SOC Beginner Level Project

Linux Endpoint Monitoring using Splunk Forwarder

Saad Naveed

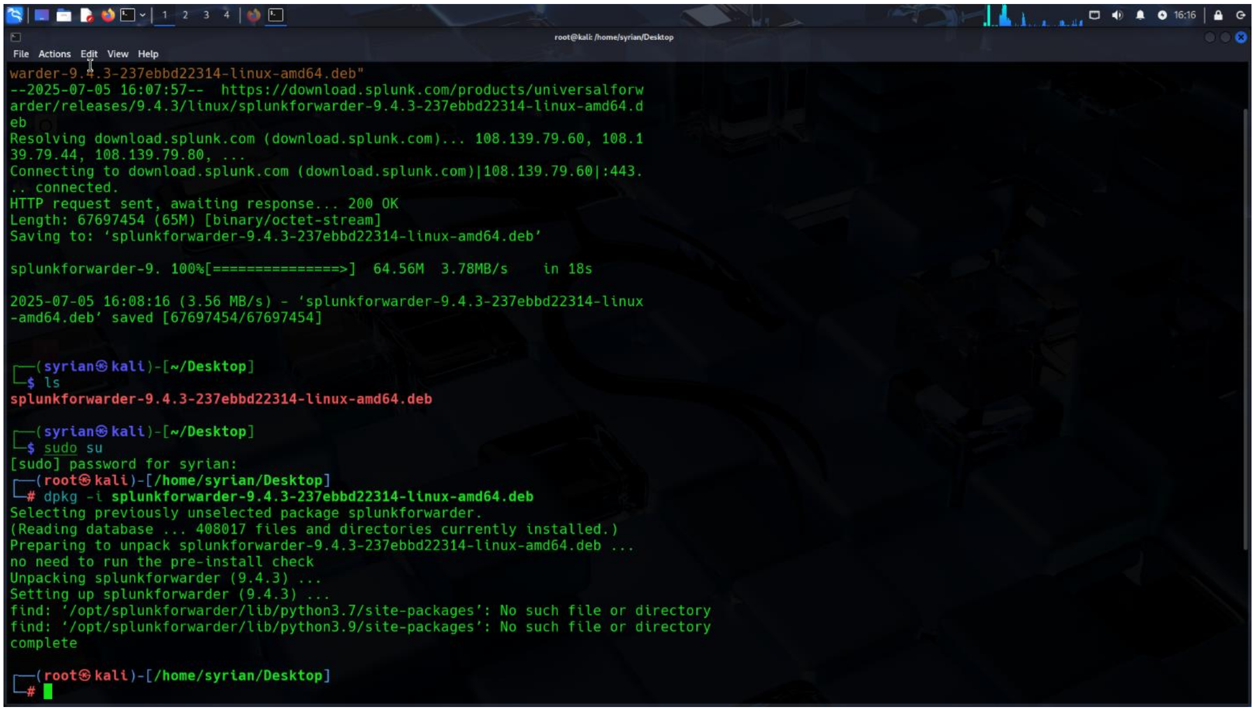
Cybersecurity & Digital Forensics

Date: 7th July 2025

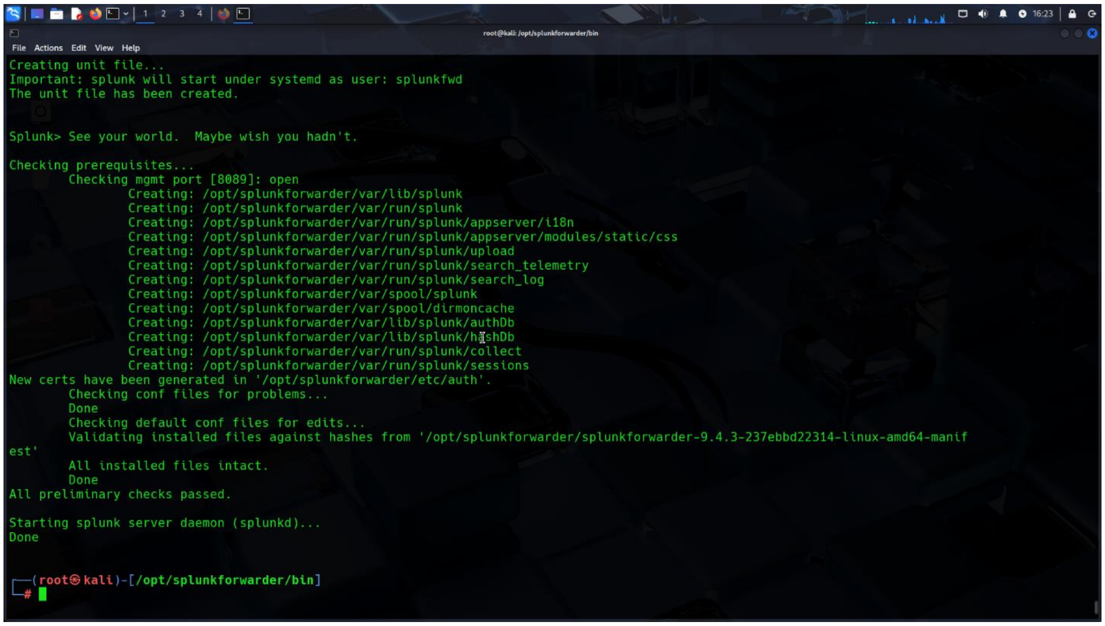
Project Objective

To set up and configure a basic SOC (Security Operations Center) environment by using Splunk Universal Forwarder on Kali Linux to monitor and forward system activity logs to a central Splunk Indexer for real-time visibility and analysis.

In this screenshot showing installation Splunk forwarder in Kali.



```
warder-9.4.3-237ebbd22314-linux-amd64.deb"
--2025-07-05 16:07:57--  https://download.splunk.com/products/universalforw
arder/releases/9.4.3/linux/splunkforwarder-9.4.3-237ebbd22314-linux-amd64.d
eb
Resolving download.splunk.com (download.splunk.com)... 108.139.79.60, 108.1
39.79.44, 108.139.79.80, ...
Connecting to download.splunk.com (download.splunk.com)|108.139.79.60|:443.
.. connected.
HTTP request sent, awaiting response... 200 OK
Length: 67697454 (65M) [binary/octet-stream]
Saving to: ‘splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb’

splunkforwarder-9. 100%[===============>]  64.56M  3.78MB/s    in 18s

2025-07-05 16:08:16 (3.56 MB/s) - ‘splunkforwarder-9.4.3-237ebbd22314-linux
-amd64.deb’ saved [67697454/67697454]


┌──(syrian㉿kali)-[~/Desktop]
└─$ ls
splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb

┌──(syrian㉿kali)-[~/Desktop]
└─$ sudo su
[sudo] password for syrian:
┌──(root㉿kali)-[/home/syrian/Desktop]
└─# dpkg -i splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb
Selecting previously unselected package splunkforwarder.
(Reading database ... 408017 files and directories currently installed.)
Preparing to unpack splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb ...
no need to run the pre-install check
Unpacking splunkforwarder (9.4.3) ...
Setting up splunkforwarder (9.4.3) ...
find: ‘/opt/splunkforwarder/lib/python3.7/site-packages’: No such file or directory
find: ‘/opt/splunkforwarder/lib/python3.9/site-packages’: No such file or directory
complete

┌──(root㉿kali)-[/home/syrian/Desktop]
└─#
```

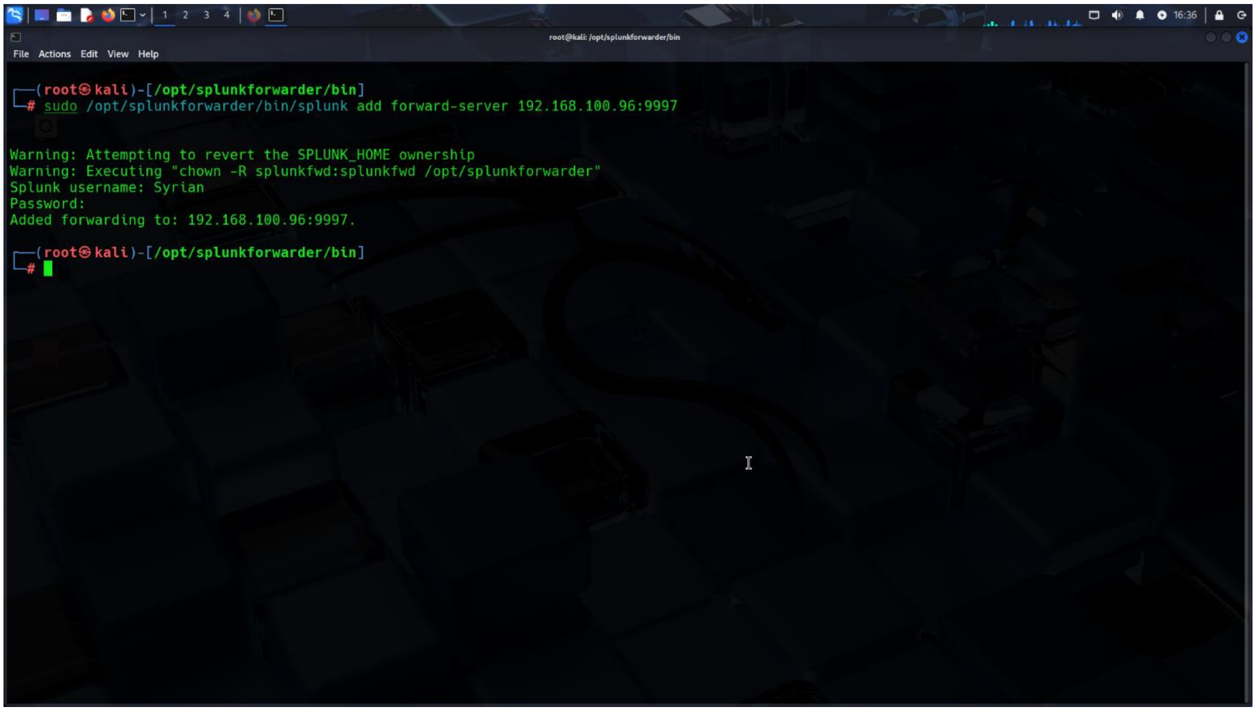


root@kali: /opt/splunkforwarder/bin
File Actions Edit View Help
16:23

```
Creating unit file...
Important: splunk will start under systemd as user: splunkfwd
The unit file has been created.


Splunk> See your world.  Maybe wish you hadn't.

Checking prerequisites...
        Checking mgmt port [8089]: open
                Creating: /opt/splunkforwarder/var/lib/splunk
                Creating: /opt/splunkforwarder/var/run/splunk
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
                Creating: /opt/splunkforwarder/var/run/splunk/upload
                Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
                Creating: /opt/splunkforwarder/var/run/splunk/search_log
                Creating: /opt/splunkforwarder/var/spool/splunk
                Creating: /opt/splunkforwarder/var/spool/dirmoncache
                Creating: /opt/splunkforwarder/var/lib/splunk/authDb
                Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
                Creating: /opt/splunkforwarder/var/run/splunk/collect
                Creating: /opt/splunkforwarder/var/run/splunk/sessions
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.4.3-237ebbd22314-linux-amd64-manif
est'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done


┌──(root㉿kali)-[/opt/splunkforwarder/bin]
└─#
```

This is my host windows machine Ip address: 192.168.100.96

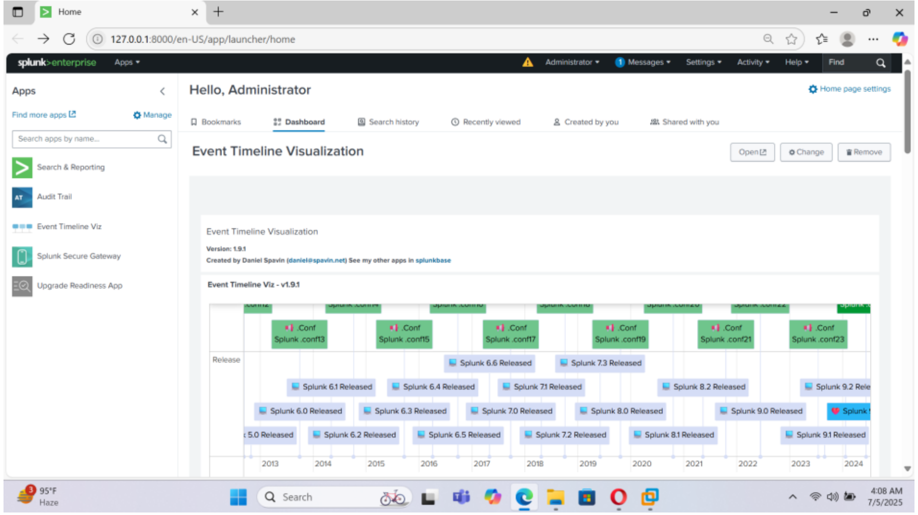
Now this ensere connection.



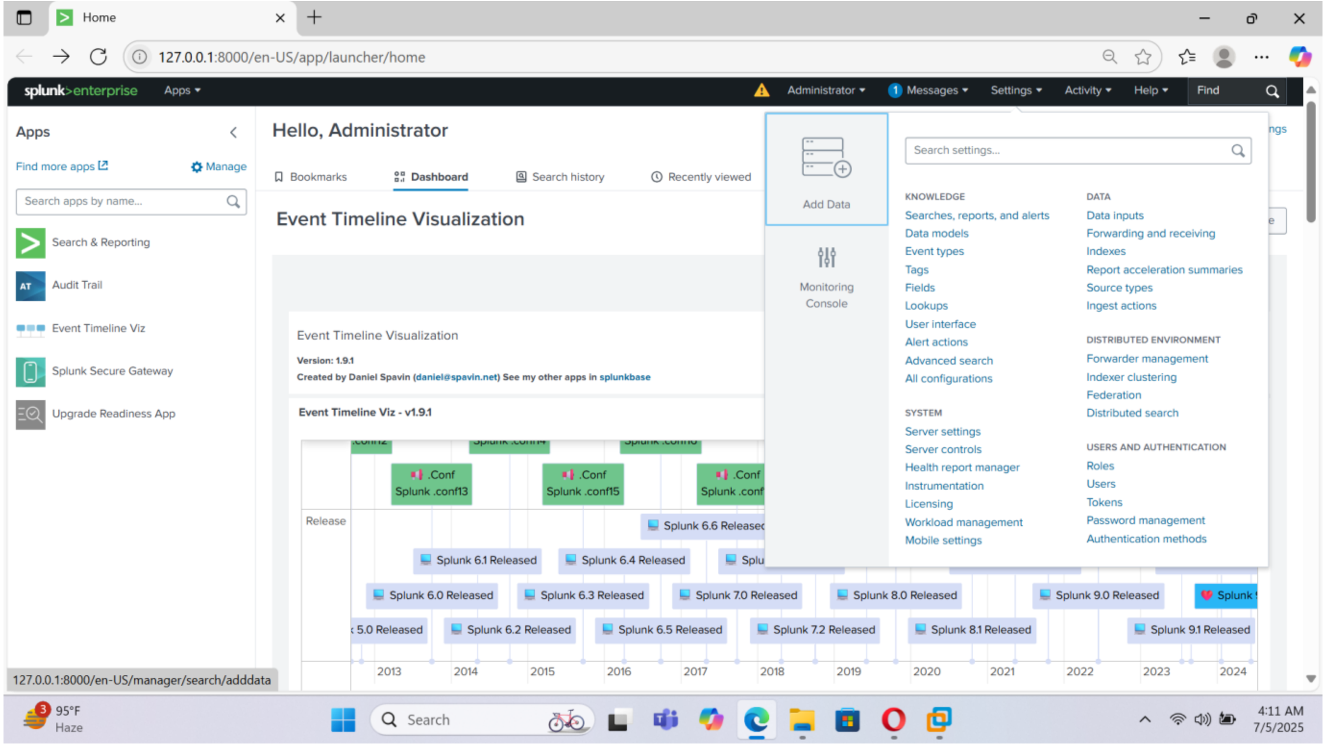
File Actions Edit View Help
root@kali: /opt/splunkforwarder/bin

```
┌──(root㉿kali)-[/opt/splunkforwarder/bin]
└─# sudo /opt/splunkforwarder/bin/splunk add forward-server 192.168.100.96:9997

Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Splunk username: Syrian
Password:
Added forwarding to: 192.168.100.96:9997.

┌──(root㉿kali)-[/opt/splunkforwarder/bin]
└─# 
```

Now I start Splunk in window machine.



And done some required setting click setting and select forwarding and receiving.



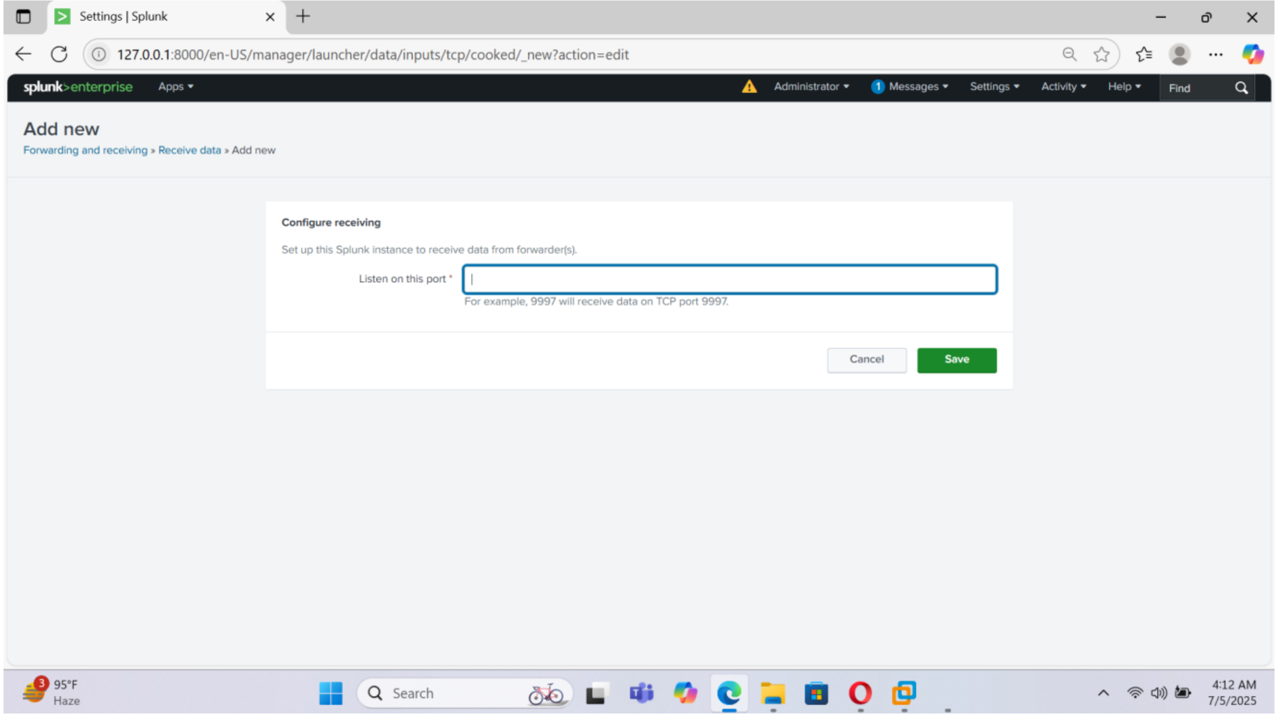
Event Timeline Visualization

Version: 1.9.1

Created by Daniel Spavin (daniel@spavin.net) See my other apps in splunkbase

Event Timeline Viz - v1.9.1

Now I entered port number that connect both.



Configure receiving

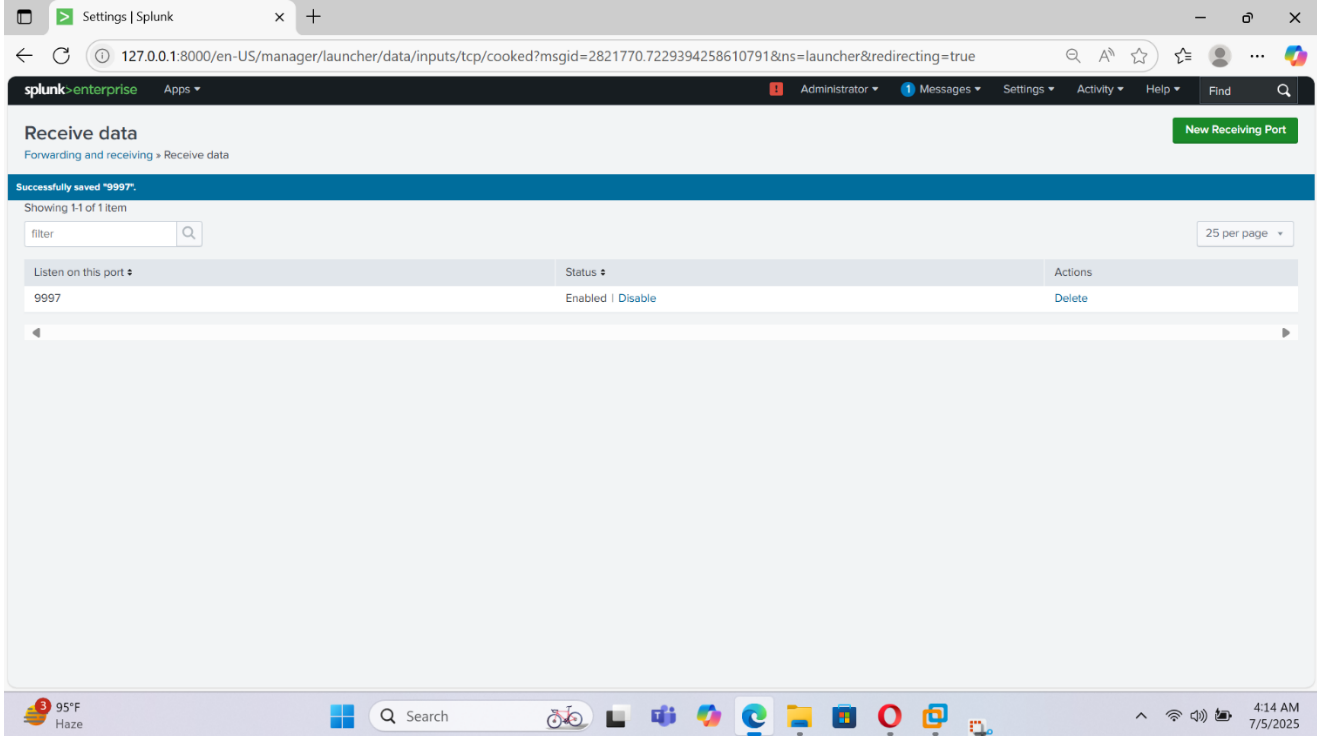
Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *

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

Click Configure receiving and then enter port (9997) and press save.

Now it’s done.



Receive data

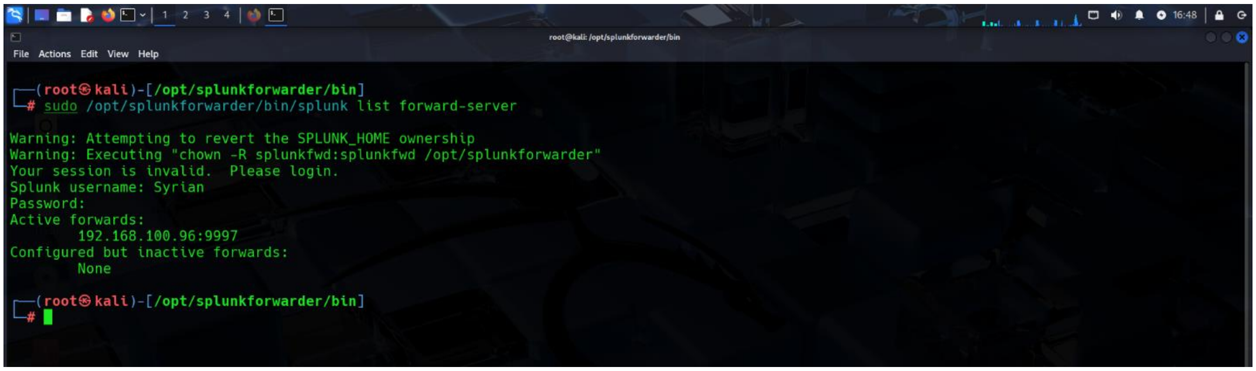
Forwarding and receiving » Receive data

Successfully saved "9997".

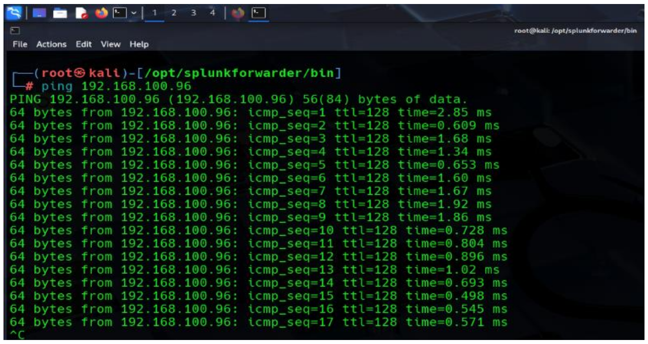
Showing 1-1 of 1 item

Listen on this port	Status	Actions
9997	Enabled | Disable	Delete

Now I checked Connection it’s establish or not.

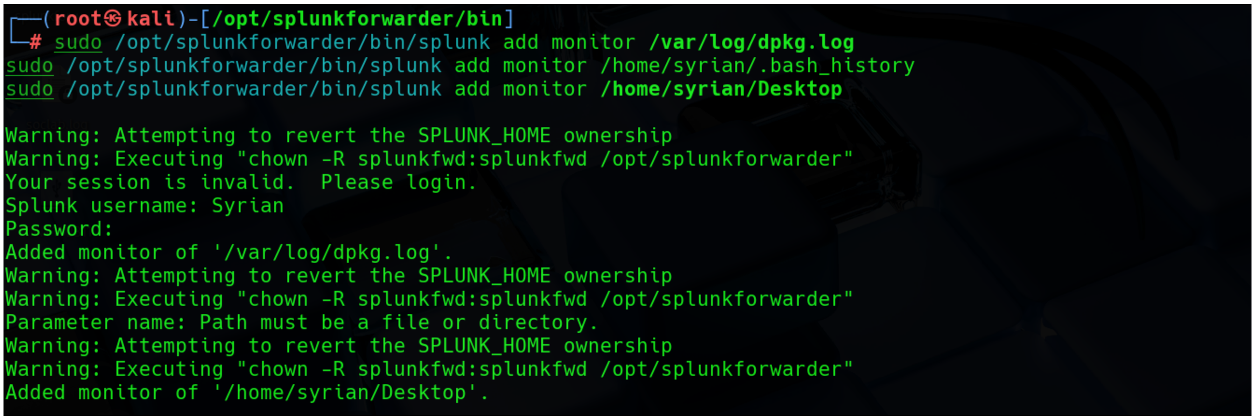


```
┌──(root㉿kali)-[/opt/splunkforwarder/bin]
└─# sudo /opt/splunkforwarder/bin/splunk list forward-server

Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid.  Please login.
Splunk username: Syrian
Password:
Active forwards:
        192.168.100.96:9997
Configured but inactive forwards:
        None

┌──(root㉿kali)-[/opt/splunkforwarder/bin]
└─#
```



```
┌──(root㉿kali)-[/opt/splunkforwarder/bin]
└─# ping 192.168.100.96
PING 192.168.100.96 (192.168.100.96) 56(84) bytes of data.
64 bytes from 192.168.100.96: icmp_seq=1 ttl=128 time=2.85 ms
64 bytes from 192.168.100.96: icmp_seq=2 ttl=128 time=0.609 ms
64 bytes from 192.168.100.96: icmp_seq=3 ttl=128 time=1.68 ms
64 bytes from 192.168.100.96: icmp_seq=4 ttl=128 time=1.34 ms
64 bytes from 192.168.100.96: icmp_seq=5 ttl=128 time=0.653 ms
64 bytes from 192.168.100.96: icmp_seq=6 ttl=128 time=1.60 ms
64 bytes from 192.168.100.96: icmp_seq=7 ttl=128 time=1.67 ms
64 bytes from 192.168.100.96: icmp_seq=8 ttl=128 time=1.92 ms
64 bytes from 192.168.100.96: icmp_seq=9 ttl=128 time=1.86 ms
64 bytes from 192.168.100.96: icmp_seq=10 ttl=128 time=0.728 ms
64 bytes from 192.168.100.96: icmp_seq=11 ttl=128 time=0.804 ms
64 bytes from 192.168.100.96: icmp_seq=12 ttl=128 time=0.896 ms
64 bytes from 192.168.100.96: icmp_seq=13 ttl=128 time=1.02 ms
64 bytes from 192.168.100.96: icmp_seq=14 ttl=128 time=0.693 ms
64 bytes from 192.168.100.96: icmp_seq=15 ttl=128 time=0.498 ms
64 bytes from 192.168.100.96: icmp_seq=16 ttl=128 time=0.545 ms
64 bytes from 192.168.100.96: icmp_seq=17 ttl=128 time=0.571 ms
^C
```

Now Generate Log.



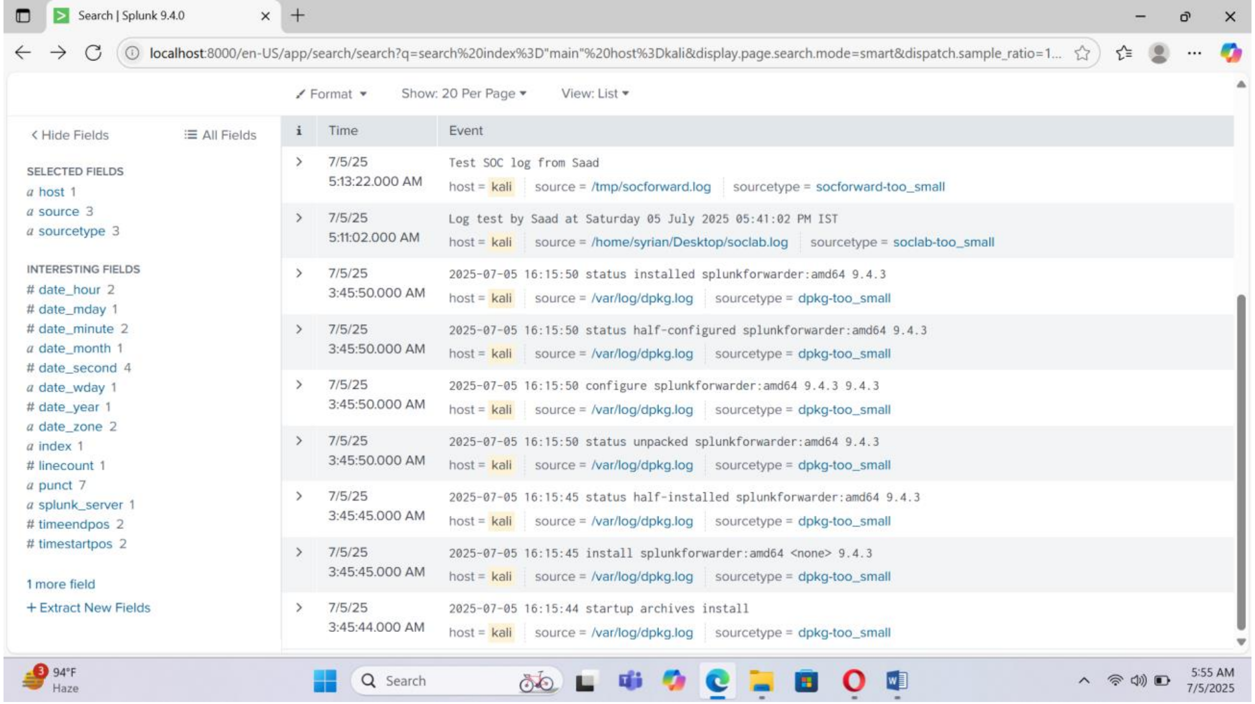
```
┌──(root㉿kali)-[/opt/splunkforwarder/bin]
└─# sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/dpkg.log
sudo /opt/splunkforwarder/bin/splunk add monitor /home/syrian/.bash_history
sudo /opt/splunkforwarder/bin/splunk add monitor /home/syrian/Desktop

Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid.  Please login.
Splunk username: Syrian
Password:
Added monitor of '/var/log/dpkg.log'.
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Parameter name: Path must be a file or directory.
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/home/syrian/Desktop'.
```

And now open Splunk and run this.

index="main" host=kali

This query will return

- All logs that were forwarded from your **Kali machine**
- But **only** those that were saved into the **main index**


Search | Splunk 9.4.0
localhost:8000/en-US/app/search/search?q=search%20index%3D"main"%20host%3Dkali&display.page.search.mode=smart&dispatch.sample_ratio=1...
Format
Show: 20 Per Page
View: List
< Hide Fields
All Fields
94°F
Haze
Search
5:55 AM
7/5/2025

SELECTED FIELDS
a host 1
a source 3
a sourcetype 3

INTERESTING FIELDS
# date_hour 2
# date_mday 1
# date_minute 2
a date_month 1
# date_second 4
a date_wday 1
# date_year 1
a date_zone 2
a index 1
# linecount 1
a punct 7
a splunk_server 1
# timeendpos 2
# timestartpos 2

1 more field
+ Extract New Fields

i	Time	Event
>	7/5/25 5:13:22.000 AM	Test SOC log from Saad host = kali source = /tmp/socforward.log sourcetype = socforward-too_small
>	7/5/25 5:11:02.000 AM	Log test by Saad at Saturday 05 July 2025 05:41:02 PM IST host = kali source = /home/syrian/Desktop/soclab.log sourcetype = soclab-too_small
>	7/5/25 3:45:50.000 AM	2025-07-05 16:15:50 status installed splunkforwarder:amd64 9.4.3 host = kali source = /var/log/dpkg.log sourcetype = dpkg-too_small
>	7/5/25 3:45:50.000 AM	2025-07-05 16:15:50 status half-configured splunkforwarder:amd64 9.4.3 host = kali source = /var/log/dpkg.log sourcetype = dpkg-too_small
>	7/5/25 3:45:50.000 AM	2025-07-05 16:15:50 configure splunkforwarder:amd64 9.4.3 9.4.3 host = kali source = /var/log/dpkg.log sourcetype = dpkg-too_small
>	7/5/25 3:45:50.000 AM	2025-07-05 16:15:50 status unpacked splunkforwarder:amd64 9.4.3 host = kali source = /var/log/dpkg.log sourcetype = dpkg-too_small
>	7/5/25 3:45:45.000 AM	2025-07-05 16:15:45 status half-installed splunkforwarder:amd64 9.4.3 host = kali source = /var/log/dpkg.log sourcetype = dpkg-too_small
>	7/5/25 3:45:45.000 AM	2025-07-05 16:15:45 install splunkforwarder:amd64 <none> 9.4.3 host = kali source = /var/log/dpkg.log sourcetype = dpkg-too_small
>	7/5/25 3:45:44.000 AM	2025-07-05 16:15:44 startup archives install host = kali source = /var/log/dpkg.log sourcetype = dpkg-too_small

Kali machine logs like software installations and test entries are successfully reaching your Splunk system and are being correctly indexed and searchable.