King Fahd University of Petroleum & Minerals
Seconde Semester 2024/2025 (Term252)

ICS344 Phase 2 Report: Visual Analysis with a SIEM Dashboard

Group number: 07

Group Members:

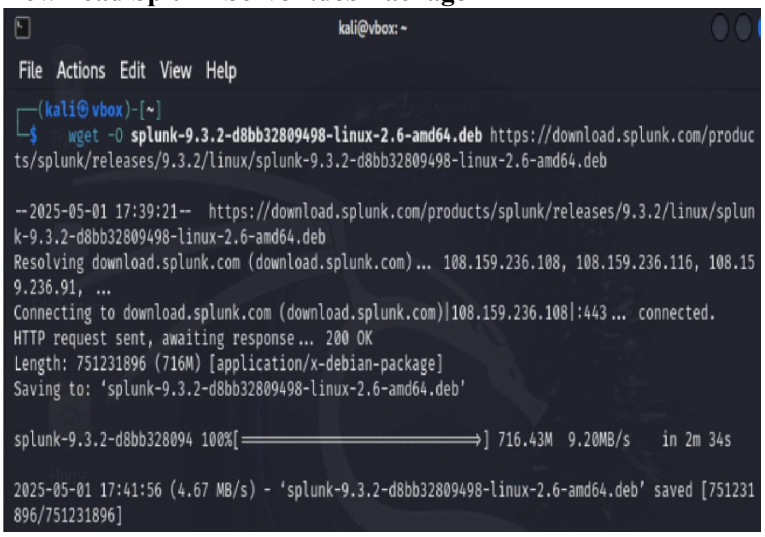
Student name	ID
Shahad Almarhoon	202158610
Ghufran Alhulaymi	202175090
Jood Faqera	202182590

Objective:

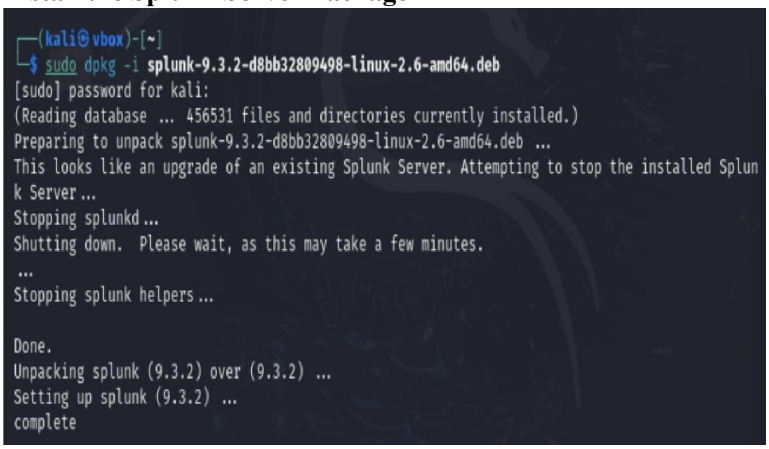
The objective of this phase is to deploy Splunk as a SIEM to centralize log collection, enable real-time monitoring for threats, improve incident response with faster investigations, ensure compliance through log retention, and support forensic analysis with historical data. This involves setting up the Splunk Server and Universal Forwarders to collect and forward logs to the server for analysis. Once configured, Splunk provides visibility into security events, allowing for alerts, dashboards, and threat detection, forming the foundation for advanced security monitoring and response.

1. Install Splunk Server

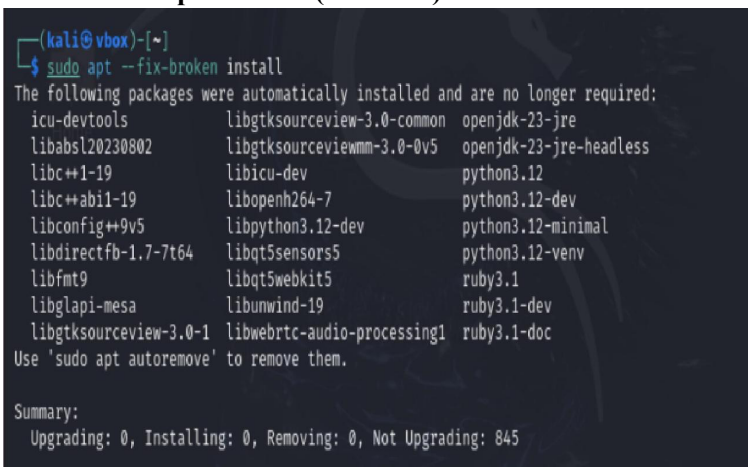
- **Download Splunk Server .deb Package**



- **Install the Splunk Server Package**



- **Fix Broken Dependencies (if needed)**



- **Start Splunk for the First Time**

```
┌──(kali㉿vbox)-[~]
└─$ sudo /opt/splunk/bin/splunk start --accept-license
```

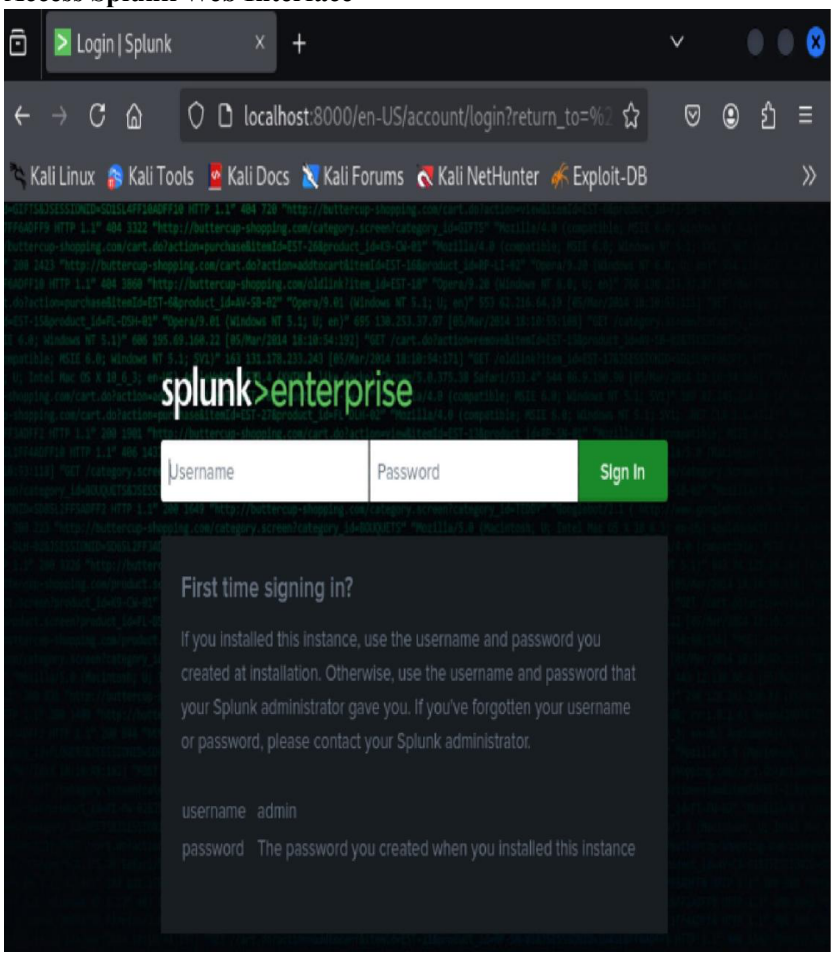
```
Waiting for web server at http://127.0.0.1:8000 to be available..... D
one


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

The Splunk web interface is at http://vbox:8000
```

- **Enable Splunk at System Boot**

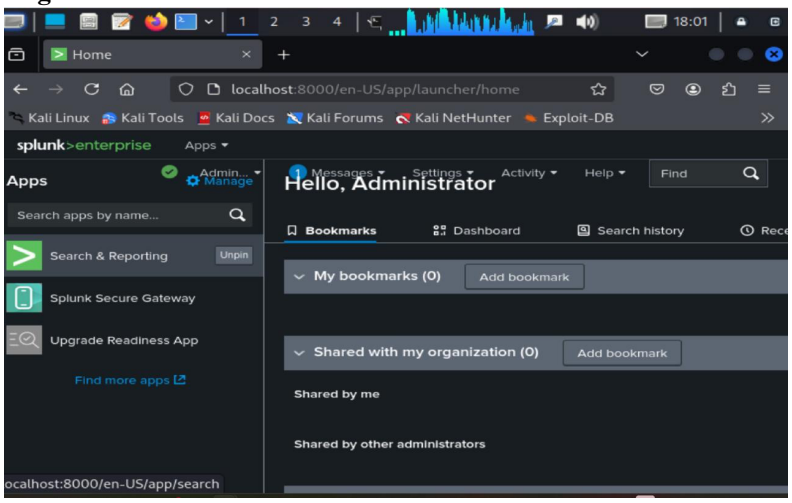
```
┌──(kali㉿vbox)-[~]
└─$ sudo /opt/splunk/bin/splunk enable boot-start
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
```

2. Configured Splunk Web Interface

- **Access Splunk Web Interface**



- **Log in with the Default Credentials**



3. Install Splunk Forwarder

- **Download Splunk Forwarder**

```
vagrant@metasploitable3-ub1404:~$ wget -O splunkforwarder-9.4.1-amd64.deb "https
://download.splunk.com/products/universalforwarder/releases/9.4.1/linux/splunkfo
rwarder-9.4.1-e3bdab203ac8-linux-amd64.deb"
--2025-05-02 20:50:49--  https://download.splunk.com/products/universalforwarder
/releases/9.4.1/linux/splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 108.159.236.84, 108.159.2
36.108, 108.159.236.91, ...
Connecting to download.splunk.com (download.splunk.com)|108.159.236.84|:443... c
onnected.
HTTP request sent, awaiting response... 200 OK
Length: 99029222 (94M) [binary/octet-stream]
Saving to: 'splunkforwarder-9.4.1-amd64.deb'

100%[======================================>] 99,029,222  3.95MB/s   in 17s

2025-05-02 20:51:07 (5.42 MB/s) - 'splunkforwarder-9.4.1-amd64.deb' saved [99029
222/99029222]
```

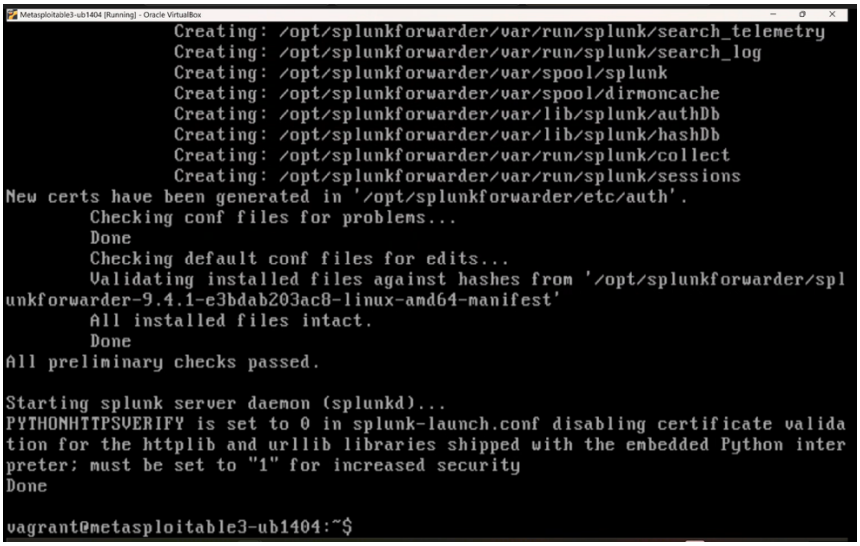
- **Install the Forwarder Package**

```
vagrant@metasploitable3-ub1404:~$ sudo dpkg -i splunkforwarder-9.4.1-amd64.deb
Selecting previously unselected package splunkforwarder.
(Reading database ... 127930 files and directories currently installed.)
Preparing to unpack splunkforwarder-9.4.1-amd64.deb ...
no need to run the pre-install check
Unpacking splunkforwarder (9.4.1) ...
Setting up splunkforwarder (9.4.1) ...
find: `/opt/splunkforwarder/lib/python3.7/site-packages': No such file or direct
ory
find: `/opt/splunkforwarder/lib/python3.9/site-packages': No such file or direct
ory
complete
vagrant@metasploitable3-ub1404:~$
```

- **Fix Any Broken Dependencies**

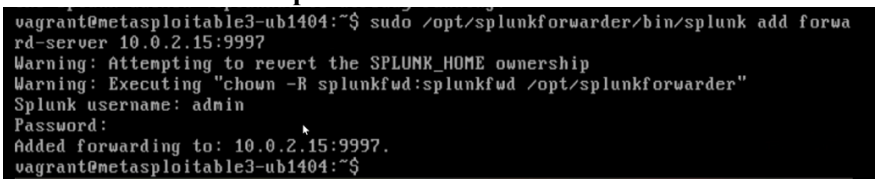
```
vagrant@metasploitable3-ub1404:~$ sudo apt --fix-broken install
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  amd64-microcode linux-modules-extra-3.13.0-170-generic
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
vagrant@metasploitable3-ub1404:~$ _
```

- **Start Splunk Forwarder and Accept the License**

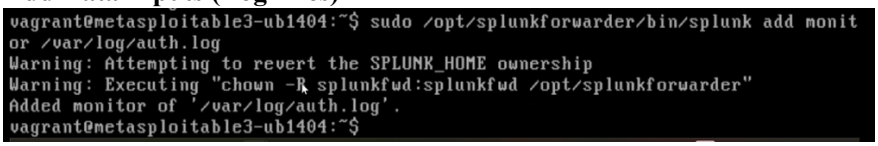


4. Configure Splunk Forwarder

- **Connect Forwarder to Splunk Server**

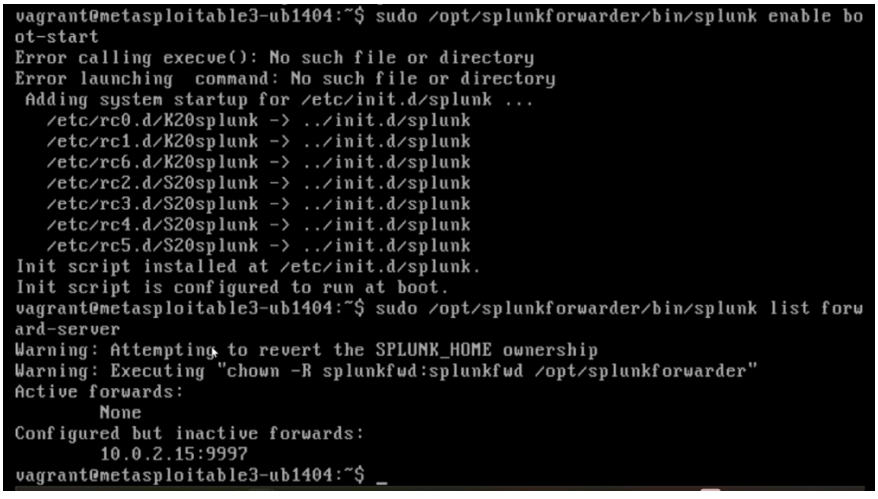


- **Add Data Inputs (Log Files)**



5. Enable Forwarder on System Boot

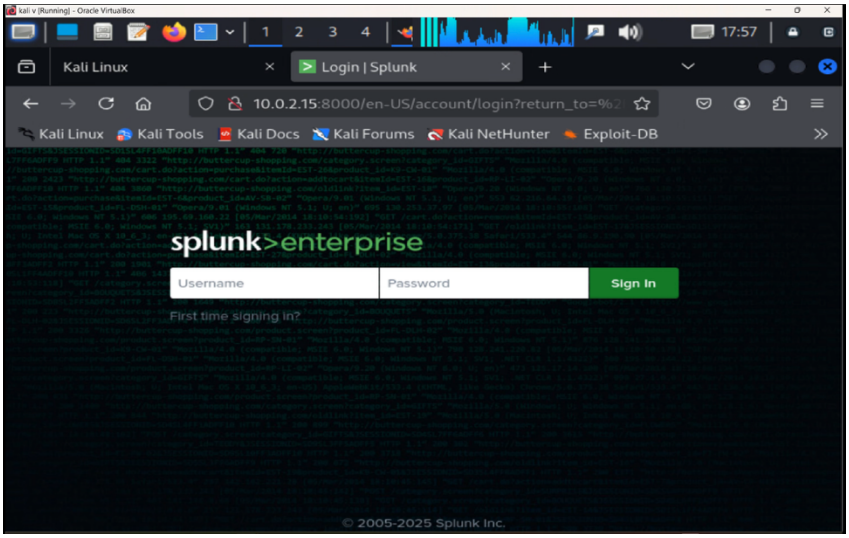
- **Enable Forwarder**

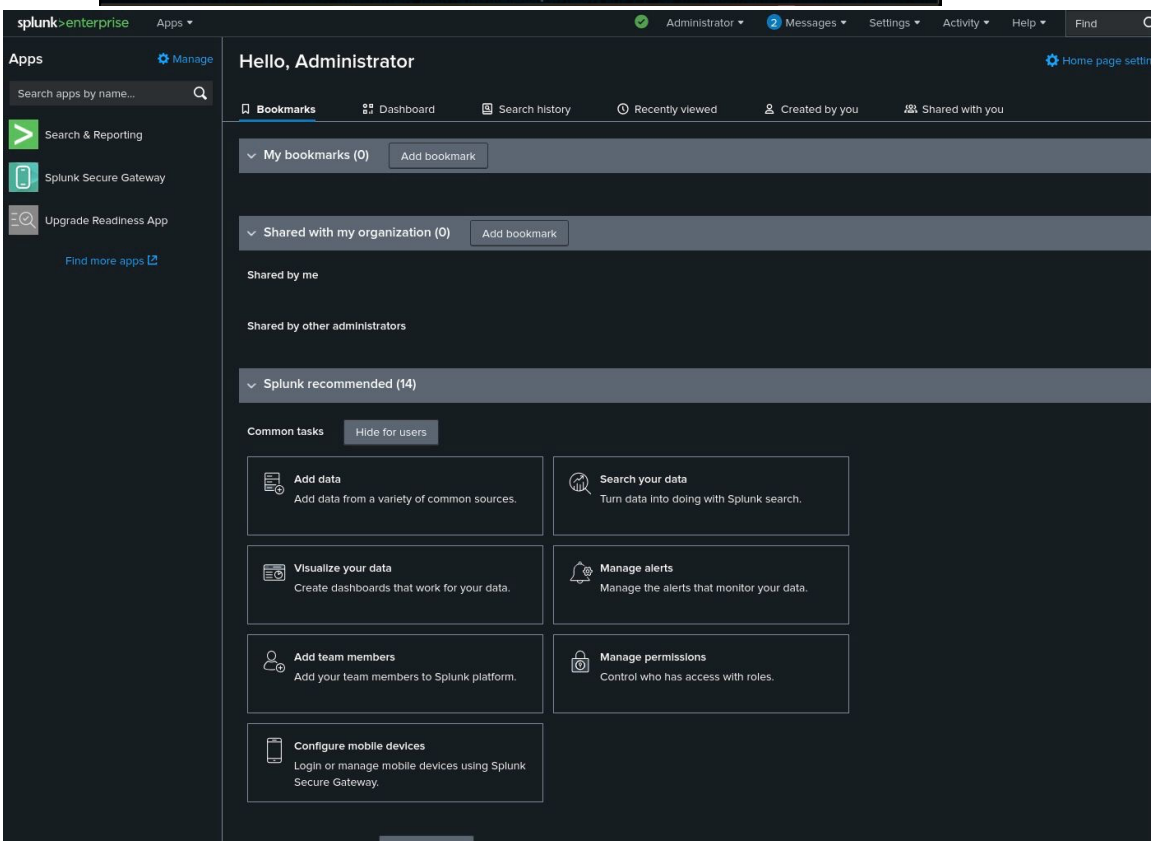


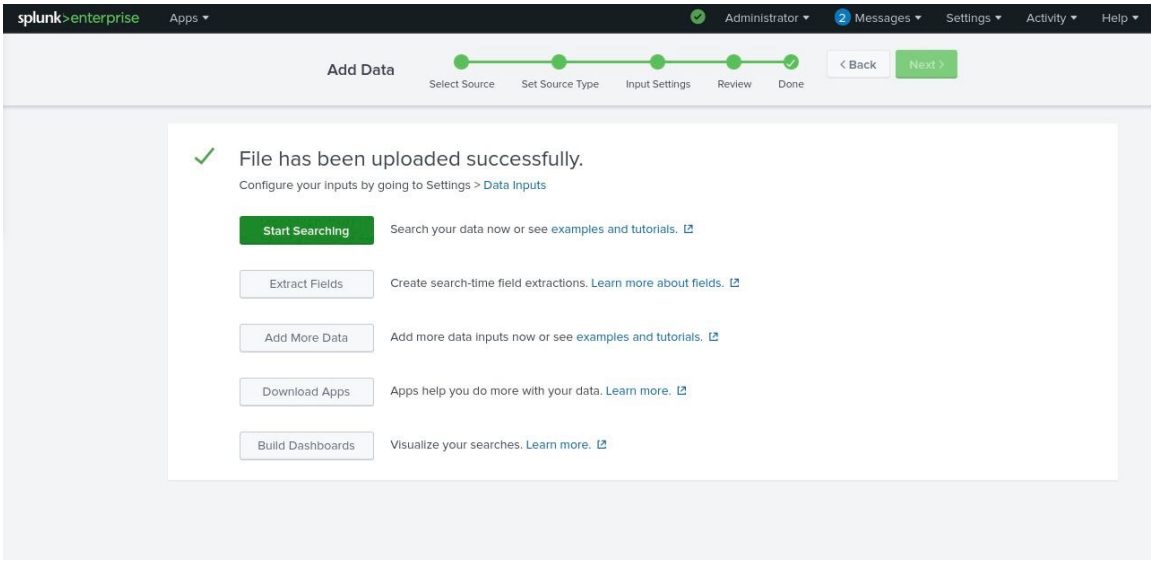
Verify the Setup

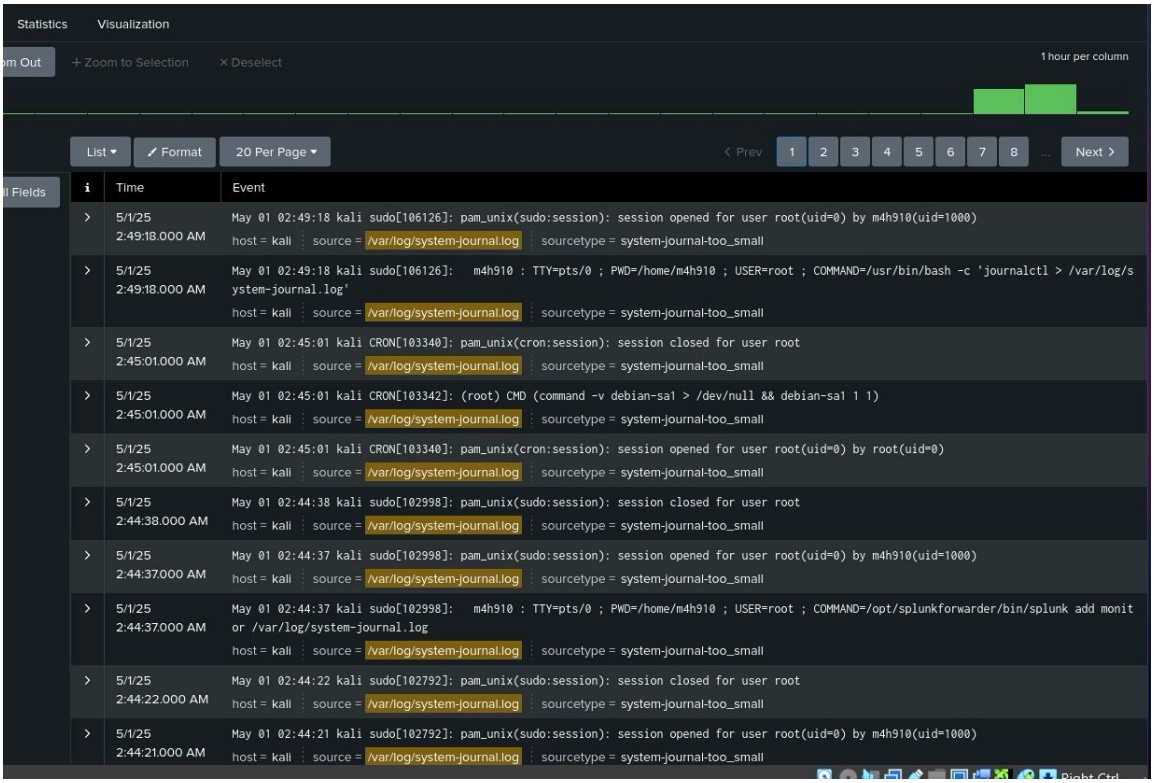
```
┌──(kali㉿vbox)-[~]
└─$ scp vagrant@192.168.100.118:/home/vagrant/auth.log ~/Desktop/

The authenticity of host '192.168.100.118 (192.168.100.118)' can't be established.
ED25519 key fingerprint is SHA256:Rpy8shmBT8uIqZeMsZCG6N5gHXDNSWQ0tEgSgF7t/SM.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.100.118' (ED25519) to the list of known hosts.
vagrant@192.168.100.118's password:
```

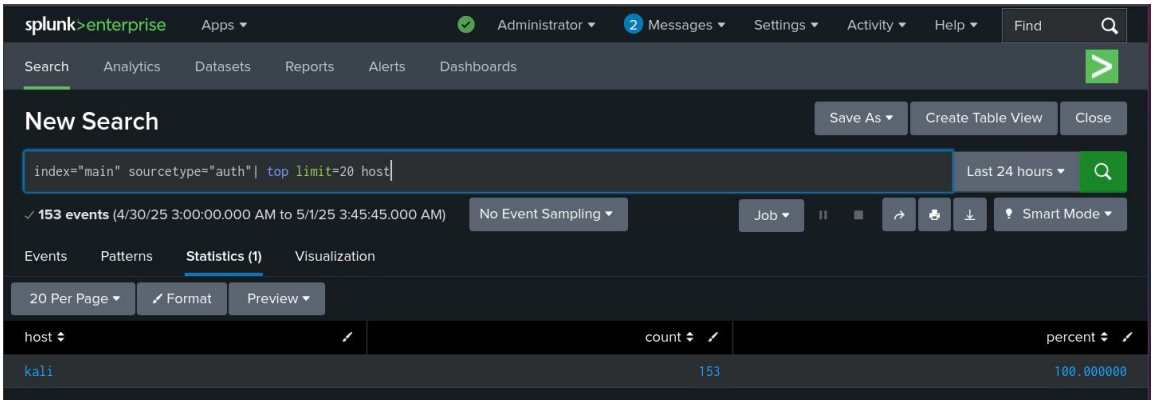
```
                /var/log/Xorg.0.log
                /var/log/Xorg.0.log.old
Monitored Files:
        $SPLUNK_HOME/etc/splunk.version
        /var/log/system-journal.log
```

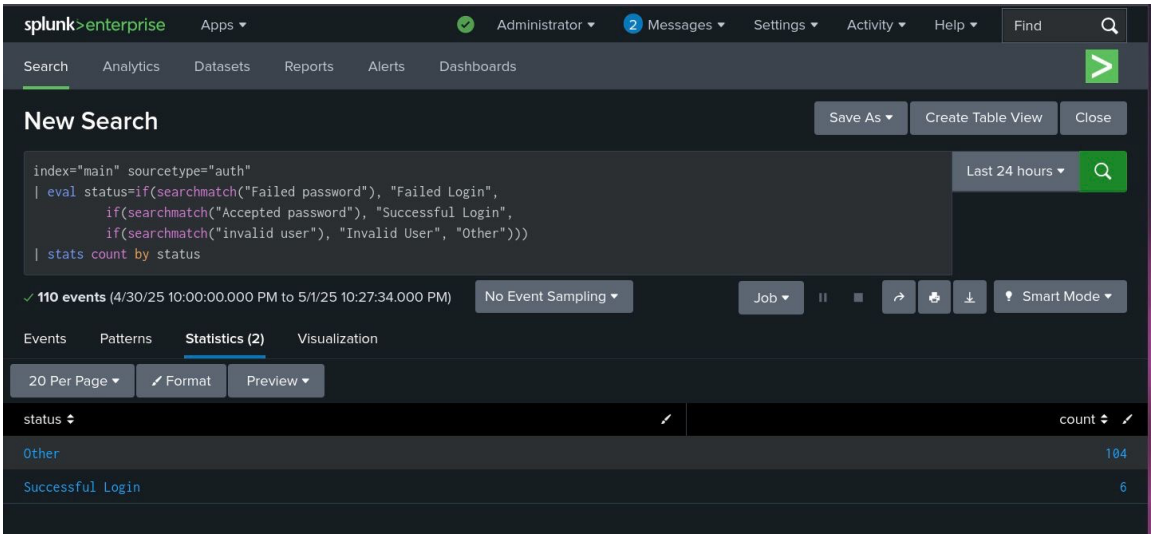

Kali Linux
Login | Splunk
10.0.2.15:8000/en-US/account/login?return_to=%2
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
splunk>enterprise
Username
Password
Sign In
First time signing in?
© 2005-2025 Splunk Inc.


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Apps
Manage
Search apps by name...
Search & Reporting
Splunk Secure Gateway
Upgrade Readiness App
Find more apps
Hello, Administrator
Home page settin
Bookmarks
Dashboard
Search history
Recently viewed
Created by you
Shared with you
My bookmarks (0)
Add bookmark
Shared with my organization (0)
Add bookmark
Shared by me
Shared by other administrators
Splunk recommended (14)
Common tasks
Hide for users
Add data
Add data from a variety of common sources.
Search your data
Turn data into doing with Splunk search.
Visualize your data
Create dashboards that work for your data.
Manage alerts
Manage the alerts that monitor your data.
Add team members
Add your team members to Splunk platform.
Manage permissions
Control who has access with roles.
Configure mobile devices
Login or manage mobile devices using Splunk Secure Gateway.


splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Next >
File has been uploaded successfully.
Configure your inputs by going to Settings > Data Inputs
Start Searching
Search your data now or see examples and tutorials.
Extract Fields
Create search-time field extractions. Learn more about fields.
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.


Statistics
Visualization
+ Zoom to Selection
× Deselect
1 hour per column
List
Format
20 Per Page
< Prev
1 2 3 4 5 6 7 8
Next >
Time
Event
5/1/25 2:49:18.000 AM
May 01 02:49:18 kali sudo[106126]: pam_unix(sudo:session): session opened for user root(uid=0) by m4h910(uid=1000)
host = kali source = /var/log/system-journal.log sourcetype = system-journal-too_small
5/1/25 2:49:18.000 AM
May 01 02:49:18 kali sudo[106126]: m4h910 : TTY=pts/0 ; PWD=/home/m4h910 ; USER=root ; COMMAND=/usr/bin/bash -c 'journalctl > /var/log/system-journal.log'
host = kali source = /var/log/system-journal.log sourcetype = system-journal-too_small
5/1/25 2:45:01.000 AM
May 01 02:45:01 kali CRON[103340]: pam_unix(cron:session): session closed for user root
host = kali source = /var/log/system-journal.log sourcetype = system-journal-too_small
5/1/25 2:45:01.000 AM
May 01 02:45:01 kali CRON[103342]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
host = kali source = /var/log/system-journal.log sourcetype = system-journal-too_small
5/1/25 2:45:01.000 AM
May 01 02:45:01 kali CRON[103340]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
host = kali source = /var/log/system-journal.log sourcetype = system-journal-too_small
5/1/25 2:44:38.000 AM
May 01 02:44:38 kali sudo[102998]: pam_unix(sudo:session): session closed for user root
host = kali source = /var/log/system-journal.log sourcetype = system-journal-too_small
5/1/25 2:44:37.000 AM
May 01 02:44:37 kali sudo[102998]: pam_unix(sudo:session): session opened for user root(uid=0) by m4h910(uid=1000)
host = kali source = /var/log/system-journal.log sourcetype = system-journal-too_small
5/1/25 2:44:37.000 AM
May 01 02:44:37 kali sudo[102998]: m4h910 : TTY=pts/0 ; PWD=/home/m4h910 ; USER=root ; COMMAND=/opt/splunkforwarder/bin/splunk add monitor /var/log/system-journal.log
host = kali source = /var/log/system-journal.log sourcetype = system-journal-too_small
5/1/25 2:44:22.000 AM
May 01 02:44:22 kali sudo[102792]: pam_unix(sudo:session): session closed for user root
host = kali source = /var/log/system-journal.log sourcetype = system-journal-too_small
5/1/25 2:44:21.000 AM
May 01 02:44:21 kali sudo[102792]: pam_unix(sudo:session): session opened for user root(uid=0) by m4h910(uid=1000)
host = kali source = /var/log/system-journal.log sourcetype = system-journal-too_small





Outcome:

- Successfully forwarded **SSH/system logs** from Metasploitable3 to Splunk SIEM.
- Created **visualizations** to track authentication patterns and system activities.
- Identified **suspicious events** for further analysis.