .....	7
<b>Adding a task</b> .....	10
<b>Creating a Dashboard</b> .....	17
<b>Log Monitoring</b> .....	21
SIEM: Windows Client Monitoring with Splunk .....	24
<b>Prerequisites</b> .....	24
<b>Configure a Receiving on Splunk Enterprise</b> .....	24
<b>Configure a receiver using the command line</b> .....	26
<b>Configure a receiver using a Configuration file</b> .....	27
<b>Environment</b> .....	28
<b>Install Splunk Universal Forwarder on Win10</b> .....	29
<b>Windows Log Monitoring</b> .....	39
<b>Threat Monitoring</b> .....	40
Conclusion .....	41
References .....	41



## Abstract

The Splunk is a tool with SIEM (Security Information and Event Management)-like capabilities that can capture, index, and correlate real-time data in a searchable repository from which it can generate graphs, reports, alerts, dashboards, and visualizations.

In this report, we will first demonstrate the setup of a Splunk master server, including a brief overview of dashboard creation and log monitoring. Next, we will focus on importing logs from the network environment into Splunk for indexing, as well as forwarding logs or data from client-server systems to Splunk Enterprise. Finally, we will explore how to monitor Windows logs and identify threats using Splunk queries.

**Disclaimer: This report is provided for educational and informational purpose only (Penetration Testing). Penetration Testing refers to legal intrusion tests that aim to identify vulnerabilities and improve cybersecurity, rather than for malicious purposes.**



# SIEM: Log Monitoring Lab Setup with Splunk

## 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

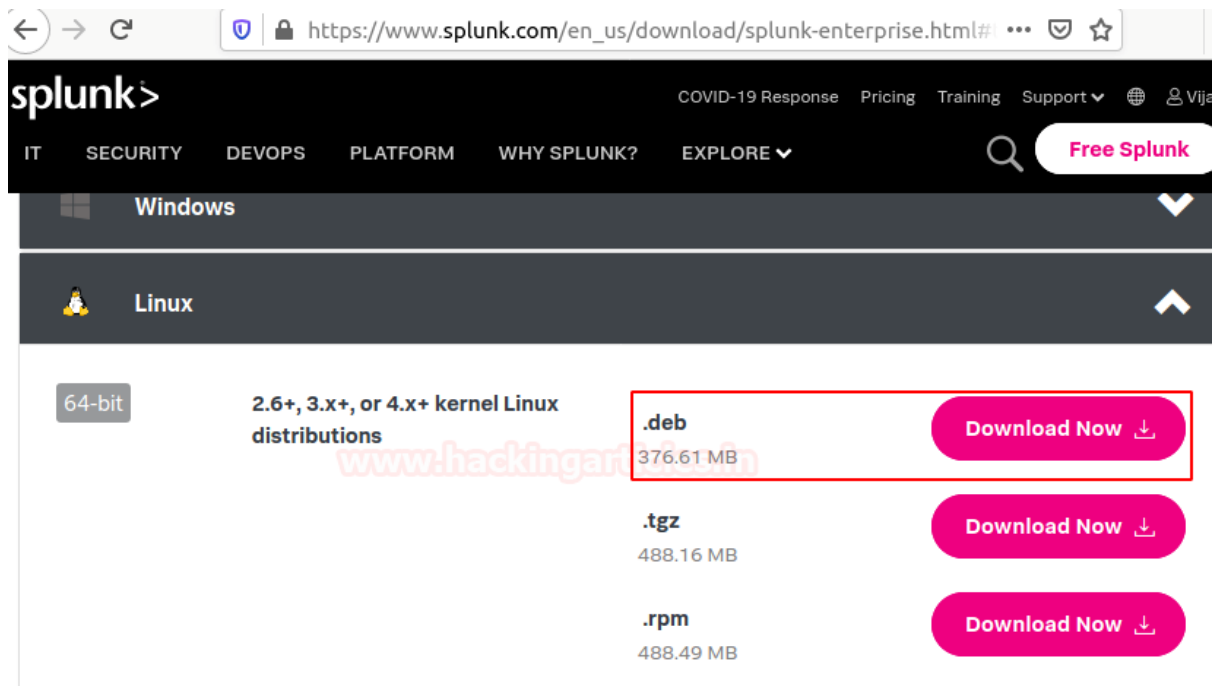
## Splunk Environment

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.

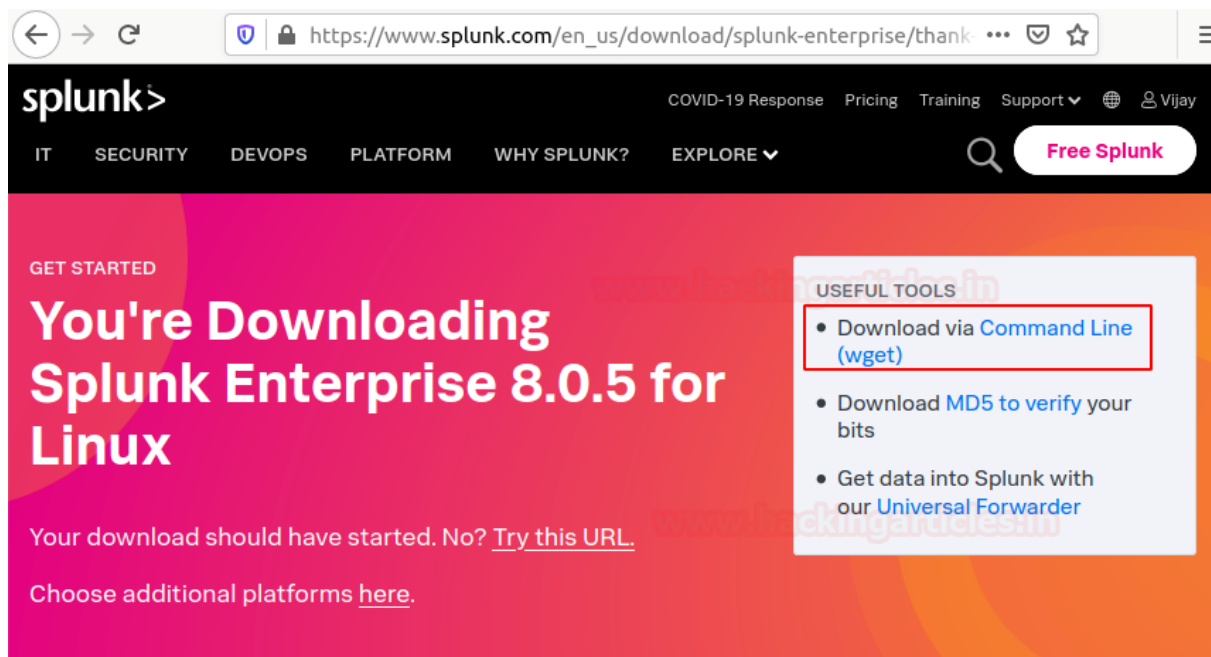
[https://www.splunk.com/en\\_us/download/splunk-enterprise.html](https://www.splunk.com/en_us/download/splunk-enterprise.html)

### 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



## 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 least
  * 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/'
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

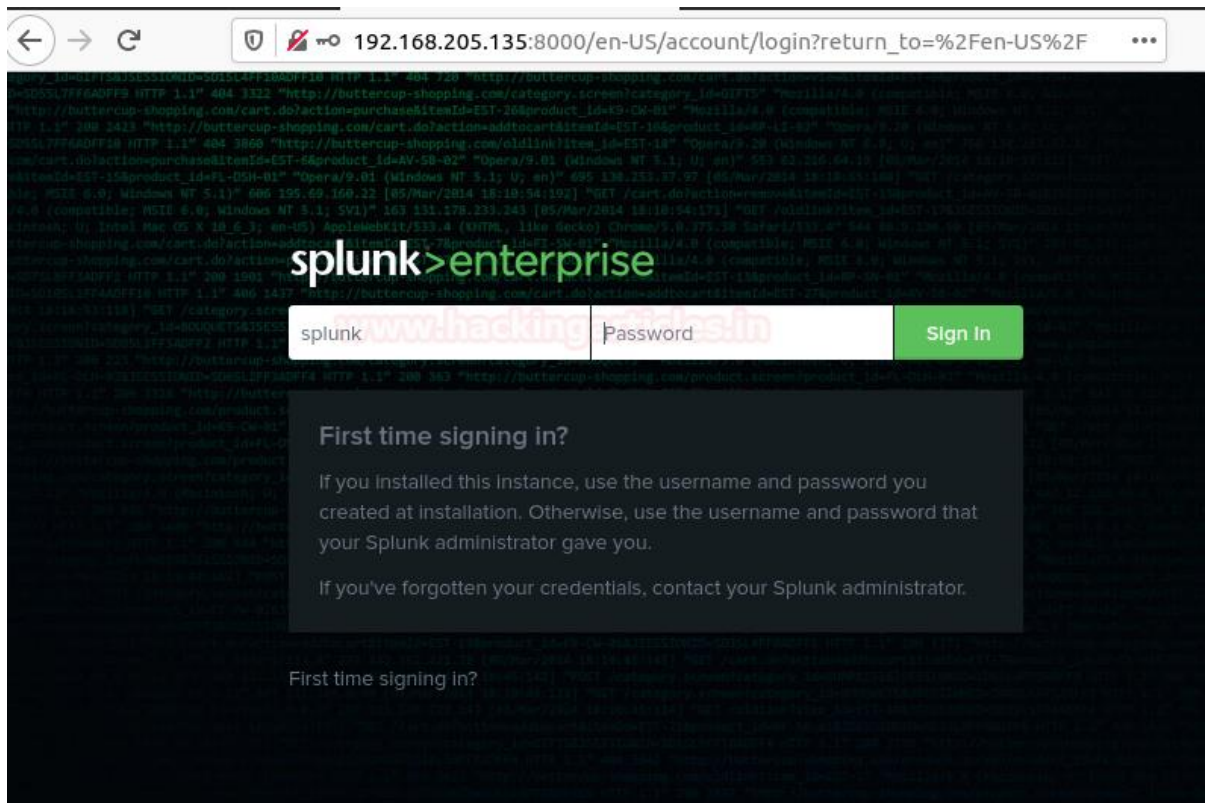
Moving '/opt/splunk/share/splunk/search_mrsparkle/modules.new' to '/opt/splunk/share/splunk/search_mrsparkle/modules'
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
root@ubuntu:/opt/splunk/bin#

```

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.



## 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 has 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
```

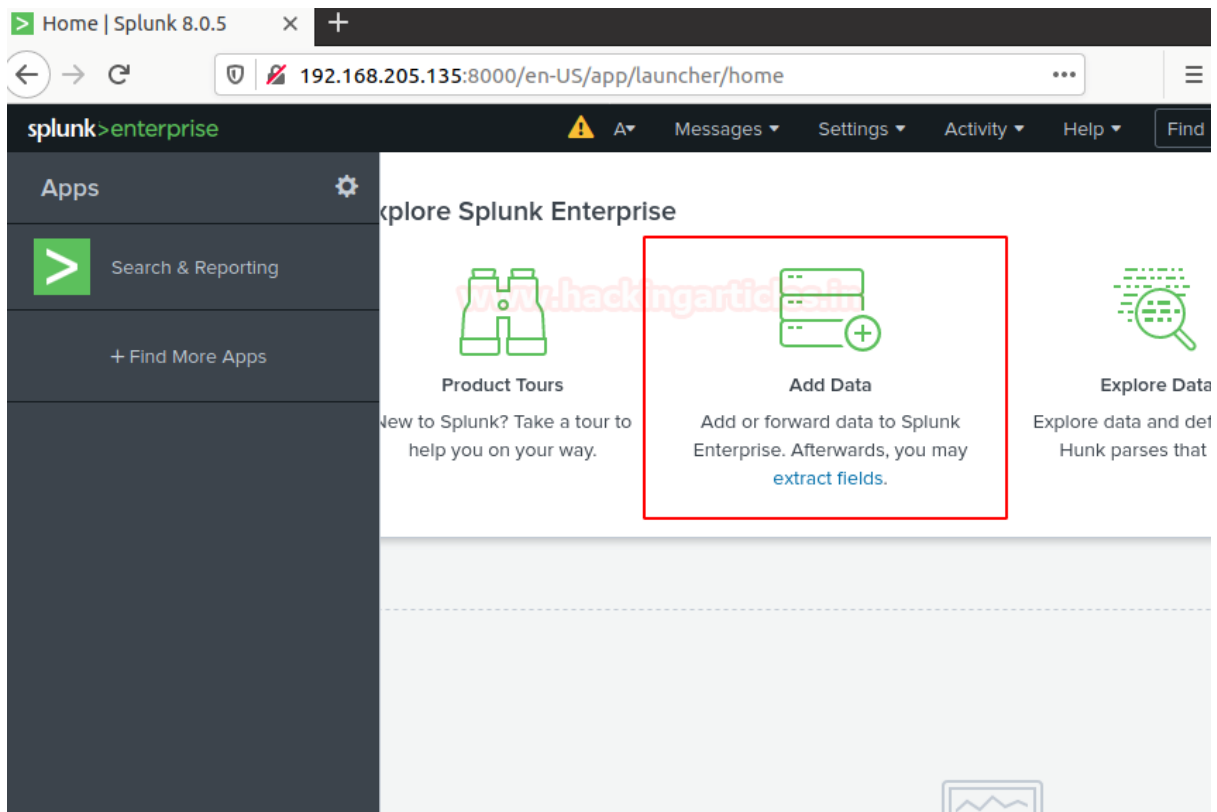
And then open Splunk search and reporting console and then run a query in the search bar.

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

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

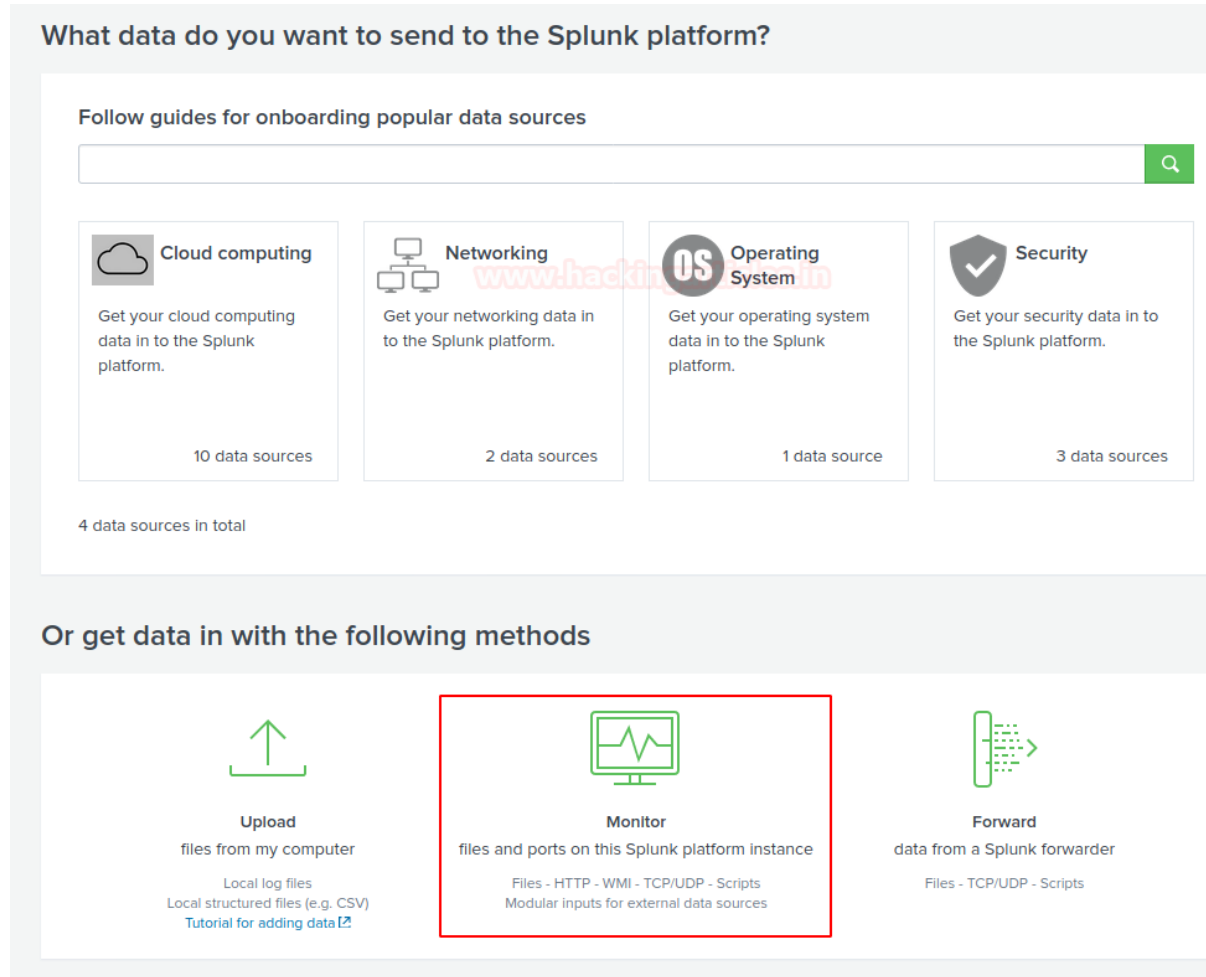
### Step 1.

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  
Get your cloud computing data in to the Splunk platform.  
10 data sources

Networking  
Get your networking data in to the Splunk platform.  
2 data sources

Operating System  
Get your operating system data in to the Splunk platform.  
1 data source

Security  
Get your security data in to the Splunk platform.  
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

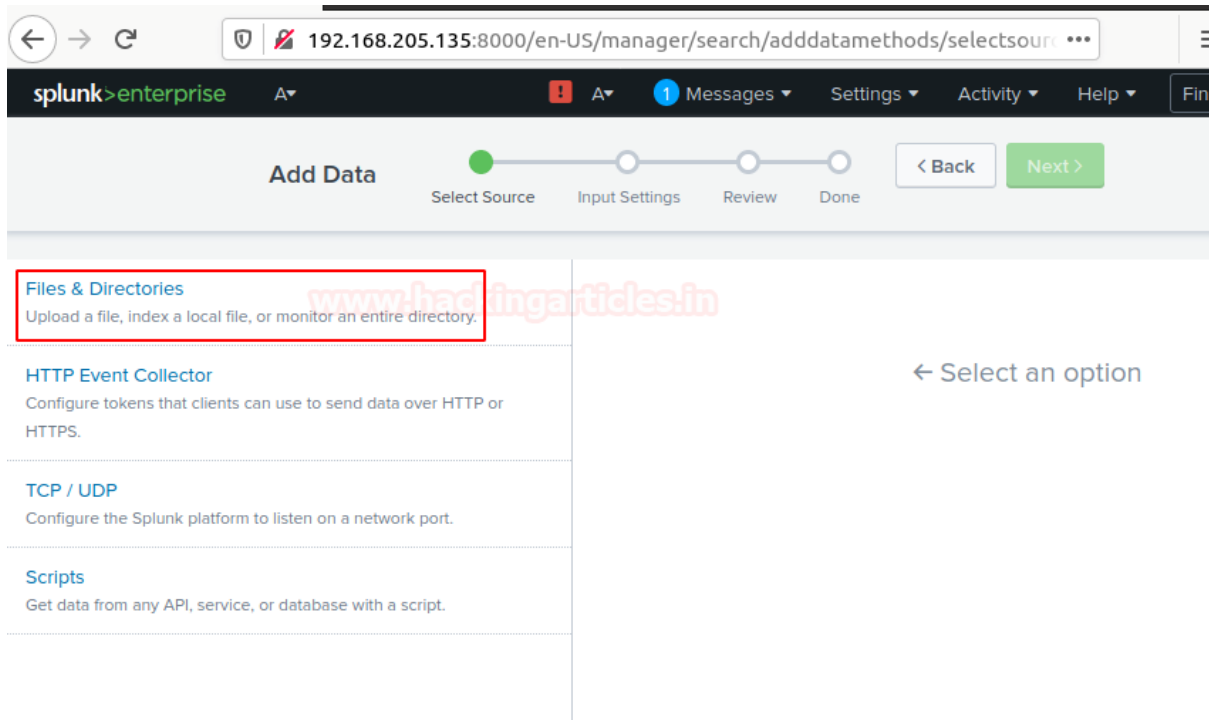
**HTTP Event Collector:** To Monitor Data streaming over HTTP

**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.



← → ↻ 192.168.205.135:8000/en-US/manager/search/adddatamethods/selectsour...

splunk>enterprise A▼ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Fin

**Add Data**

Select Source Input Settings Review Done < Back Next >

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

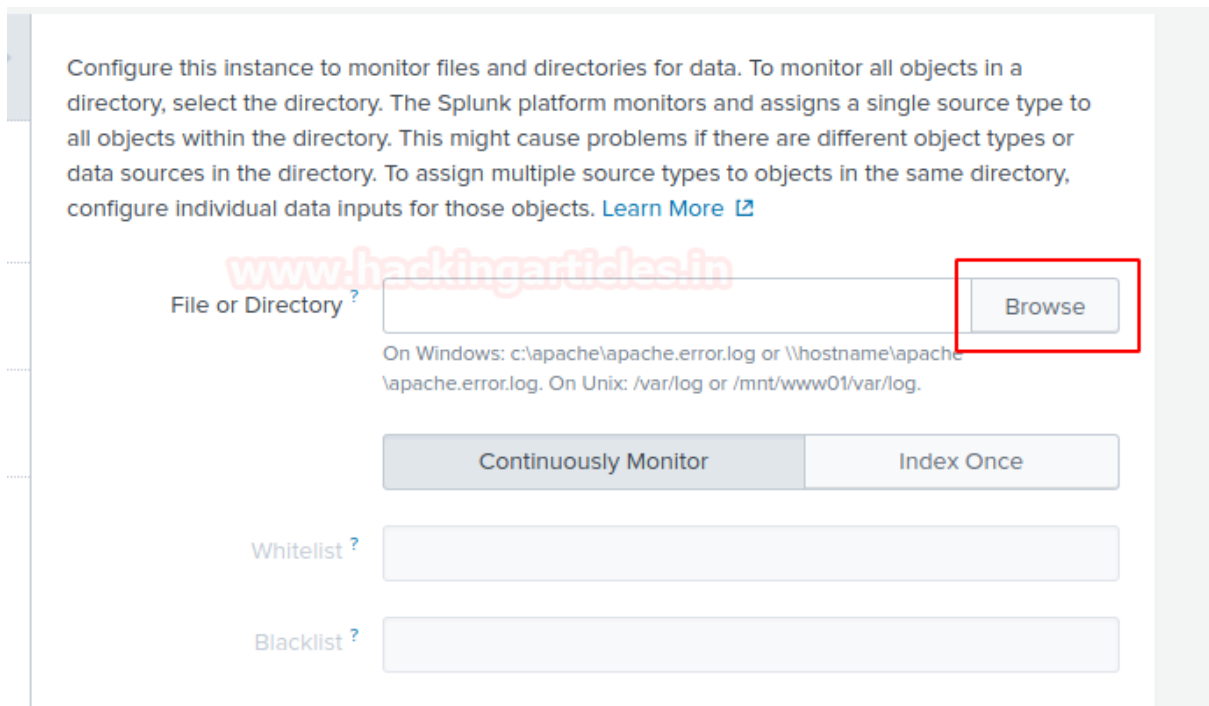
**HTTP Event Collector**  
Configure tokens that clients can use to send data over HTTP or HTTPS.

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

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

← Select an option

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 ?  Browse

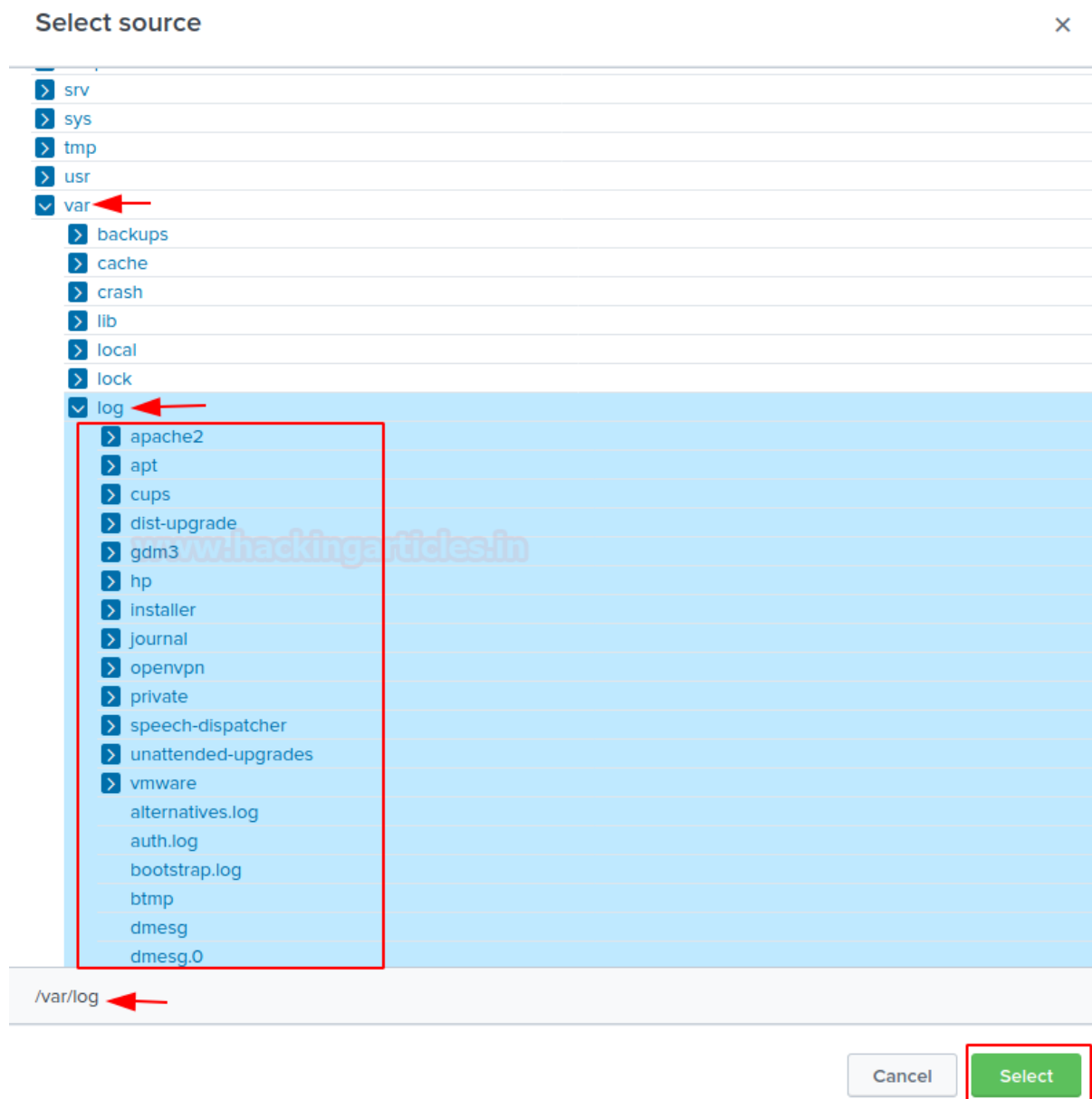
On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Continuously Monitor Index Once

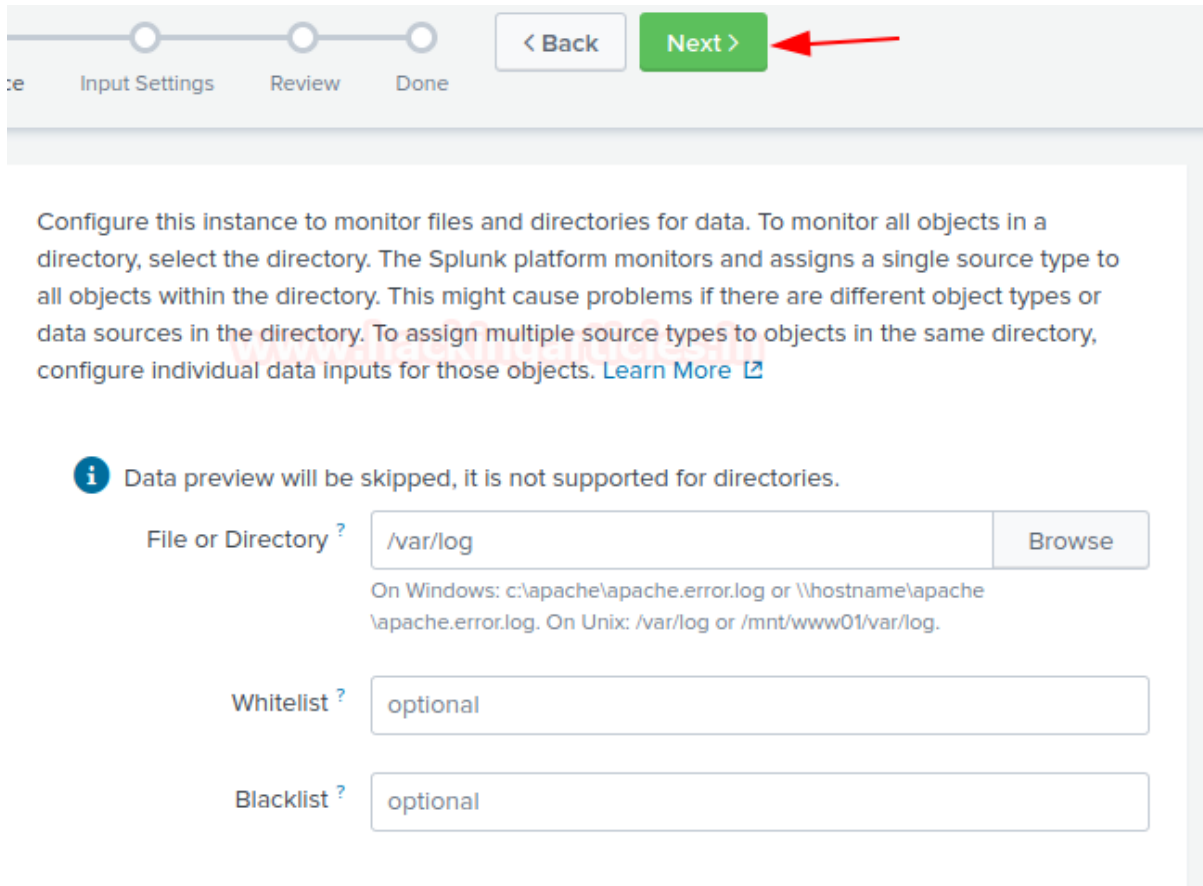
Whitelist ?

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](#)

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

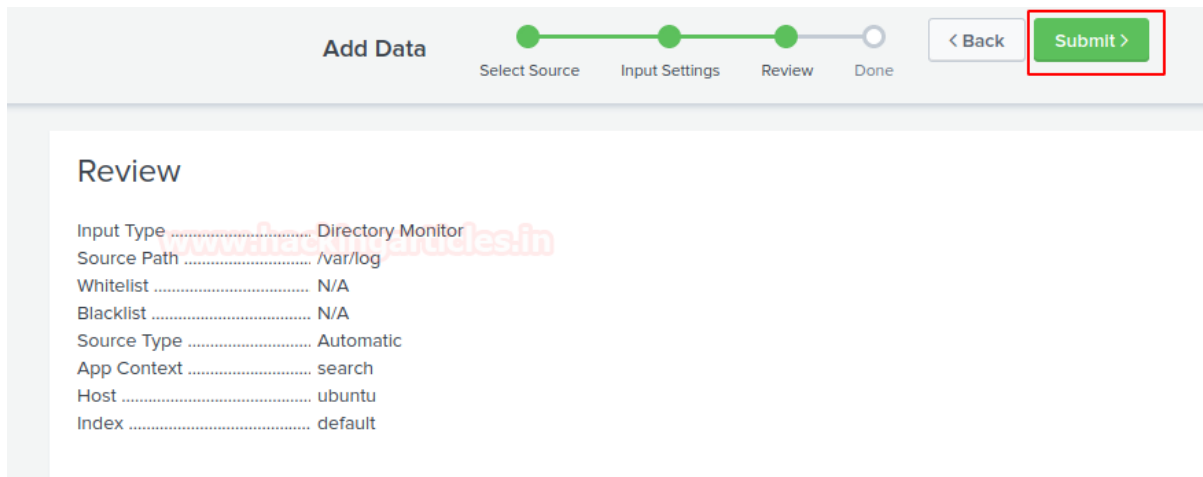
File or Directory <sup>?</sup>

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

Whitelist <sup>?</sup>

Blacklist <sup>?</sup>

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.



**Add Data**

Select Source   Input Settings   **Review**   Done

**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](#)

Start Searching

Search your data now or see [examples and tutorials](#). [🔗](#)

Add More Data

Add more data inputs now or see [examples and tutorials](#). [🔗](#)

Download Apps

Apps help you do more with your data. [Learn more](#). [🔗](#)

Build Dashboards

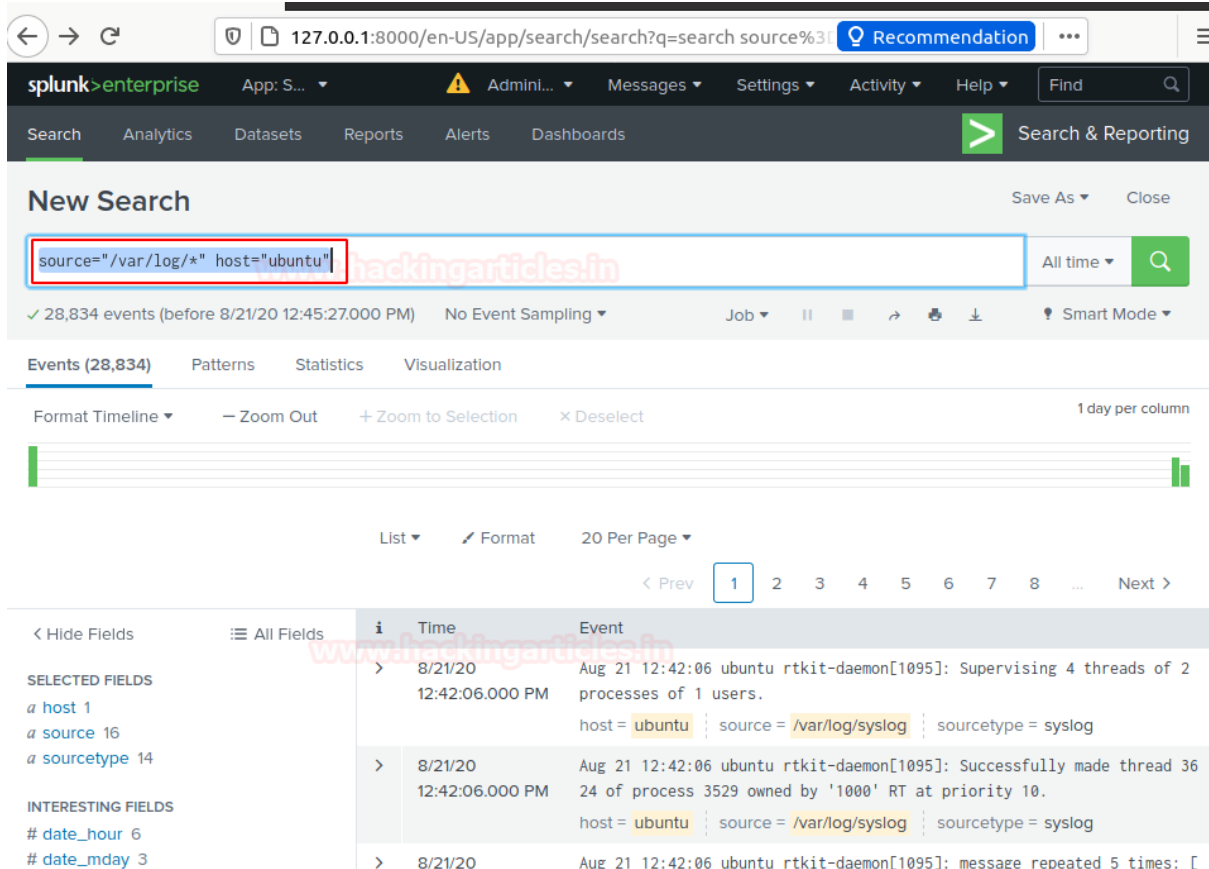
Visualize your searches. [Learn more](#). [🔗](#)

### 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"
```





The screenshot shows the Splunk Enterprise Search & Reporting interface. The search bar contains the query `source="/var/log/*" host="ubuntu"`. The search results show 28,834 events. The results are displayed in a table format with columns for Time and Event. The first two events are highlighted.

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 3624 of process 3529 owned by '1000' RT at priority 10. host = ubuntu   source = /var/log/syslog   sourcetype = syslog

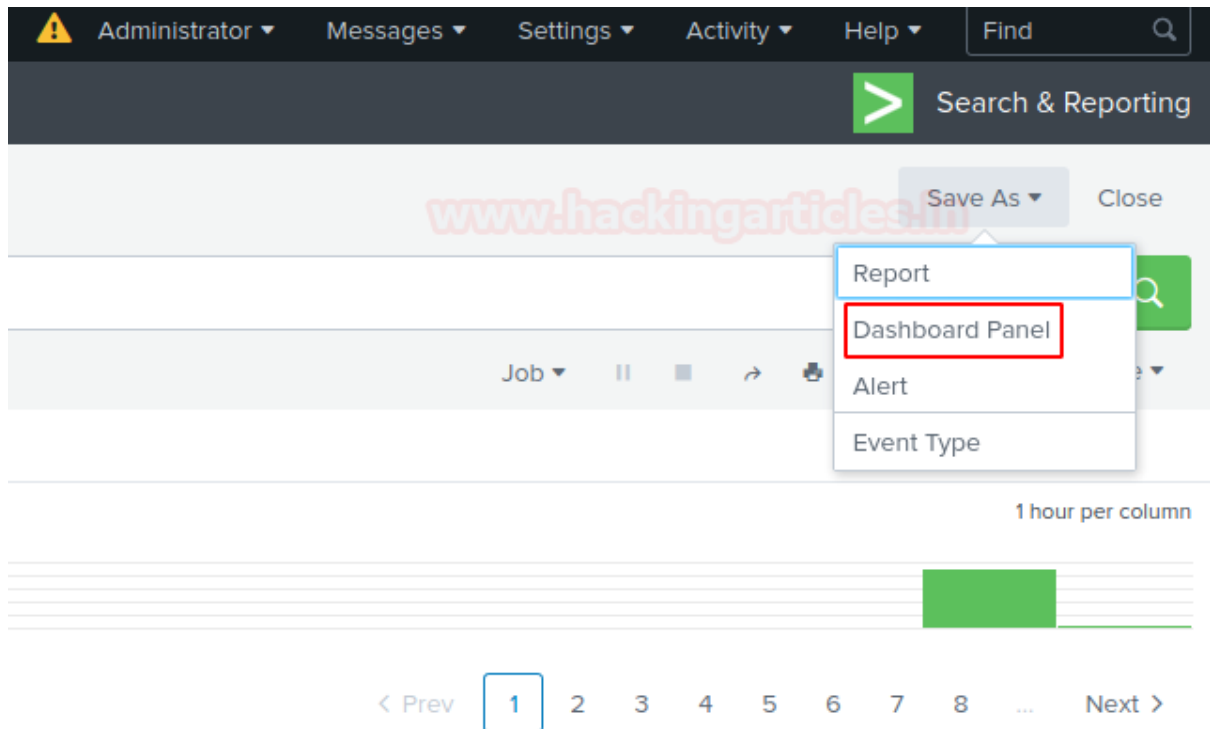
## Creating a Dashboard

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 ?

Q Inline Search

Drilldown ?

No action

Panel Content

≡ Events

Cancel

Save

**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

All

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.

system logs | Splunk 8.0.0 X +

127.0.0.1:8000/en-US/app/search/system\_logs

splunk>enterprise App: Search & Reporting

Search Analytics Datasets Reports Alerts Dashboards

### system logs

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

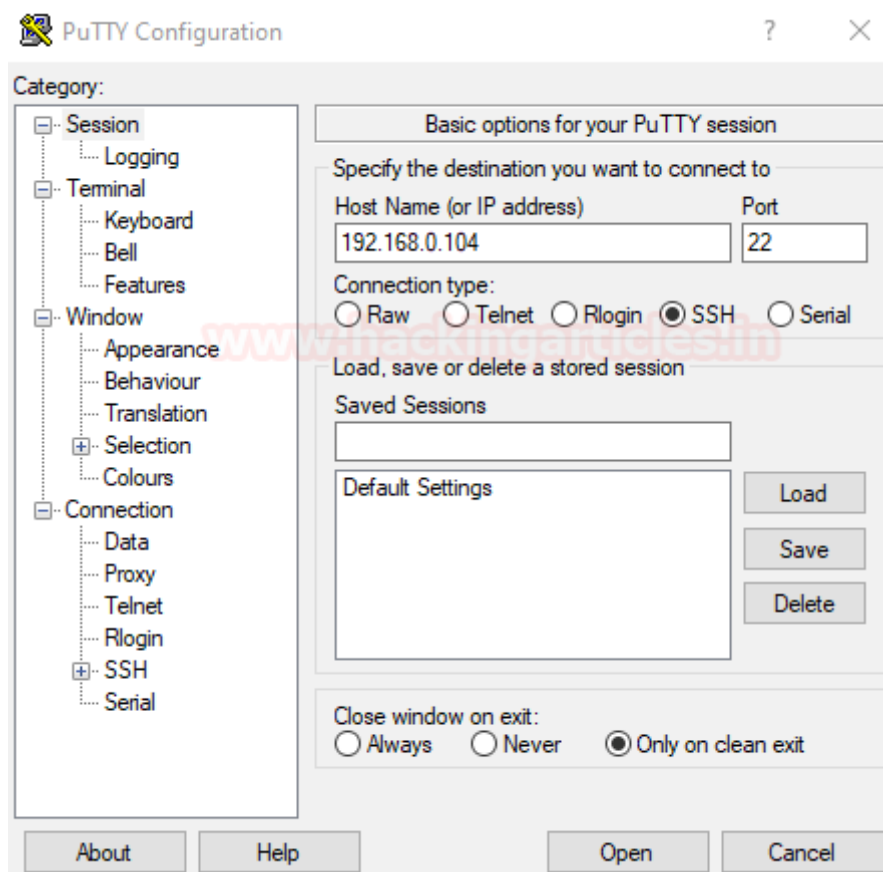
This one is a little bit special, as we can go into the **“Dashboard”** tab select the options that you want to monitor

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



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

```
splunk@ubuntu: ~
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`.

**New Search** Save As Close

Last 24 hours 🔍

✓ 7 events (8/20/20 1:00:00.000 PM to 8/21/20 1:04:27.000 PM) No Event Sampling

Job ⏏ ⏏ ⏏ ⏏ ⏏ ⏏ Smart Mode

**Events (7)** Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

www.hackingarticles.in

List Format 20 Per Page

	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

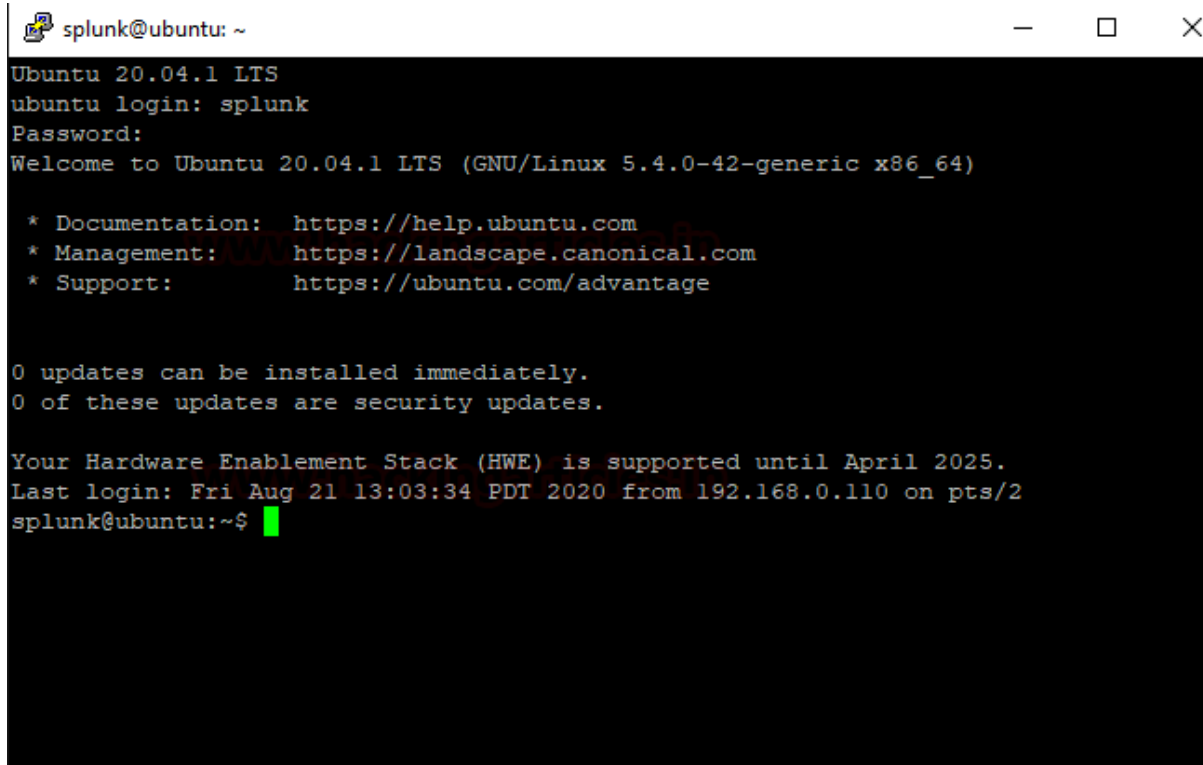
**SELECTED FIELDS**  
[a host](#) 1  
[a source](#) 1  
[a sourcetype](#) 1

**INTERESTING FIELDS**  
[# date\\_hour](#) 2  
[# date\\_mday](#) 1  
[# date\\_minute](#) 4  
[a date\\_month](#) 1  
[# date\\_second](#) 4

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.



```
splunk@ubuntu: ~
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**.

List ▾   Format   20 Per Page ▾		
i	Time	Event
>	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 Aug 21 13:12:58 ubuntu vsftpd: pam_unix(vsftpd:auth): Couldn't open /etc/security: No such file or directory
1:12:58.000 PM host = ubuntu source = /var/log/auth.log sourcetype = auth-too_small

> 8/21/20 Fri Aug 21 13:12:58 2020 [pid 12787] CONNECT: Client "::-ffff:192.168.0.110"
1:12:58.000 PM host = ubuntu source = /var/log/vsftpd.log sourcetype = vsftpd-too_small

> 8/21/20 Aug 21 13:11:38 ubuntu gnome-shell[1805]: ../clutter/clutter/clutter-actor.c:10556: The clutter_actor_set_allocatio
1:11:38.000 PM 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.

# SIEM: Windows Client Monitoring with Splunk

## Prerequisites

To configure Splunk universal Forwarder on your client-server, there are some prerequisites required for installation.

- Windows, Linux systems, or cloud servers with admin access.
- Splunk Universal forwarder
- Attacker: Kali Linux

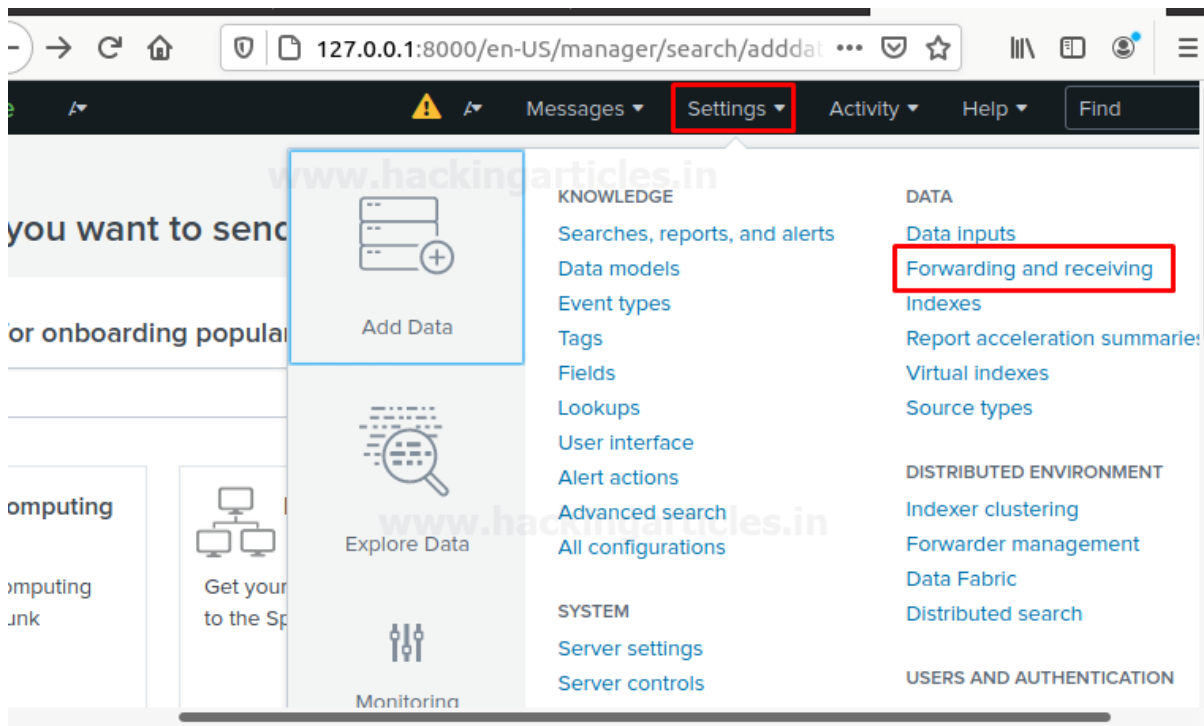
## Configure a Receiving on Splunk Enterprise

On your Splunk Dashboard, you must configure an indexer to receive data before you can send data to it. If you did not do this, then your data not going anywhere.

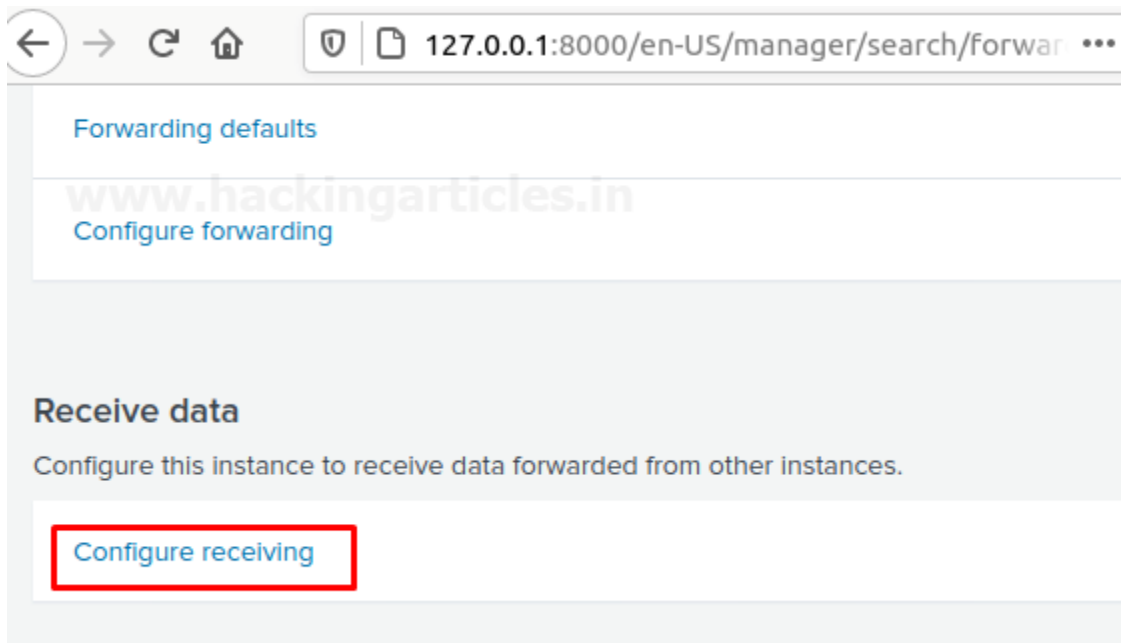
Use the Splunk web interface to configure a receiver for Splunk-to-Splunk (S2S) communication. To do this follow the below steps



- Log into Splunk web using your credentials
- On Splunk web go to **Settings > Forwarding and Receiving**

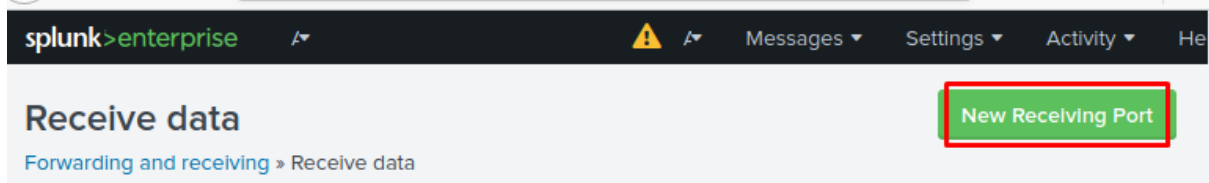


Select “configure Receiving”.



Verify the existing ports are open or not. If there are no ports available, then add a port also you cannot create a duplicate receiver port. The most suitable receiver port on indexers is **port 9997**.

Select “New receiving port.”



- Add a port number and save and do not forget to verify that port is available or not reserved to any other service or instance.

#### Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

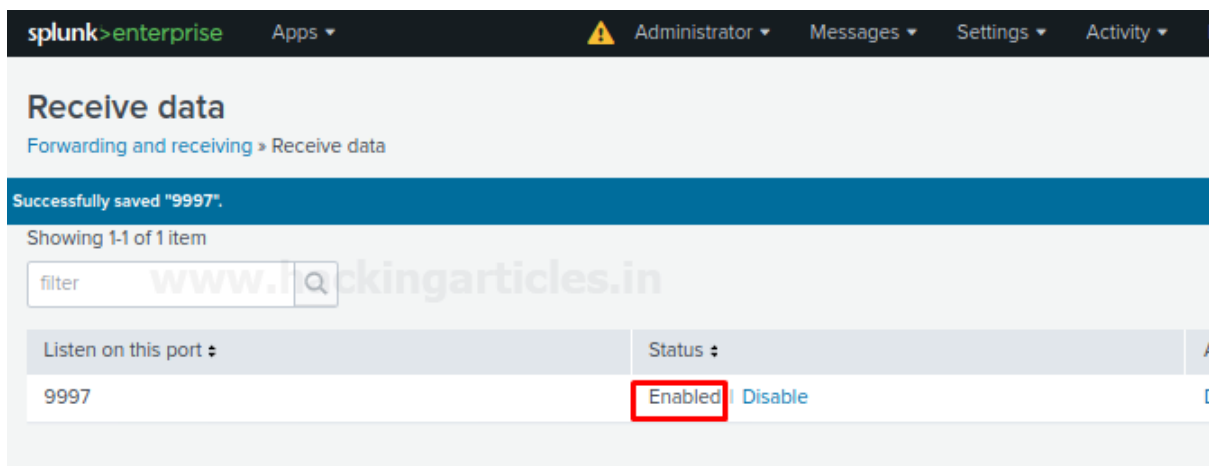
Listen on this port \* 9997

For example, 9997 will receive data on TCP port 9997.

Cancel

Save

Check the status for receiving port, it should enable for listening to the traffic.



## Configure a receiver using the command line

Use the command-line interface with Admin privilege in windows 10 or terminal with root user to configure a receiver for S2S communications. To do this follow the steps as described below.

- Open a shell with admin rights or the terminal with root user
- Change the path to \$SPLUNK\_HOME/bin
- (For Linux) Type:



```
./splunk enable listen 9997 -auth admin:password
```

- (For windows) Type:

```
Splunk enables listen 9997 -auth admin: password
```

- Restart Splunk for the changes to take effect by going into Splunk web interface **setting > server control > restart Splunk**.

Or

## Configure a receiver using a Configuration file

### For windows

Configure **inputs.conf** file for S2S communication:

- Open a shell prompt
- Change the path to \$SPLUNK\_HOME/etc/system/local
- Edit the **conf** file.
- Edit the input.conf file with [ splunktcp ] stanza and define the receiving port. Example:

```
[splunktcp://9997]
```

```
disabled = 0
```

- Save the file.
- Restart Splunk to take effect of the saved changes.

### For Linux

Open the Splunk forwarder directory wherever it installs and locate the file named **input.conf** and make changes as described above or as per your requirements.

## Environment

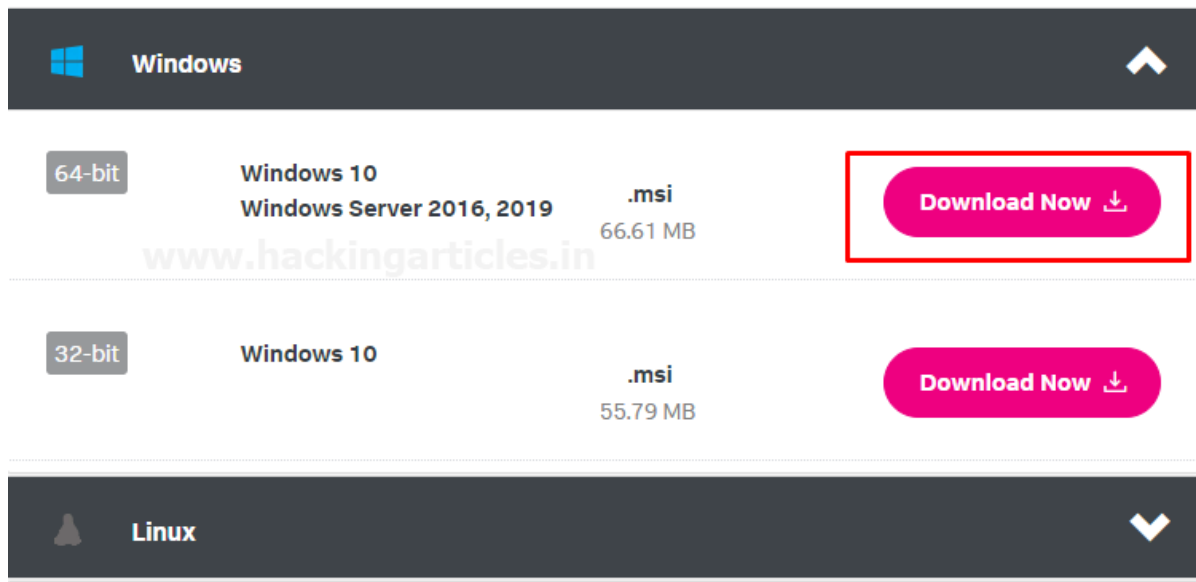
In this section, we will target to install a **Splunk Universal Forwarder** on a **Windows Machine** or server. You can download Splunk forwarder by following the below link.

[https://www.splunk.com/en\\_us/download/universal-forwarder.html](https://www.splunk.com/en_us/download/universal-forwarder.html)

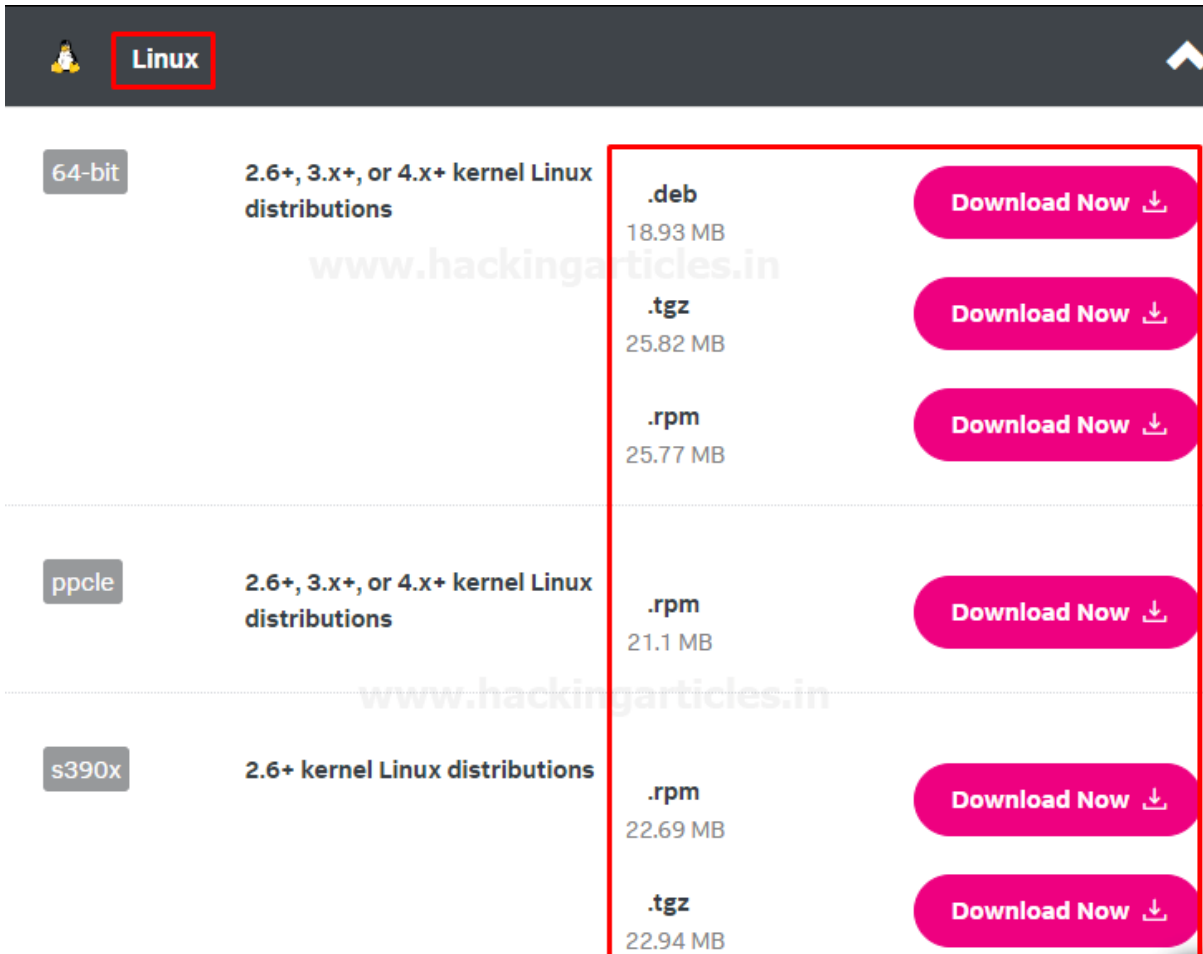
### Choose your installation package

- Create a Splunk Account and download Splunk universal forwarder for Windows version by the given above link.
- We choose **Windows 10 64 bit .msi** Package for the installation in windows. You can choose it as per your system requirements.

### Choose Your Installation Package



Or also for **Linux systems**, you can go with the options are available to download on the Splunk website by drop down the option Linux then select and download package as per your choice as shown below.



Architecture	Kernel Version	Format	Size	Action
64-bit	2.6+, 3.x+, or 4.x+ kernel Linux distributions	.deb	18.93 MB	<a href="#">Download Now</a>
		.tgz	25.82 MB	<a href="#">Download Now</a>
		.rpm	25.77 MB	<a href="#">Download Now</a>
ppcle	2.6+, 3.x+, or 4.x+ kernel Linux distributions	.rpm	21.1 MB	<a href="#">Download Now</a>
s390x	2.6+ kernel Linux distributions	.rpm	22.69 MB	<a href="#">Download Now</a>
		.tgz	22.94 MB	<a href="#">Download Now</a>

## Install Splunk Universal Forwarder on Win10

To install Universal forwarder into your operating systems, follow the steps as described below:

Visit the Splunk official website and select and download universal forwarder for **Windows 10 .msi file**. It will download a Zip file into your downloads as shown below.

GET STARTED

## Choose Your Download

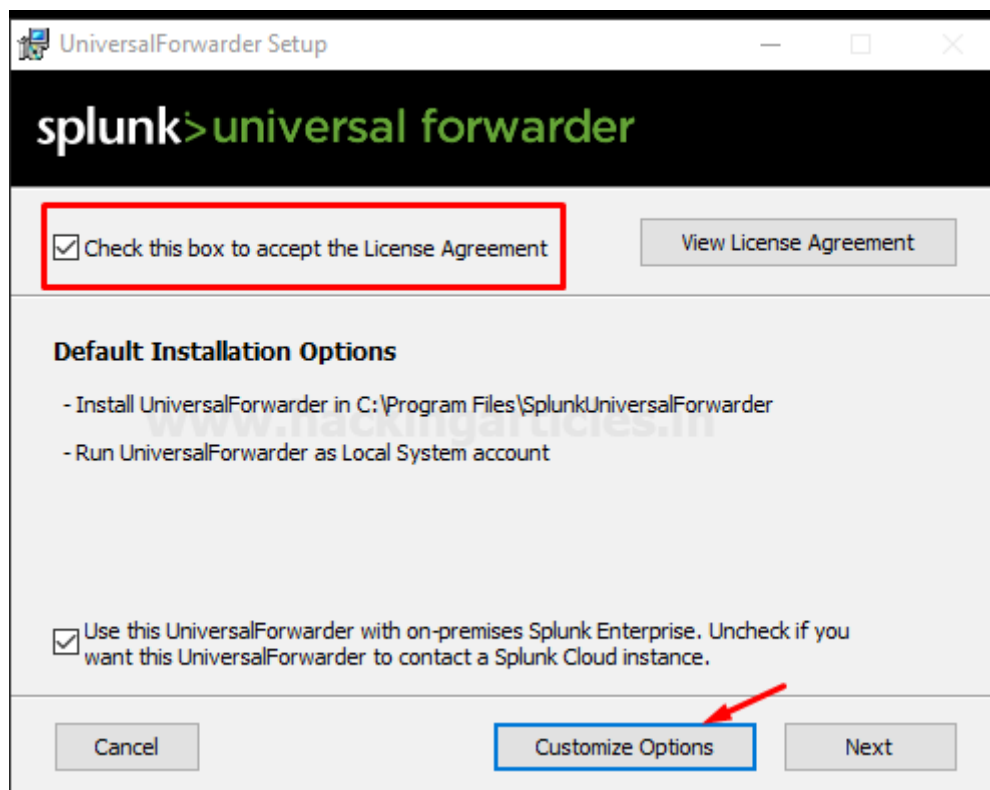
### Splunk Universal Forwarder 8.0.5

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

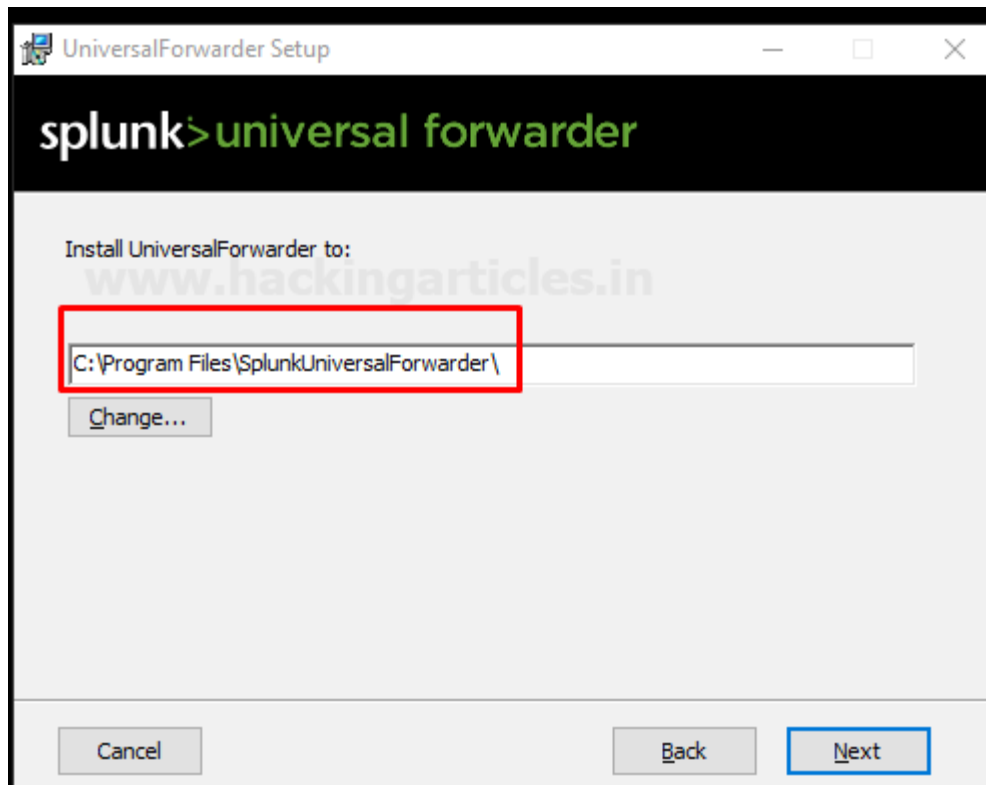
#### Choose Your Installation Package

 <b>Windows</b>	 Linux	 Solaris	 Mac OS	 FreeBSD	 AIX
64-bit	Windows 10 Windows Server 2016, 2019	.msi	66.61 MB	<a href="#">Download Now</a> 	

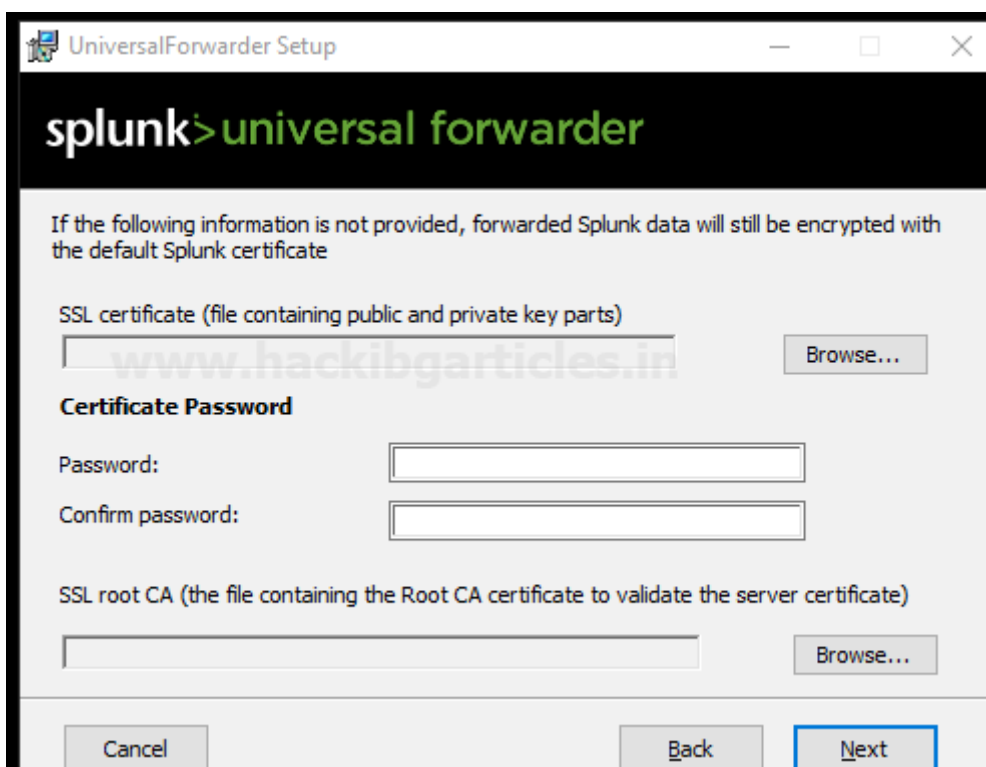
When it gets downloaded open it and start the installation process and accept the license agreement then go to **customize options** as shown below:



Further, select the installation directory wherever you want to install it as shown below



Further, it will ask you to for an SSL certificate for the encryption with your encryption key if you do not have the SSL certificate then don't worry forwarded Splunk data will still be encrypted with the default Splunk certificate all you need to do is go with **Next** option.

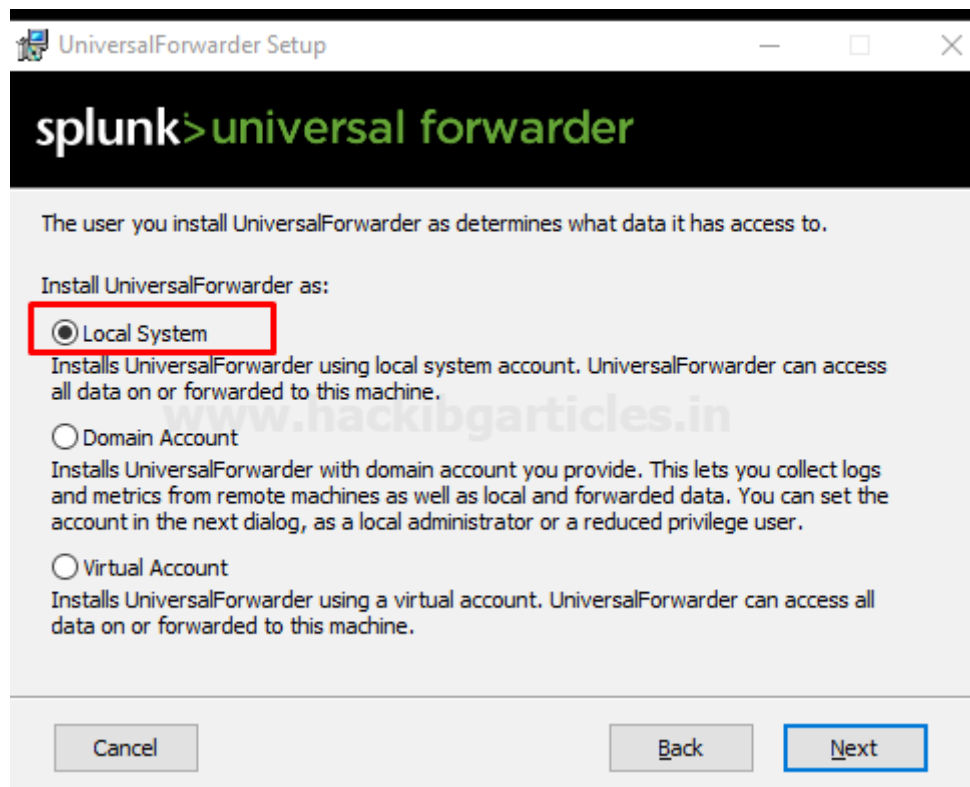


On the next dialogue you will have two options:

- Local System. If you specify the Local System user during the installation process, the universal forwarder can access all your data on that is available on your local system or forwarded to this machine.
- Domain account. This option installs the forwarder as the Windows user specifies this lets you collect logs and metrics from remote machines as well as local and forwarded data. You can set the permissions of account in the next dialogue, as a local administrator or a reduced privilege user It does not collect data from resources that the Windows user does not have access to.

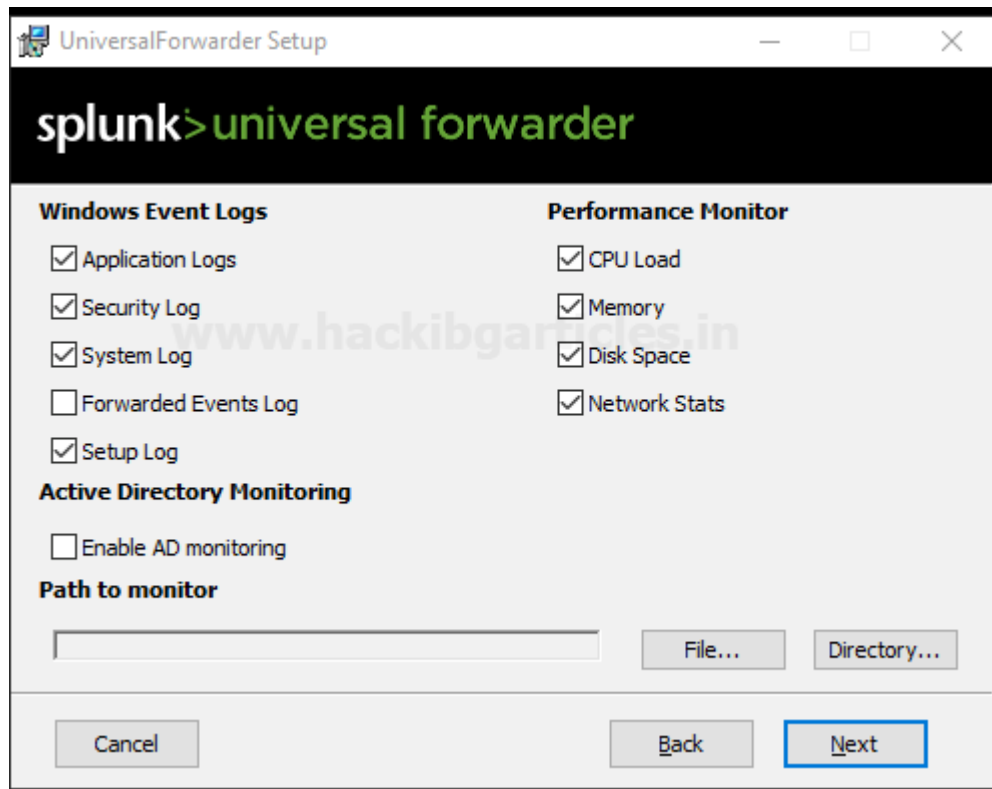
So, we go with the option **Local Systems** and Install the forwarder as a Local account to do any of the following:

- Read Event Logs remotely
- It Collects all your system performance counters remotely
- Read network shares for log files
- It can Access the Active Directory schema, using [Active Directory monitoring](#) if you select it

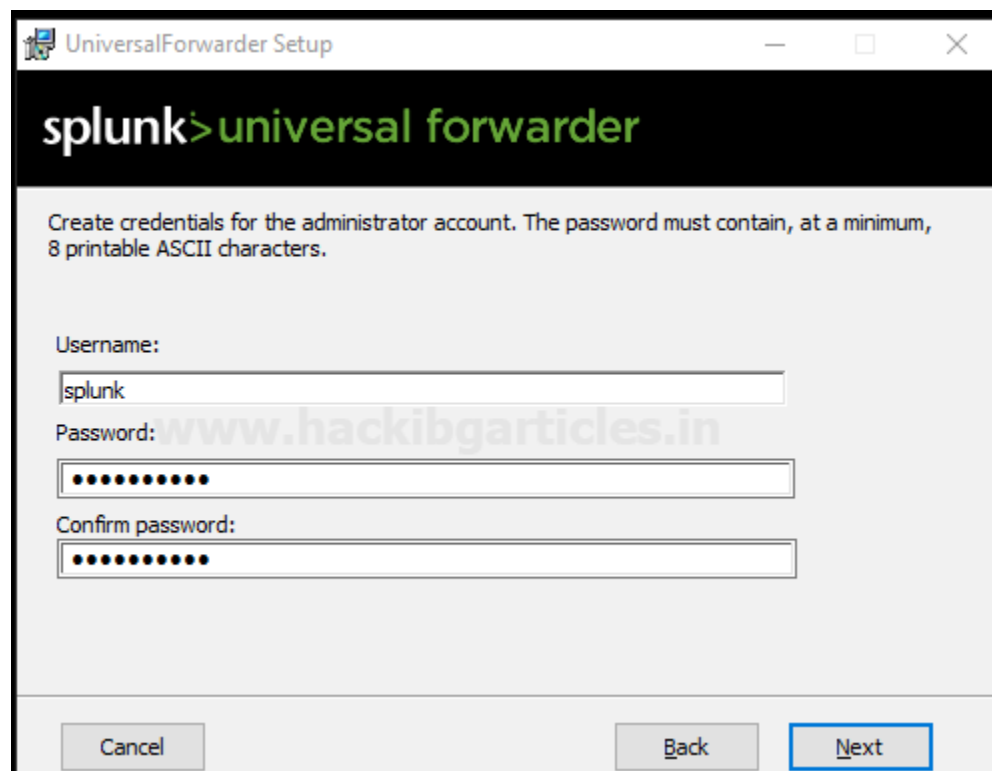


Then, it will ask you to select the applications or log files that you want to forward to Splunk Enterprise or receiver and then proceed with the next option as shown below.





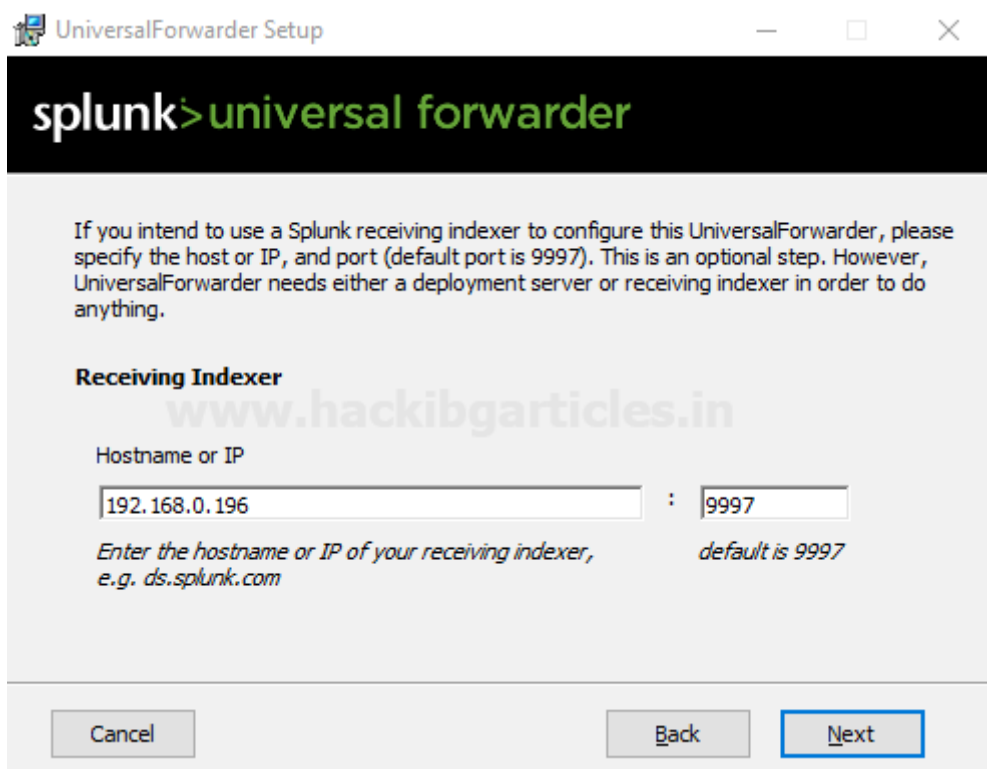
In the next dialogue, it will ask you to create credentials for the administrator account to encrypt all your files on Splunk Enterprise.



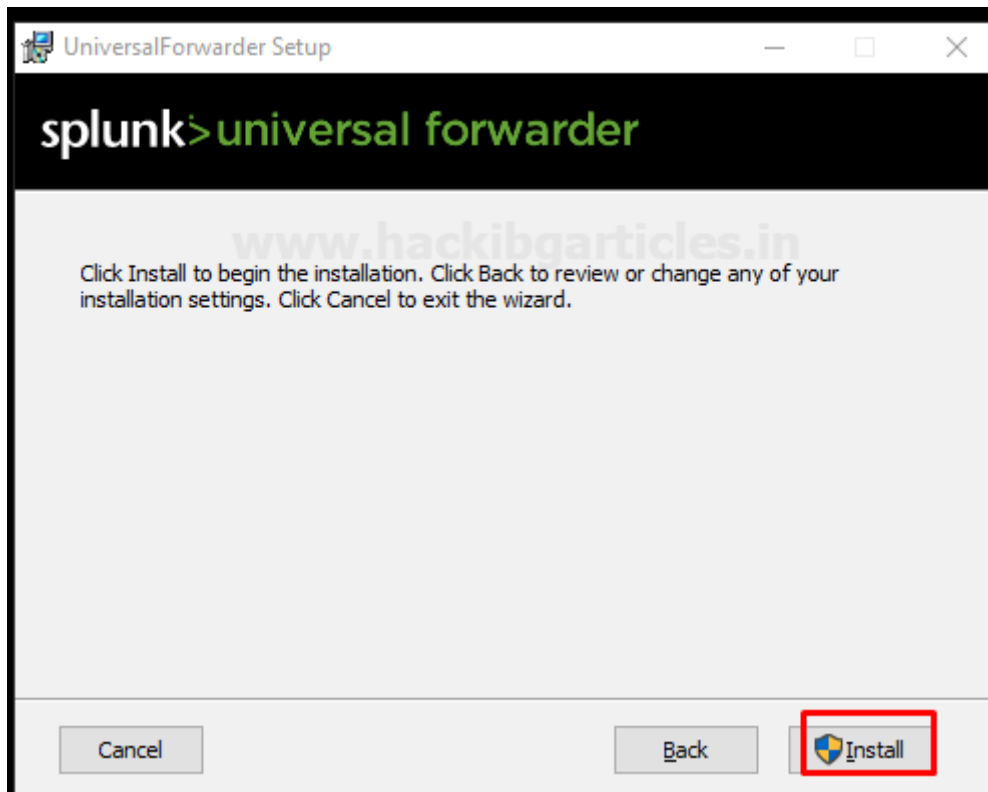
On the next dialogue, it will be (optional) to configure your forwarder as a deployment server if you choose it then enter the hostname or IP address and management port for your deployment server and click next

In my case, I will leave it blank and prefer to go with the next option.

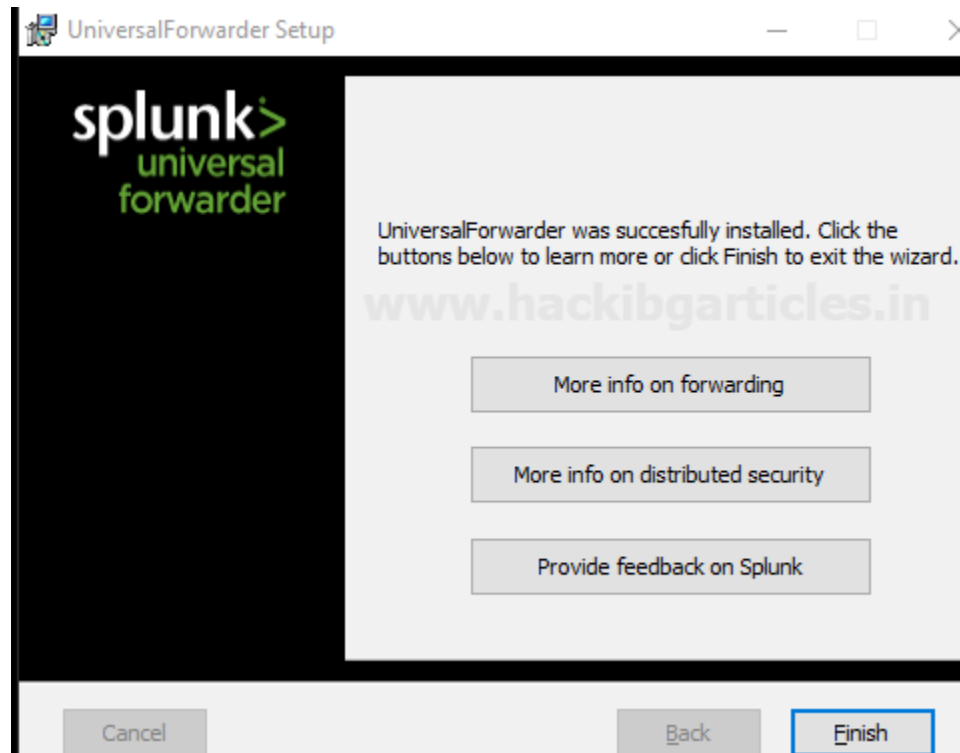
On the next dialogue setup Receiving indexer by entering the Hostname or IP and port as shown below



And then finally select option Install it will install Splunk forwarder in your windows environment



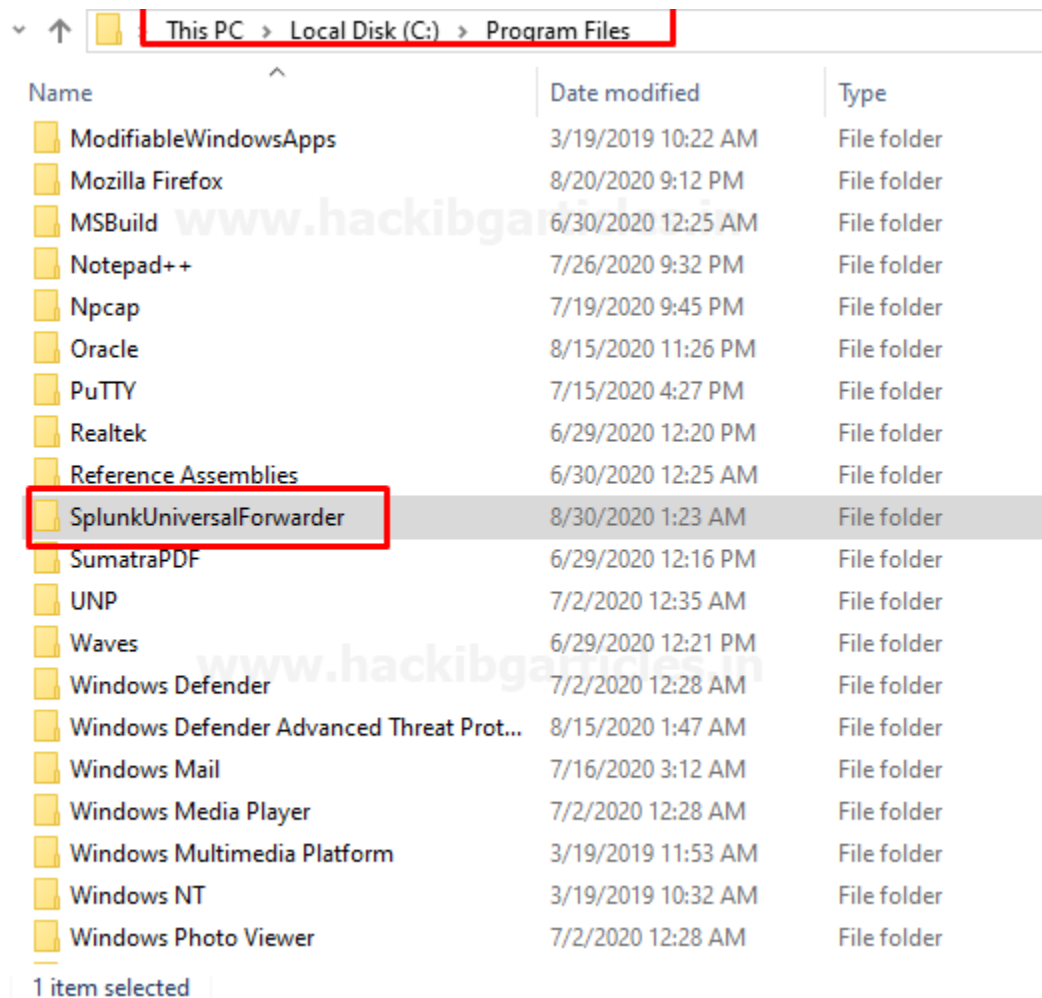
After that finish, the installation process.



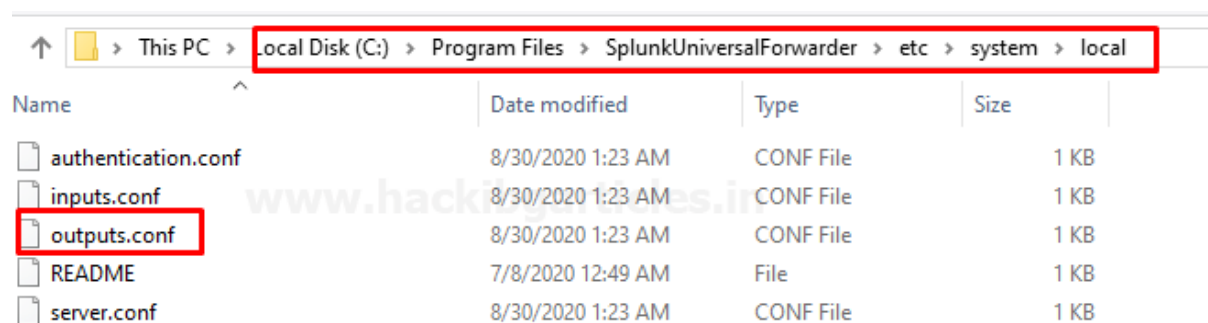
Let's verify the output.conf file to check if it is forwarded to the Receiver or not.

To do this follow the steps as described below.

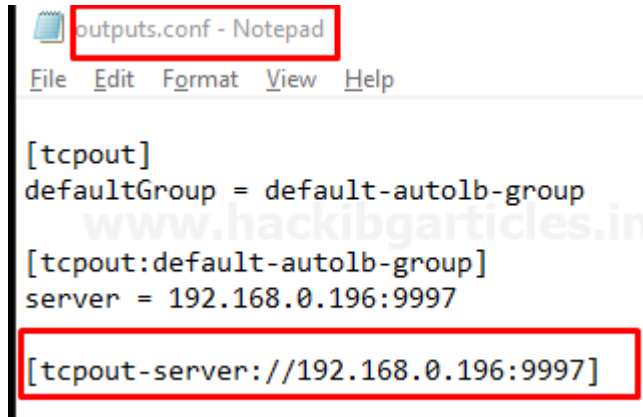
Go to file manager and open the directory where Splunk Universal forwarder installed.



Open the file SplunkUniversalForwarder file and then open the output.conf file it will be found in under **etc > system > local**



By opening it we can verify it either it is redirected to the correct IP or not as entered during the installation process if not you can make changes by editing it.



```
outputs.conf - Notepad
File Edit Format View Help

[tcpout]
defaultGroup = default-autolb-group

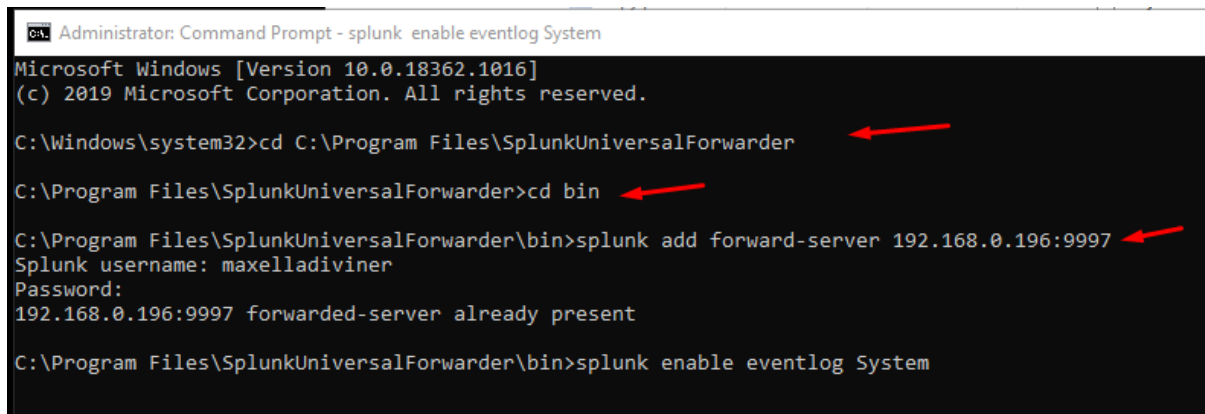
[tcpout:default-autolb-group]
server = 192.168.0.196:9997

[tcpout-server://192.168.0.196:9997]
```

### Configure Universal Forwarder to Send Data to Splunk Enterprise

Open CMD as Admin privilege and follow the steps described below:

```
cd c:\Program Files\SplunkUniversalForwarder
cd bin
splunk add-forward-server 192.168.0.196:9997
splunk enable eventlog system
splunk restart
```



```
Administrator: Command Prompt - splunk enable eventlog System
Microsoft Windows [Version 10.0.18362.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Program Files\SplunkUniversalForwarder
C:\Program Files\SplunkUniversalForwarder>cd bin
C:\Program Files\SplunkUniversalForwarder\bin>splunk add forward-server 192.168.0.196:9997
Splunk username: maxelladiviner
Password:
192.168.0.196:9997 forwarded-server already present
C:\Program Files\SplunkUniversalForwarder\bin>splunk enable eventlog System
```

Congratulations! You have successfully added Windows as a client

Let's check what happens to the Splunk GUI interface is it added or not

**host** X

2 Values, 100% of events Selected

**Reports**

Top values Top values by time Rare values

Events with this field

Values	Count	%
ubuntu	12,522	91.268%
DESKTOP-A0AP00M	1,198	8.732%

As you can see our client is successfully added

Now search your client into Search and reporting application by simply running a query `index="main"`

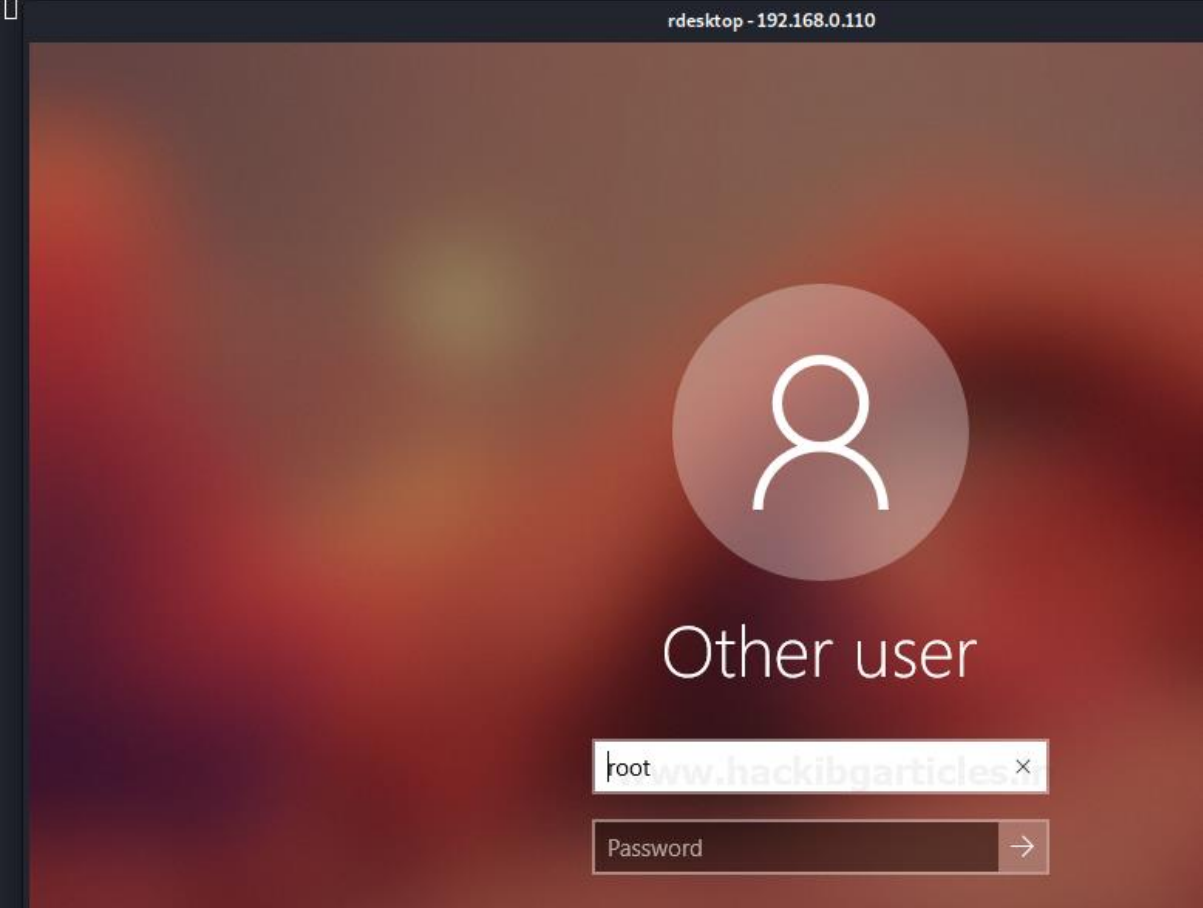
i	Time	Event
>	8/29/20 1:04:20.000 PM	08/30/2020 01:34:20.941 +0530 collection="Available Memory" object=Memory counter="Available Bytes" instance=0 <a href="#">Show all 6 lines</a> <b>host = DESKTOP-A0AP00M</b>   source = Perfmon:Available Memory sourcetype = Perfmon:Available Memory
>	8/29/20 1:04:20.000 PM	08/30/2020 01:34:20.939 +0530 collection="Network Interface" object="Network Interface" counter="Bytes Sent/sec" instance="Intel[R] Ethernet Connection [5] I219-LM" <a href="#">Show all 6 lines</a> <b>host = DESKTOP-A0AP00M</b>   source = Perfmon:Network Interface sourcetype = Perfmon:Network Interface
>	8/29/20 1:04:20.000 PM	08/30/2020 01:34:20.939 +0530 collection="Network Interface" object="Network Interface" counter="Bytes Received/sec"

## Windows Log Monitoring

Let's check it shows or not suspicious activity happened on our client end

To do this I am going take RDP session of my client

```
root@kali:~# rdesktop 192.168.0.110
Autoselecting keyboard map 'en-us' from locale
Core(warning): Certificate received from server is NOT trusted by this system, an exception has b
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has b
Connection established using SSL.
```



Now I have an RDP session of my Client let's check what happens on Splunk web



```

8/29/20      08/30/2020 01:40:21 AM
1:10:21.000 PM LogName=System
               SourceName=Microsoft-Windows-TerminalServices-RemoteConnectionManager
               EventCode=1056
               EventType=4
               Type=Information
               ComputerName=DESKTOP-A0AP00M
               TaskCategory=None
               OpCode=The operation completed successfully.
               RecordNumber=9894
               Keywords=Classic
               Message=A new self signed certificate to be used for RD Session Host Server authentication c
               rtificate is in the event data.
               Collapse
               host = DESKTOP-A0AP00M | source = WinEventLog:System | sourcetype = WinEventLog:System

```

Whoa! It works.

Great!

Now you can Dig down deeper it with running search Queries.

## Threat Monitoring

Let's monitor what illegal or suspicious activity happens on your client end or server

To do this I am going to perform a brute-force attack with the help of an Attacker machine:  
Kali Linux

To perform this attack run the following command below.

```
hydra -L user.txt -P pass.txt 192.168.0.196 ssh
```

where 192.168.0.196 is my client-server IP





```

root@kali:~# hydra -L user.txt -P pass.txt 192.168.0.196 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret se

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-08-29 15:29:34
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recomm
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), ~3 t
[DATA] attacking ssh://192.168.0.196:22/
[22][ssh] host: 192.168.0.196 login: raj password: 123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-08-29 15:29:41
root@kali:~#

```

Let's check what happens to Splunk web

hold tight! It's gonna a little bit special

Run a Query in the Application search and Reporting "sshd: session" and then see

i	Time	Event
>	8/29/20 12:38:00.000 PM	Aug 29 12:38:00 ubuntu sshd[7943]: Connection closed by invalid user paras 192.168.0.147 port 56450 [preauth] host = ubuntu   source = /var/log/auth.log   sourcetype = auth
>	8/29/20 12:37:59.000 PM	Aug 29 12:37:59 ubuntu sshd[8035]: Connection closed by invalid user jeenali 192.168.0.147 port 56492 [preauth] host = ubuntu   source = /var/log/auth.log   sourcetype = auth
>	8/29/20 12:37:59.000 PM	Aug 29 12:37:59 ubuntu sshd[7961]: Connection closed by authenticating user raj 192.168.0.147 port 56482 [preauth] host = ubuntu   source = /var/log/auth.log   sourcetype = auth
>	8/29/20 12:37:59.000 PM	Aug 29 12:37:59 ubuntu sshd[7957]: Connection closed by authenticating user raj 192.168.0.147 port 56476 [preauth] host = ubuntu   source = /var/log/auth.log   sourcetype = auth
>	8/29/20 12:37:59.000 PM	Aug 29 12:37:59 ubuntu sshd[7958]: Connection closed by authenticating user raj 192.168.0.147 port 56478 [preauth] host = ubuntu   source = /var/log/auth.log   sourcetype = auth

As we can see it have multiple invalid logins Attempts of invalid user.

Now you can monitor your whole Environment by using these steps.

## Conclusion

Hence, one can make use of these commands as a cybersecurity professional to assess vulnerabilities on systems and keep these systems away from threat.

## References

- <https://www.hackingarticles.in/siem-log-monitoring-lab-setup-with-splunk/>
- <https://www.hackingarticles.in/siem-windows-client-monitoring-with-splunk/>
- <https://docs.splunk.com/Documentation/Splunk/8.0.6/Data/MonitorActiveDirectory>