King Fahad University of Petroleum and Minerals

ICS344 Project Report

Group number: 06

Section: F08

Phase2

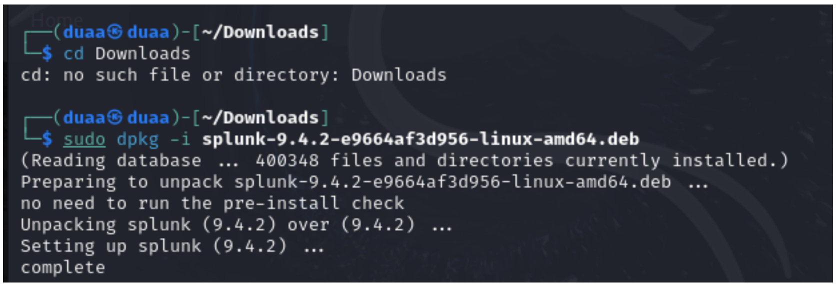
Duaa Alhassan	Zainab Almaskeen.	Renad Alqahtani
202168790	202175370	202169930

3/5/2025

Phase 2: Visual Analysis with a SIEM Dashboard

The goal of Phase 2 is to use a SIEM platform, specifically Splunk, to collect, visualize, and analyze logs from the victim machine (Metasploitable3) to gain insights into the SSH brute-force attacks performed in Phase 1.

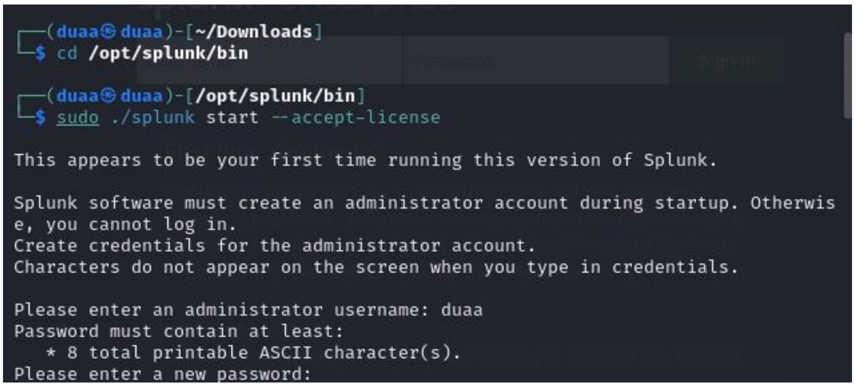
1- Splunk Installation (on Attacker Machine - Kali Linux):



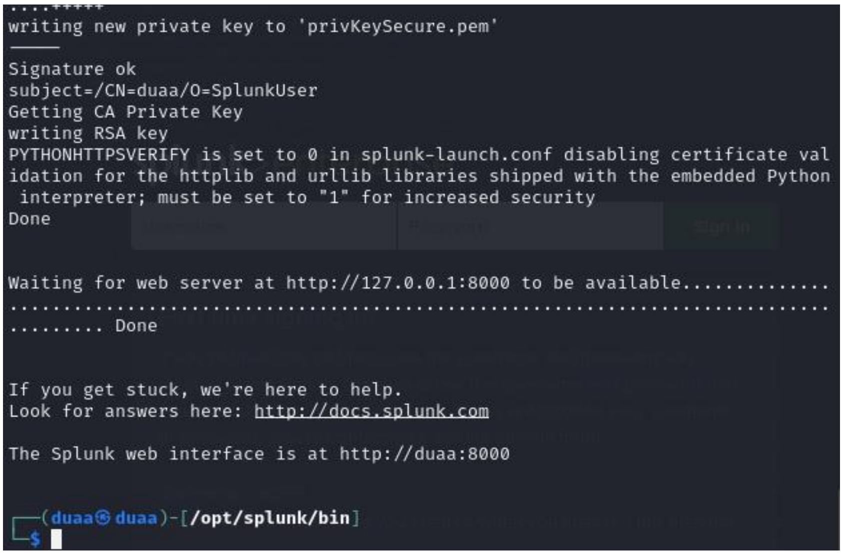
```
┌──(duaa㉿duaa)-[~/Downloads]
└─$ cd Downloads
cd: no such file or directory: Downloads

┌──(duaa㉿duaa)-[~/Downloads]
└─$ sudo dpkg -i splunk-9.4.2-e9664af3d956-linux-amd64.deb
(Reading database ... 400348 files and directories currently installed.)
Preparing to unpack splunk-9.4.2-e9664af3d956-linux-amd64.deb ...
no need to run the pre-install check
Unpacking splunk (9.4.2) over (9.4.2) ...
Setting up splunk (9.4.2) ...
complete
```

Then start Splunk with the following command:

- cd /opt/splunk/bin
- sudo ./splunk start --accept-license



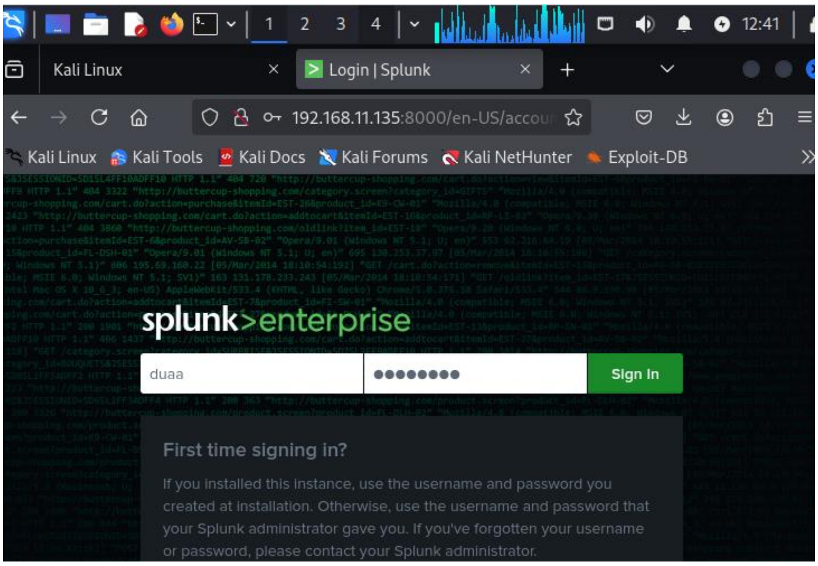
```
┌──(duaa㉿duaa)-[~/Downloads]
└─$ cd /opt/splunk/bin

┌──(duaa㉿duaa)-[/opt/splunk/bin]
└─$ sudo ./splunk start --accept-license

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

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

Please enter an administrator username: duaa
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
```



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


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


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

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


┌──(duaa㉿duaa)-[/opt/splunk/bin]
└─$ 
```

Then open web browser and type: http://<your_machine_IP>:8000 as: : http://192.168.11.135:8000

Then you will see splunk opened, log in with the administrator credentials you set during installation.

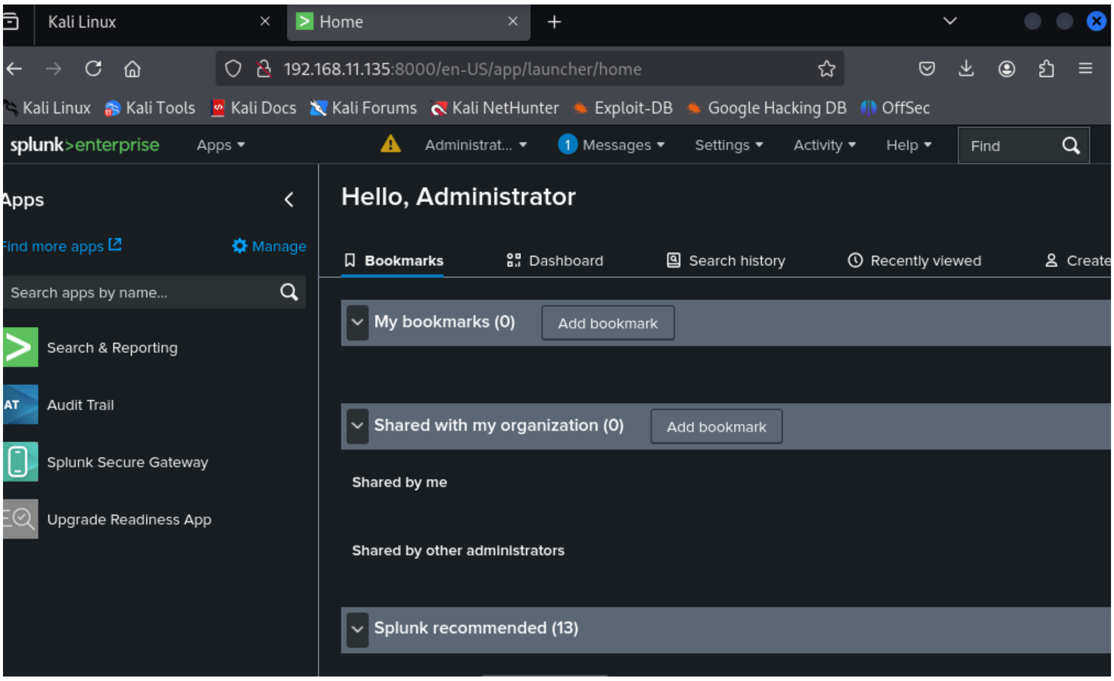


duaa

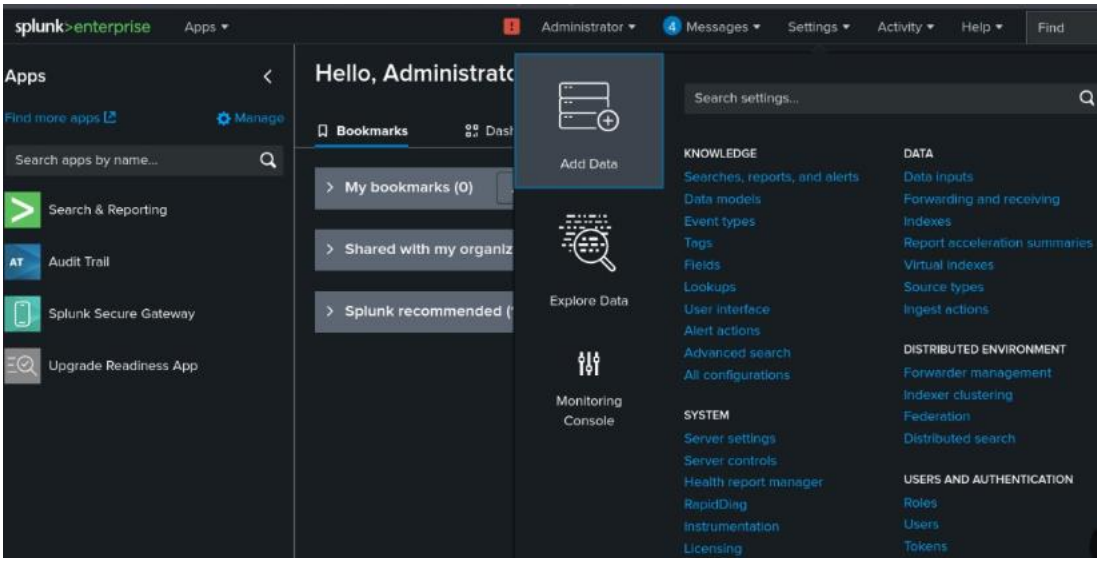
●●●●●●●●

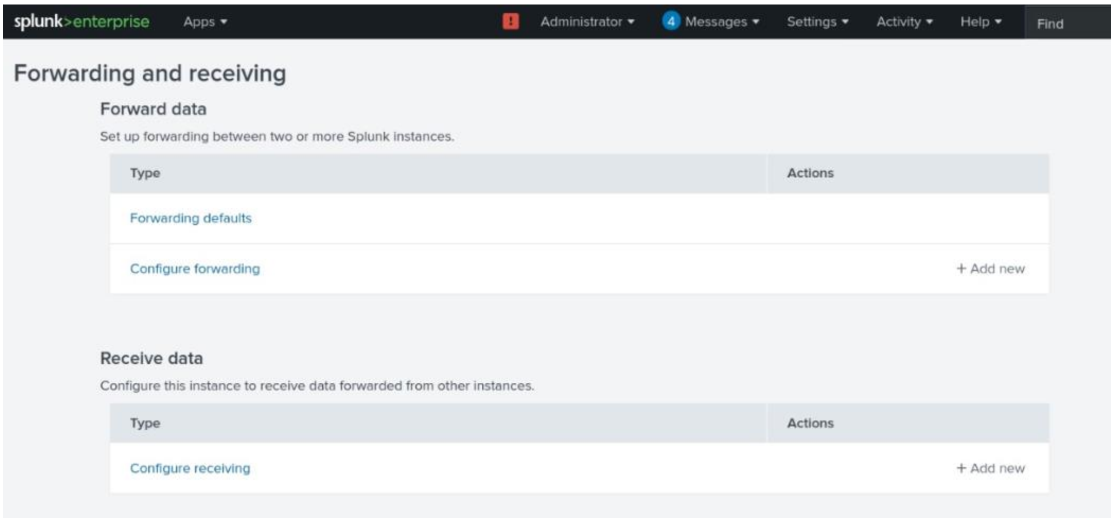
First time signing in?

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 username or password, please contact your Splunk administrator.



2- Configuring Splunk to Receive Logs as:





Forwarding and receiving

Forward data

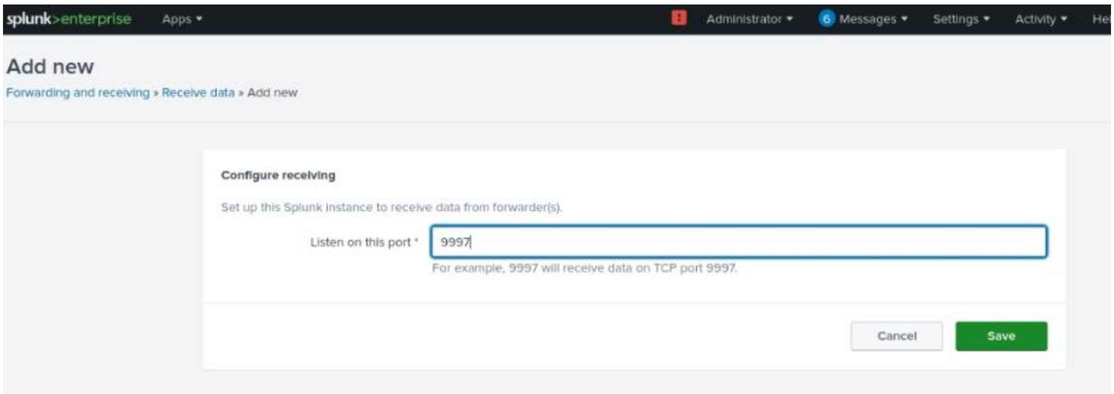
Set up forwarding between two or more Splunk instances.

Type	Actions
Forwarding defaults	
Configure forwarding	+ Add new

Receive data

Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new



Add new

Forwarding and receiving » Receive data » Add new

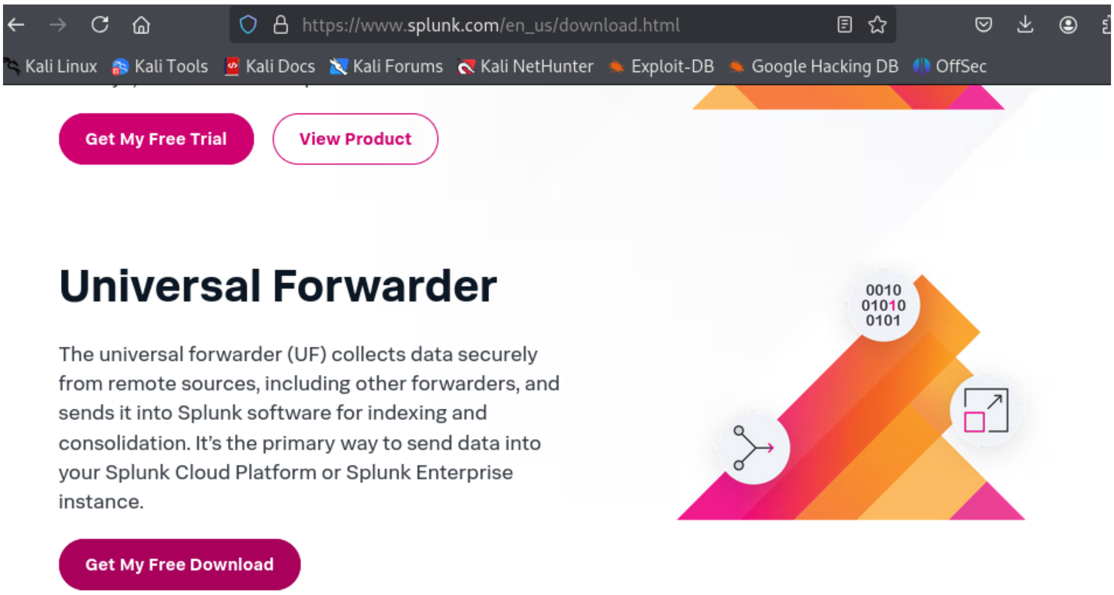
Configure receiving

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.

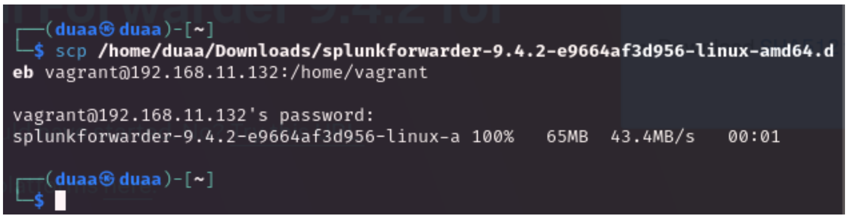
3- Download the Splunk Universal Forwarder:



Universal Forwarder

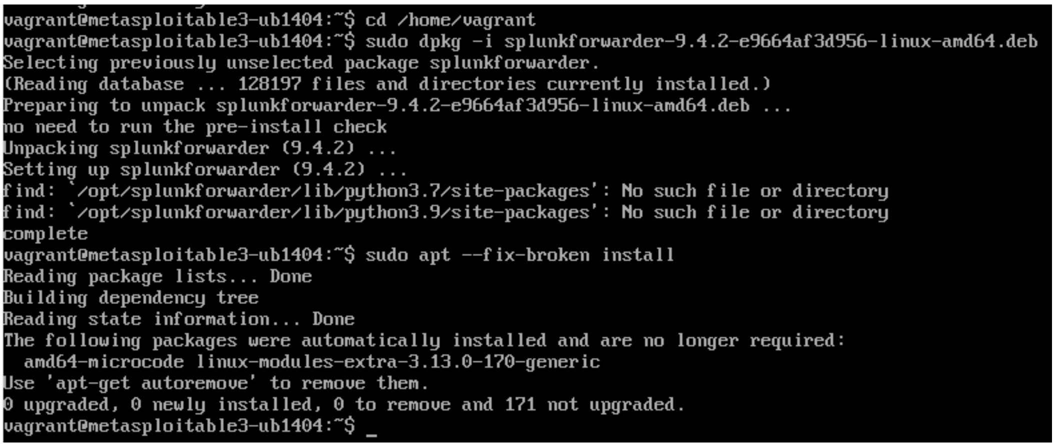
The universal forwarder (UF) collects data securely from remote sources, including other forwarders, and sends it into Splunk software for indexing and consolidation. It's the primary way to send data into your Splunk Cloud Platform or Splunk Enterprise instance.

4- Transfer the Package from kali to Metasploitable3:



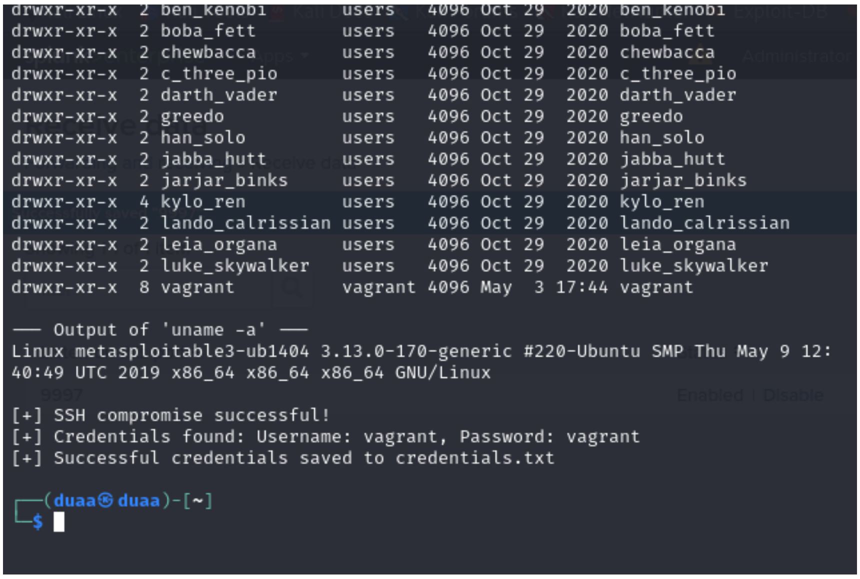
```
┌──(duaa㉿duaa)-[~]
└─$ scp /home/duaa/Downloads/splunkforwarder-9.4.2-e9664af3d956-linux-amd64.d
eb vagrant@192.168.11.132:/home/vagrant

vagrant@192.168.11.132's password:
splunkforwarder-9.4.2-e9664af3d956-linux-a 100%   65MB  43.4MB/s   00:01

┌──(duaa㉿duaa)-[~]
└─$ █
```

Then install the package on matasploitable3 by running the following commands:



```
vagrant@metasploitable3-ub1404:~$ cd /home/vagrant
vagrant@metasploitable3-ub1404:~$ sudo dpkg -i splunkforwarder-9.4.2-e9664af3d956-linux-amd64.deb
Selecting previously unselected package splunkforwarder.
(Reading database ... 128197 files and directories currently installed.)
Preparing to unpack splunkforwarder-9.4.2-e9664af3d956-linux-amd64.deb ...
no need to run the pre-install check
Unpacking splunkforwarder (9.4.2) ...
Setting up splunkforwarder (9.4.2) ...
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
vagrant@metasploitable3-ub1404:~$ sudo apt --fix-broken install
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  amd64-microcode linux-modules-extra-3.13.0-170-generic
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 171 not upgraded.
vagrant@metasploitable3-ub1404:~$ _
```

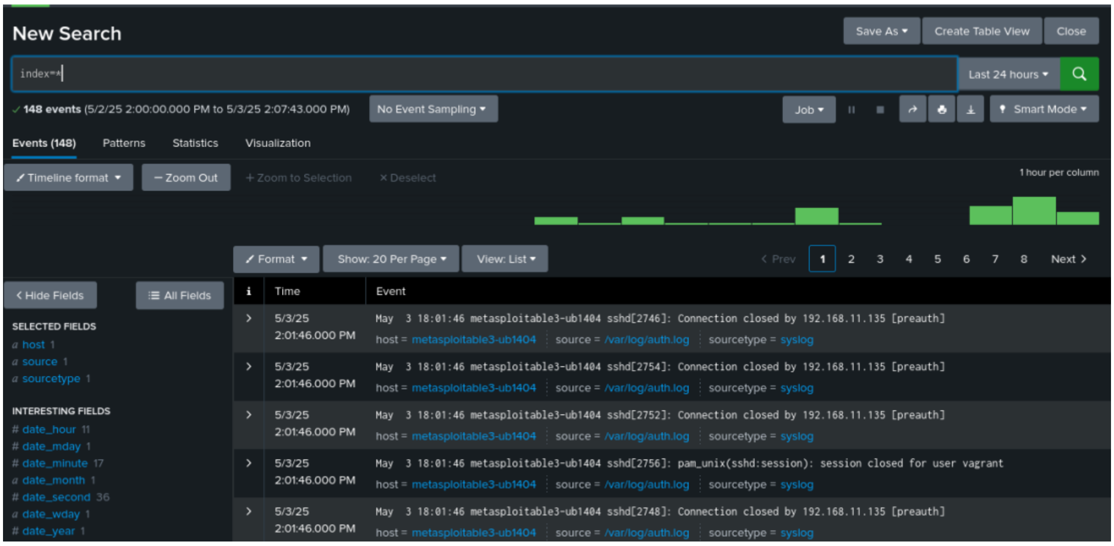
5- Executing Custom SSH Brute Force Script:



```
drwxr-xr-x  2 ben_kenobi        users   4096 Oct 29  2020 ben_kenobi
drwxr-xr-x  2 boba_fett         users   4096 Oct 29  2020 boba_fett
drwxr-xr-x  2 chewbacca         users   4096 Oct 29  2020 chewbacca
drwxr-xr-x  2 c_three_pio       users   4096 Oct 29  2020 c_three_pio
drwxr-xr-x  2 darth_vader       users   4096 Oct 29  2020 darth_vader
drwxr-xr-x  2 greedo            users   4096 Oct 29  2020 greedo
drwxr-xr-x  2 han_solo          users   4096 Oct 29  2020 han_solo
drwxr-xr-x  2 jabba_hutt        users   4096 Oct 29  2020 jabba_hutt
drwxr-xr-x  2 jarjar_binks      users   4096 Oct 29  2020 jarjar_binks
drwxr-xr-x  4 kylo_ren          users   4096 Oct 29  2020 kylo_ren
drwxr-xr-x  2 lando_calrissian  users   4096 Oct 29  2020 lando_calrissian
drwxr-xr-x  2 leia_organa       users   4096 Oct 29  2020 leia_organa
drwxr-xr-x  2 luke_skywalker    users   4096 Oct 29  2020 luke_skywalker
drwxr-xr-x  8 vagrant           vagrant 4096 May  3 17:44 vagrant

—— Output of 'uname -a' ——
Linux metasploitable3-ub1404 3.13.0-170-generic #220-Ubuntu SMP Thu May 9 12:
40:49 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux

[+] SSH compromise successful!
[+] Credentials found: Username: vagrant, Password: vagrant
[+] Successful credentials saved to credentials.txt

┌──(duaa㉿duaa)-[~]
└─$ █
```

6- Verify Splunk is Receiving Data:

By writing th e command index=* it tells Splunk to search across **all indexes** in my Splunk deployment.



New Search

```
index=*
```

✓ 148 events (5/2/25 2:00:00.000 PM to 5/3/25 2:07:43.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 11
# date_mday 1
# date_minute 17
a date_month 1
# date_second 36
a date_wday 1
# date_year 1

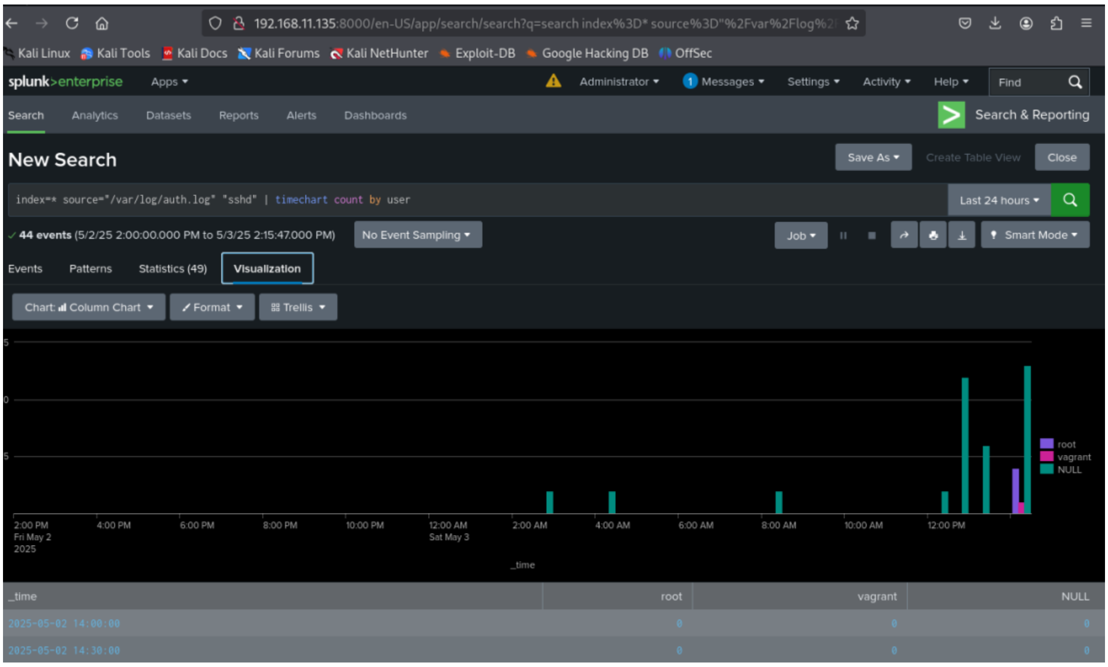
i	Time	Event
›	5/3/25 2:01:46.000 PM	May 3 18:01:46 metasploitable3-ub1404 sshd[2746]: Connection closed by 192.168.11.135 [preauth] host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog
›	5/3/25 2:01:46.000 PM	May 3 18:01:46 metasploitable3-ub1404 sshd[2754]: Connection closed by 192.168.11.135 [preauth] host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog
›	5/3/25 2:01:46.000 PM	May 3 18:01:46 metasploitable3-ub1404 sshd[2752]: Connection closed by 192.168.11.135 [preauth] host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog
›	5/3/25 2:01:46.000 PM	May 3 18:01:46 metasploitable3-ub1404 sshd[2756]: pam_unix(sshd:session): session closed for user vagrant host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog
›	5/3/25 2:01:46.000 PM	May 3 18:01:46 metasploitable3-ub1404 sshd[2748]: Connection closed by 192.168.11.135 [preauth] host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog

7- Visualizing the Attack Logs in Splunk:

To analyze the SSH brute-force attack conducted against the Metasploitable3 victim machine, Splunk's Search & Reporting dashboard was utilized to visualize the authentication events captured within the /var/log/auth.log file. The following Splunk query was executed to generate a time-based chart illustrating SSH activity:

index=* source="/var/log/auth.log" "sshd" | timechart count by user

The resulting visualization displayed a timeline of SSH activity, showing the frequency of events associated with different users. This allowed for the identification of patterns indicative of a brute-force attack, such as numerous failed login attempts for various users originating from the attacker machine's IP address, culminating in the successful login using the vagrant credentials. The time-based chart provided a clear visual representation of the attack's progression over time:

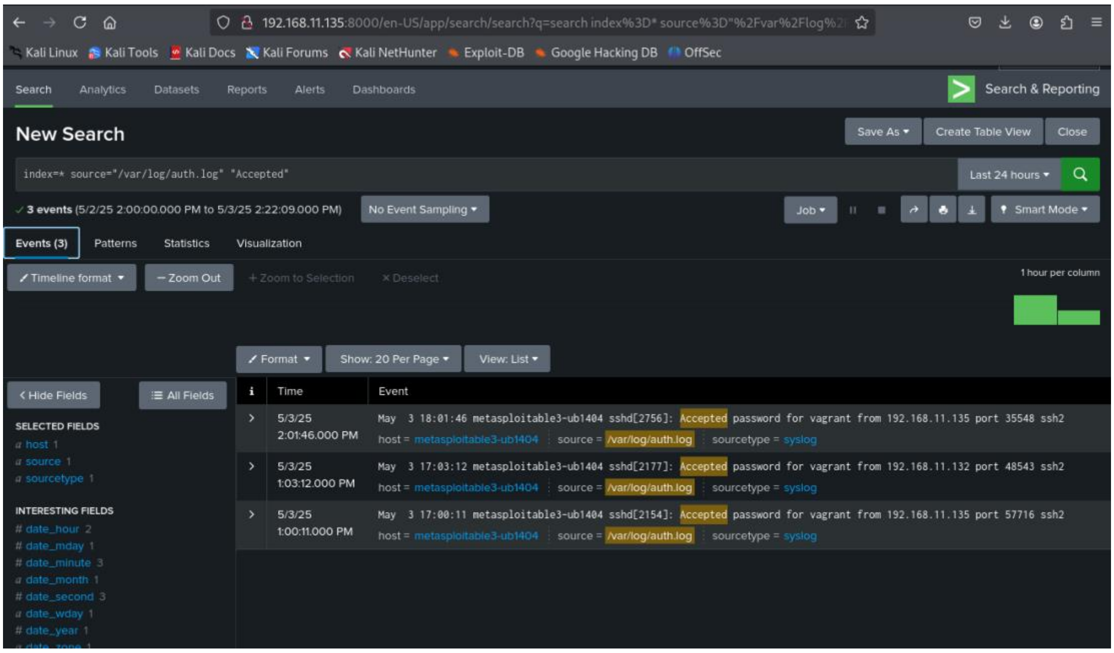


```
index=* source="/var/log/auth.log" "sshd" | timechart count by user
```

✓ 44 events (5/2/25 2:00:00.000 PM to 5/3/25 2:15:47.000 PM)

_time	root	vagrant	NULL
2025-05-02 14:00:00	0	0	0
2025-05-02 14:30:00	0	0	0

This Splunk search query also targets the /var/log/auth.log file but retrieves events containing the keyword "Accepted". These events represent successful SSH logins. Analyzing these logs can help track who logged in, from where, and at what time, which is crucial for identifying successful compromises or legitimate access:



```
index=* source="/var/log/auth.log" "Accepted"
```

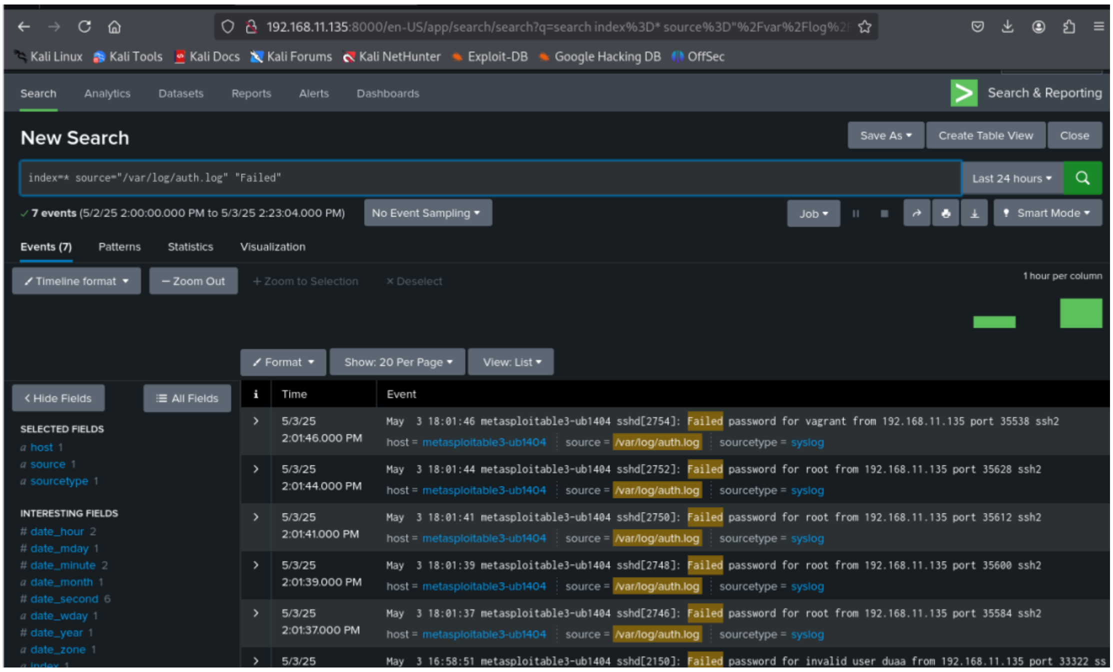
✓ 3 events (5/2/25 2:00:00.000 PM to 5/3/25 2:22:09.000 PM)

SELECTED FIELDS
host 1
source 1
sourcetype 1

INTERESTING FIELDS
date_hour 2
date_mday 1
date_minute 3
date_month 1
date_second 3
date_wday 1
date_year 1
date_zone 1

Time	Event
5/3/25 2:01:46.000 PM	May 3 18:01:46 metasploitable3-ub1404 sshd[2756]: Accepted password for vagrant from 192.168.11.135 port 35548 ssh2 host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog
5/3/25 1:03:12.000 PM	May 3 17:03:12 metasploitable3-ub1404 sshd[2177]: Accepted password for vagrant from 192.168.11.132 port 48543 ssh2 host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog
5/3/25 1:00:11.000 PM	May 3 17:00:11 metasploitable3-ub1404 sshd[2154]: Accepted password for vagrant from 192.168.11.135 port 57716 ssh2 host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog

This Splunk search query targets the /var/log/auth.log file (common location for SSH authentication logs on Linux systems) and retrieves all events within that log file that contain the keyword "Failed". This is useful for identifying unsuccessful login attempts, which are a key indicator of brute-force attacks or other unauthorized access attempts:



```
index=* source="/var/log/auth.log" "Failed"
```

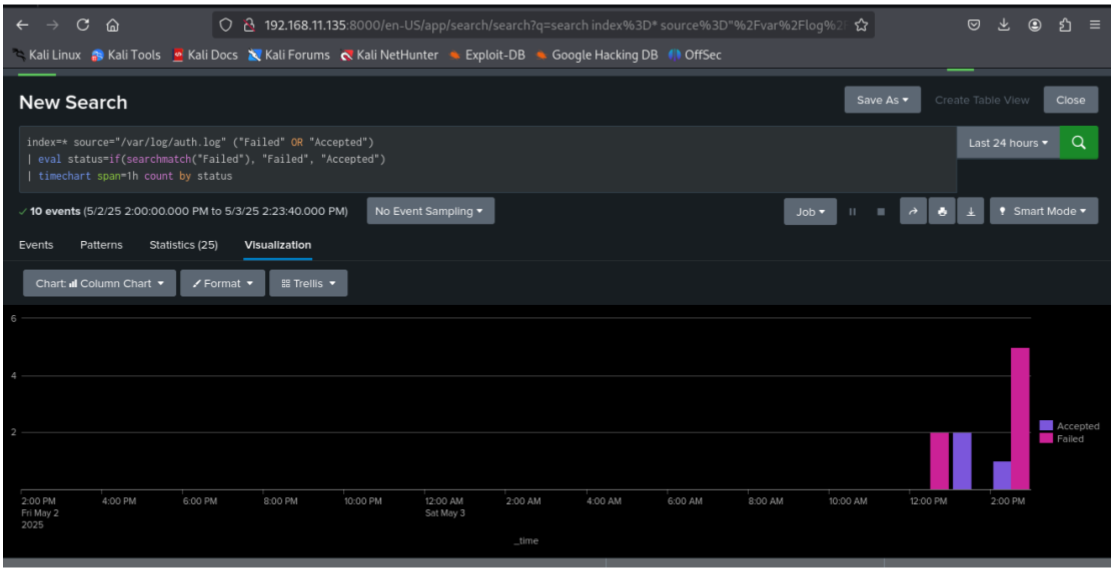
✓ 7 events (5/2/25 2:00:00.000 PM to 5/3/25 2:23:04.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 2
# date_mday 1
# date_minute 2
a date_month 1
# date_second 6
a date_wday 1
# date_year 1
a date_zone 1
a index 1

```
i  Time                 Event
>  5/3/25               May  3 18:01:46 metasploitable3-ub1404 sshd[2754]: Failed password for vagrant from 192.168.11.135 port 35538 ssh2
   2:01:46.000 PM       host = metasploitable3-ub1404   source = /var/log/auth.log   sourcetype = syslog
>  5/3/25               May  3 18:01:44 metasploitable3-ub1404 sshd[2752]: Failed password for root from 192.168.11.135 port 35628 ssh2
   2:01:44.000 PM       host = metasploitable3-ub1404   source = /var/log/auth.log   sourcetype = syslog
>  5/3/25               May  3 18:01:41 metasploitable3-ub1404 sshd[2750]: Failed password for root from 192.168.11.135 port 35612 ssh2
   2:01:41.000 PM       host = metasploitable3-ub1404   source = /var/log/auth.log   sourcetype = syslog
>  5/3/25               May  3 18:01:39 metasploitable3-ub1404 sshd[2748]: Failed password for root from 192.168.11.135 port 35600 ssh2
   2:01:39.000 PM       host = metasploitable3-ub1404   source = /var/log/auth.log   sourcetype = syslog
>  5/3/25               May  3 18:01:37 metasploitable3-ub1404 sshd[2746]: Failed password for root from 192.168.11.135 port 35584 ssh2
   2:01:37.000 PM       host = metasploitable3-ub1404   source = /var/log/auth.log   sourcetype = syslog
>  5/3/25               May  3 16:58:51 metasploitable3-ub1404 sshd[2150]: Failed password for invalid user duaa from 192.168.11.135 port 33322 ss
```

The following query aims to visualize SSH login attempts (both successful and failed) over time. It creates a chart showing the count of "Failed" and "Accepted" login attempts in hourly intervals:



```
index=* source="/var/log/auth.log" ("Failed" OR "Accepted")
| eval status=if(searchmatch("Failed"), "Failed", "Accepted")
| timechart span=1h count by status
```

✓ 10 events (5/2/25 2:00:00.000 PM to 5/3/25 2:23:40.000 PM)

The Splunk analysis clearly demonstrates brute-force activity: a high volume of failed SSH login attempts preceding infrequent successful logins, which likely occurred when the script correctly guessed the credentials. Furthermore, the visualization indicates that the attack was carried out in timed waves, as evidenced by the spacing of login attempts. This pattern could be attributed to retry delays implemented by the attacking script or rate-limiting mechanisms on the Metasploitable3 server. In this instance, the logs recorded 7 failed and 3 accepted login attempts.