King Fahd University of Petroleum & Minerals
College of Computing and Mathematics
ICS 344: Information Security (242)
Project-P2

King Fahd University of Petroleum & Minerals

ICS 344: Information Security (242)

Term 242

Project-P2

MOHMAD ALMAHDOOD	s202034660
ALI ALABDULJABBAR	s202027280
ALI ALMATROOD	s202040180

SECTION 5

February 30, 2025

King Fahd University of Petroleum & Minerals
College of Computing and Mathematics
ICS 344: Information Security (242)
Project-P2

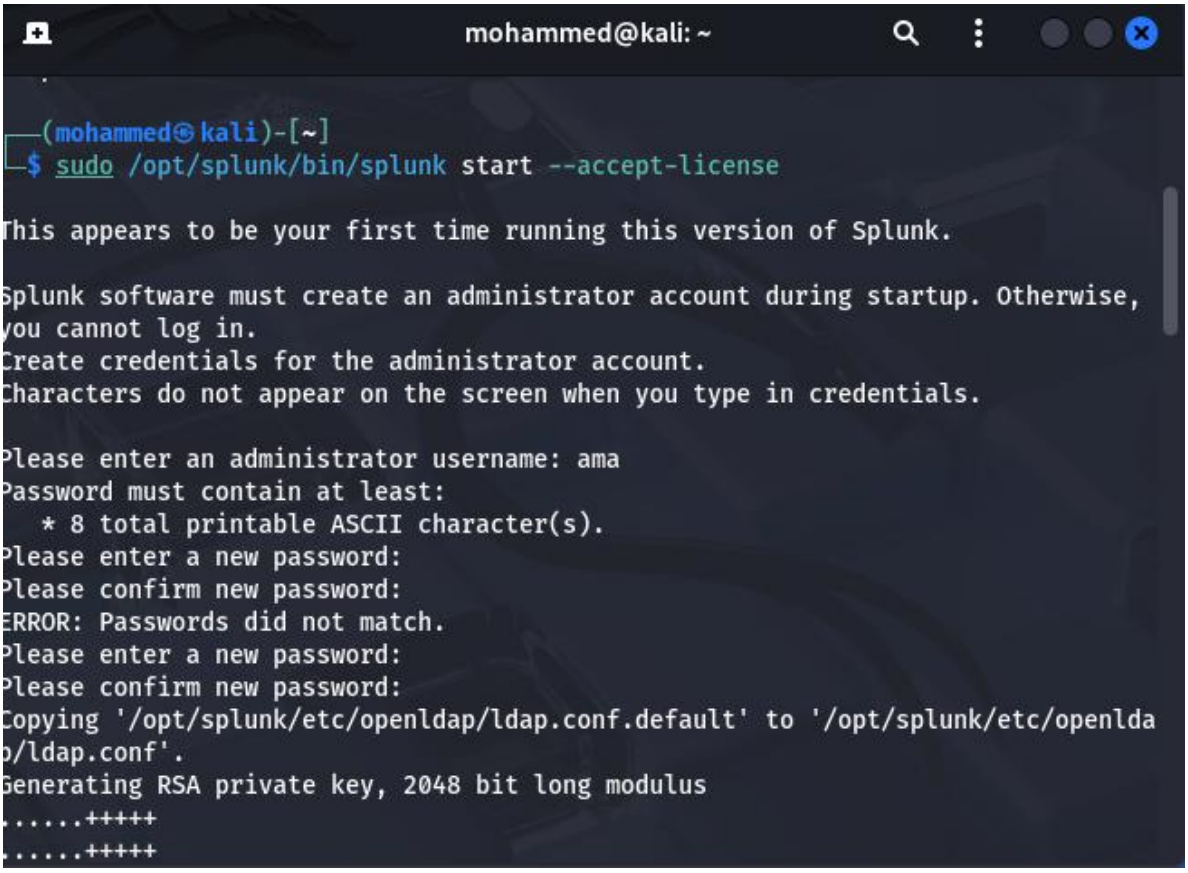
Contents

Phase 2: Visual Analysis with a SIEM Dashboard

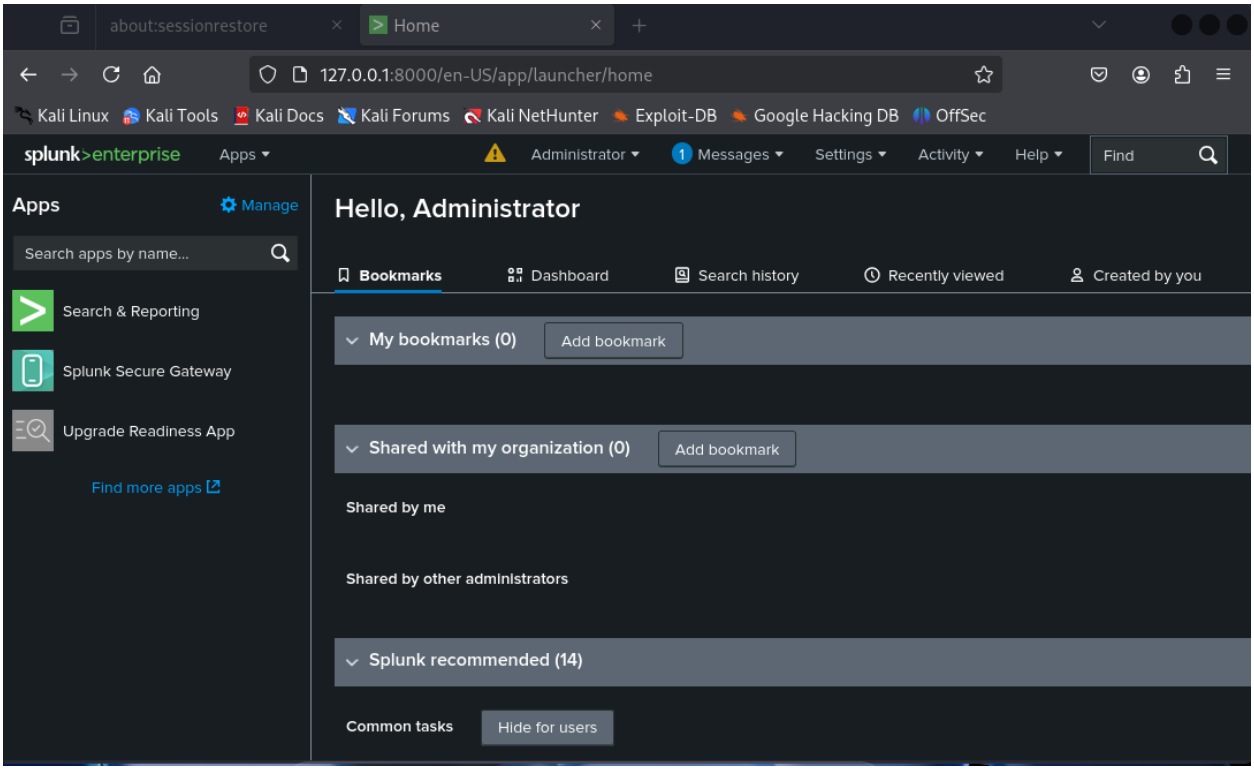
Step 1: install the SIEM tool (Splunk)

```
┌──(mohammed㉿kali)-[~]
└─$ sudo dpkg -i splunk-*.deb
(Reading database ... 500075 files and directories currently installed.)
Preparing to unpack splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb ...
This looks like an upgrade of an existing Splunk Server. Attempting to stop the
installed Splunk Server...
splunkd is not running.
Unpacking splunk (9.3.2) over (9.3.2) ...
Setting up splunk (9.3.2) ...
complete
```

Step 1.1 start Splunk and choose admin name and password

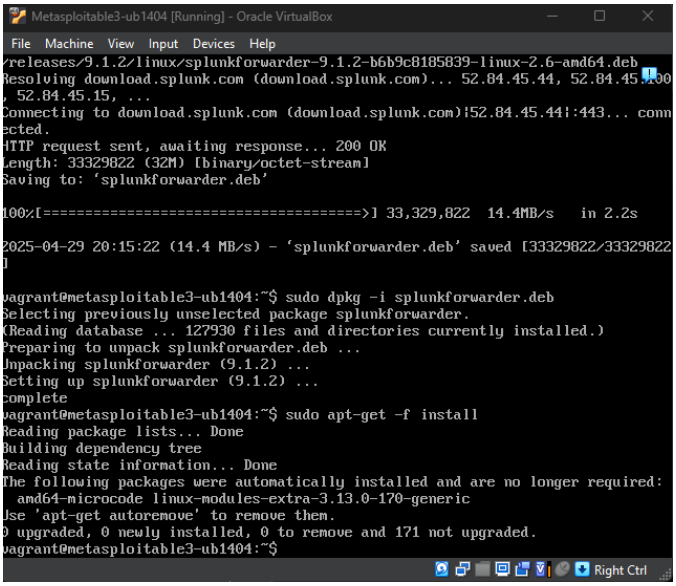


Step 1.2: sign in to the Splunk server with the credentials we made

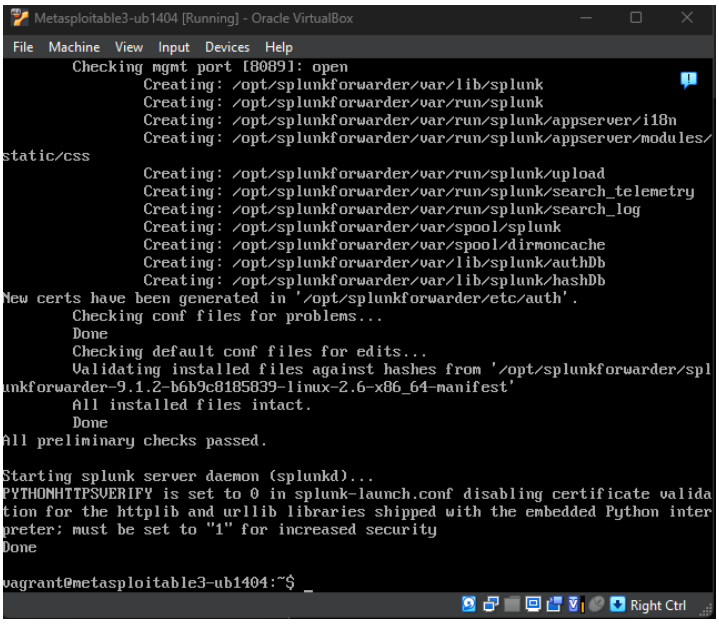


Step 2: configure Splunk universal forwarder

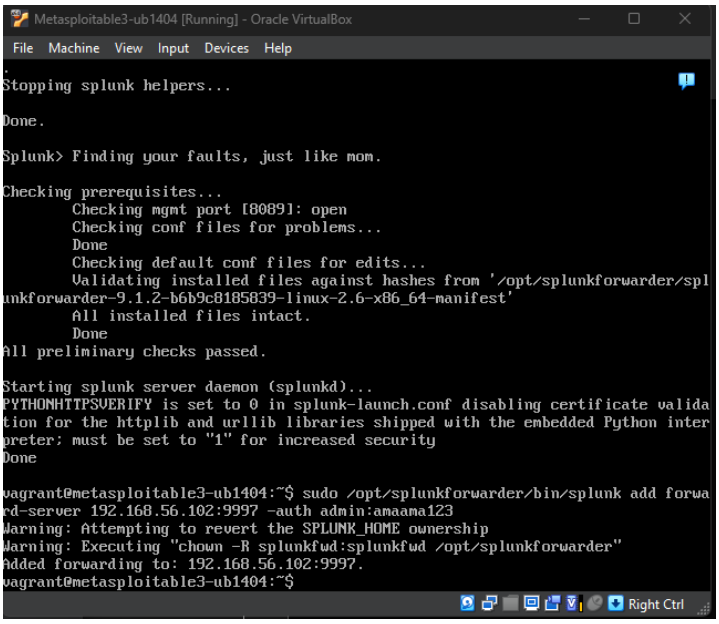
1. Install the Splunk universal forwarder on the metasploitable3 VM



2. Start the Splunk universal forwarder and accept the licenses



3. Configure the forwarder to send data to our Splunk server



4. Add the SSH authentication logs to be monitored

```
vagrant@metasploitable3-ub1404:~$ sudo /opt/splunkforwarder/bin/splunk add monit
or /var/log/auth.log -sourcetype linux_secure
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/var/log/auth.log'.
vagrant@metasploitable3-ub1404:~$
```

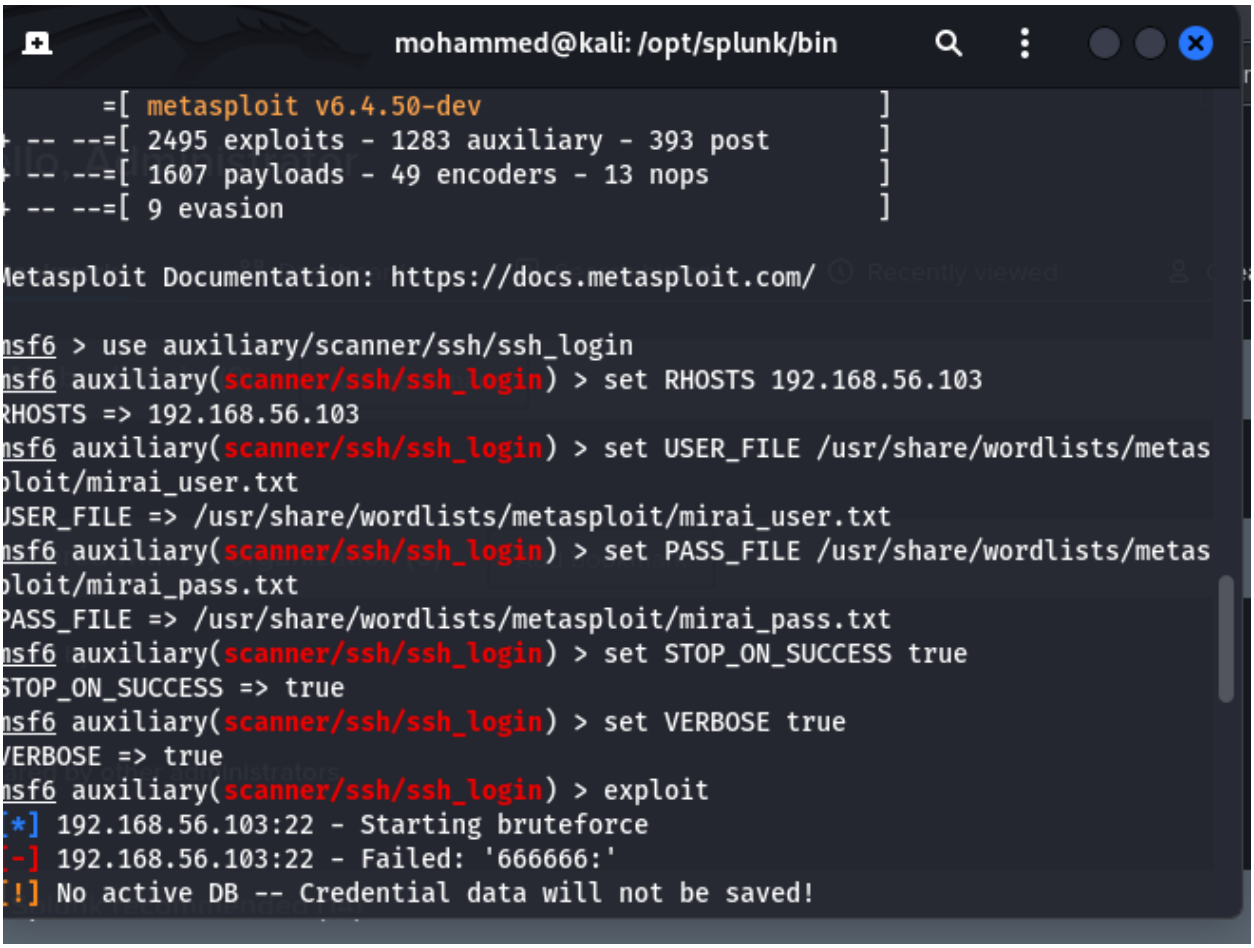
5. Restart the Splunk forwarder to apply the changes and verify the forwarder is running

```
Metasploitable3-ub1404 [Running] - Oracle VirtualBox
File  Machine  View  Input  Devices  Help
..
Stopping splunk helpers...

Done.

Splunk> Finding your faults, just like mom.

Checking prerequisites...
        Checking mgmt port [8089]: open
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/spl
unkforwarder-9.1.2-b6b9c8185839-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate valida
tion for the httplib and urllib libraries shipped with the embedded Python inter
preter; must be set to "1" for increased security
Done

vagrant@metasploitable3-ub1404:~$ sudo /opt/splunkforwarder/bin/splunk status
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
splunkd is running (PID: 2721).
splunk helpers are running (PIDs: 2722).
vagrant@metasploitable3-ub1404:~$
Right Ctrl
```

```
vagrant@metasploitable3-ub1404:~$ sudo /opt/splunkforwarder/bin/splunk list forw
ard-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: admin
Password:
Active forwards:
        192.168.56.102:9997
Configured but inactive forwards:
        None
vagrant@metasploitable3-ub1404:~$ _
Right Ctrl
```

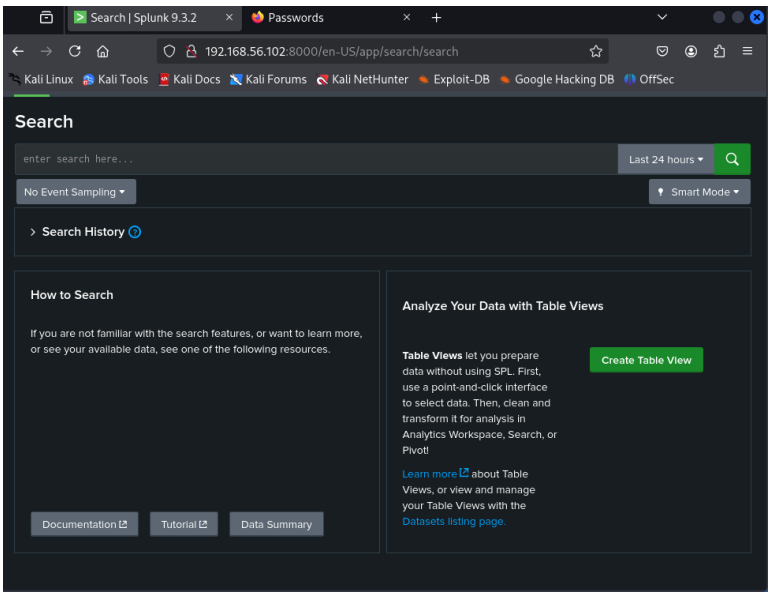
Step 3: attacking the metasploit3 ssh service using brute force

We will conduct the same attack in phase 1 to visualize the logs

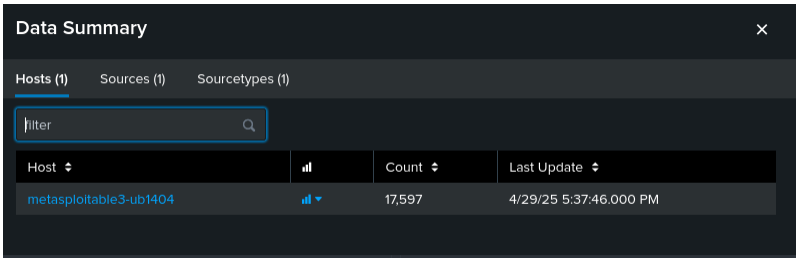


Step 4: log analysis and visualization

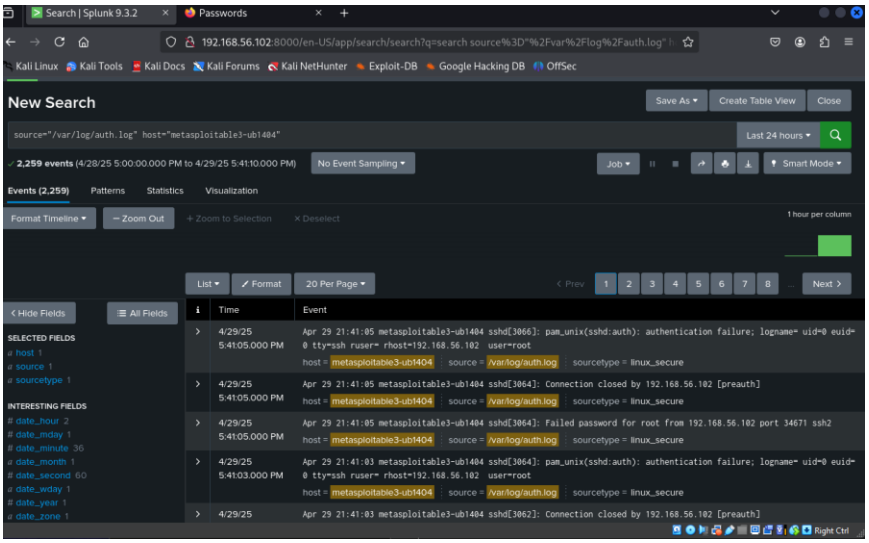
1. Open the search Splunk



2. Chose data summary

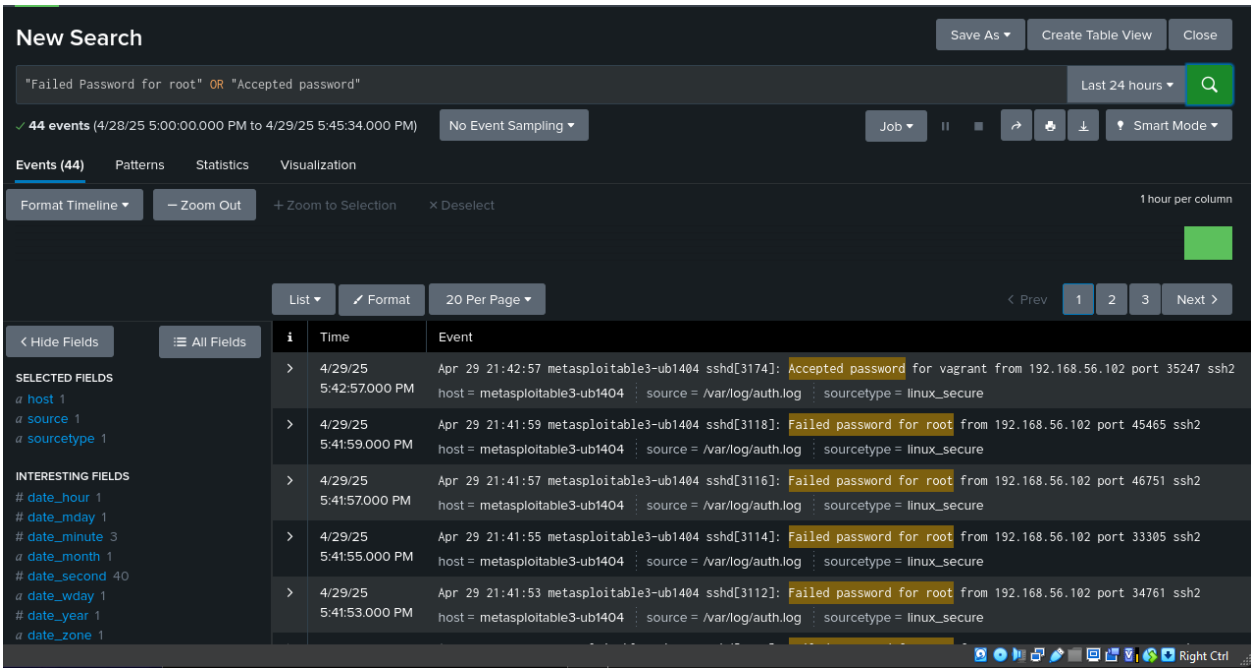


3. Chose the source and host to be metasploitable3 and var/log/auth.log



Step 5: analyze patterns

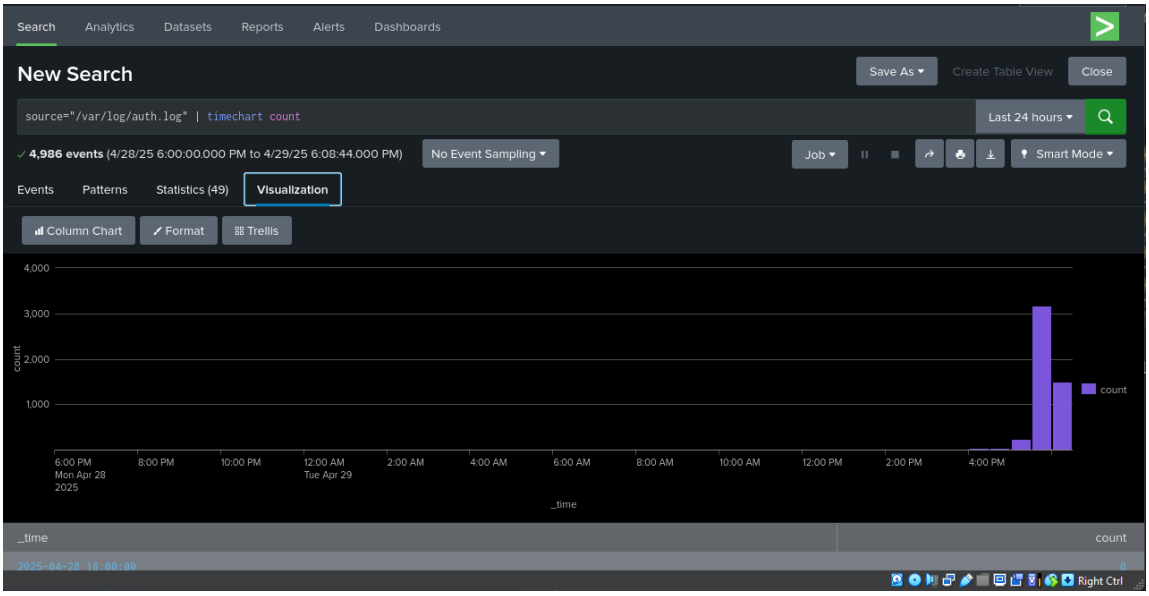
1. Make the search to show only failed passwords or accepted passwords



This will show only the logs for failed attempts and the only successful attempts.

Step 6: visualization

1. Set the timechart in the search query and click on visualization



The x axis shows the time and the y axis shows the count of logs registered

Summary:

In this phase we successfully downloaded Splunk to view the logs, configured the universal forwarder in the Metasploitable3 VM to forward all the ssh auth logs from the victim machine to the kali machine and can analyze, visualize the logs. Also, we can search for specific logs and search for specific patterns.