



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**

```
kali㉿vbox:~
File Actions Edit View Help
(kali㉿vbox) [~]
$ wget -O splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb https://download.splunk.com/products/splunk/releases/9.3.2/linux/splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb
--2025-05-01 17:39:21-- https://download.splunk.com/products/splunk/releases/9.3.2/linux/splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb
Resolving download.splunk.com (download.splunk.com) ... 108.159.236.108, 108.159.236.116, 108.159.236.91, ...
Connecting to download.splunk.com (download.splunk.com)|108.159.236.108|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 751231896 (716M) [application/x-debian-package]
Saving to: 'splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb'

splunk-9.3.2-d8bb328094 100%[=====] 716.43M 9.20MB/s in 2m 34s

2025-05-01 17:41:56 (4.67 MB/s) - 'splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb' saved [751231896/751231896]
```

- **Install the Splunk Server Package**

```
(kali㉿vbox) [~]
$ sudo dpkg -i splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb
[sudo] password for kali:
(Reading database ... 456531 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...
Stopping splunkd ...
Shutting down. Please wait, as this may take a few minutes.
...
Stopping splunk helpers ...

Done.
Unpacking splunk (9.3.2) over (9.3.2) ...
Setting up splunk (9.3.2) ...
complete
```

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

```
(kali㉿vbox) [~]
$ sudo apt --fix-broken install
The following packages were automatically installed and are no longer required:
  icu-devtools      libgtksourceview-3.0-common  openjdk-23-jre
  libabsl20230802   libgtksourceviewmm-3.0-0v5    openjdk-23-jre-headless
  libc++1-19         libicu-dev                  python3.12
  libc++abi1-19     libopenh264-7                python3.12-dev
  libconfig++9v5    libpython3.12-dev            python3.12-minimal
  libdirectfb-1.7-7t64 libqt5sensors5           python3.12-venv
  libfmt9           libqt5webkit5              ruby3.1
  libglapi-mesa     libunwind-19               ruby3.1-dev
  libgtksourceview-3.0-1 libwebrtc-audio-processing1 ruby3.1-doc
Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 845
```

- 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.
```

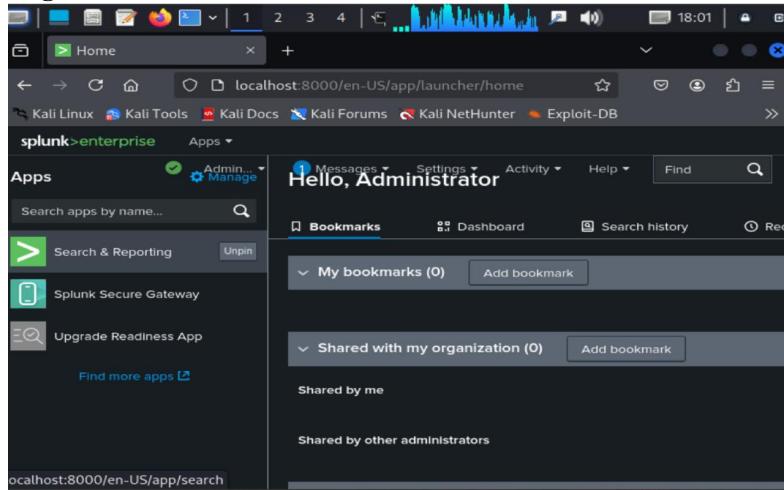
2. Configured Splunk Web Interface

- **Access Splunk Web Interface**

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.

username admin
password The password you created when you installed this instance

- 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/splunkforwarder-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, 108.159.236.108, 108.159.236.91, ...
Connecting to download.splunk.com (download.splunk.com)|108.159.236.84|:443... connected.
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 [99029222/99029222]
```

- 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 directory
find: '/opt/splunkforwarder/lib/python3.9/site-packages': No such file or directory
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

```

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-9.4.1-e3bdab203ac8-linux-amd64-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 validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done

vagrant@metasploitable3-ub1404:~$
```

4. Configure Splunk Forwarder

- **Connect Forwarder to Splunk Server**

```
vagrant@metasploitable3-ub1404:~$ sudo /opt/splunkforwarder/bin/splunk add forwarder 10.0.2.15:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Splunk username: admin
Password:
Added forwarding to: 10.0.2.15:9997.
vagrant@metasploitable3-ub1404:~$
```

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

```
vagrant@metasploitable3-ub1404:~$ sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/auth.log
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. Enable Forwarder on System Boot

- **Enable Forwarder**

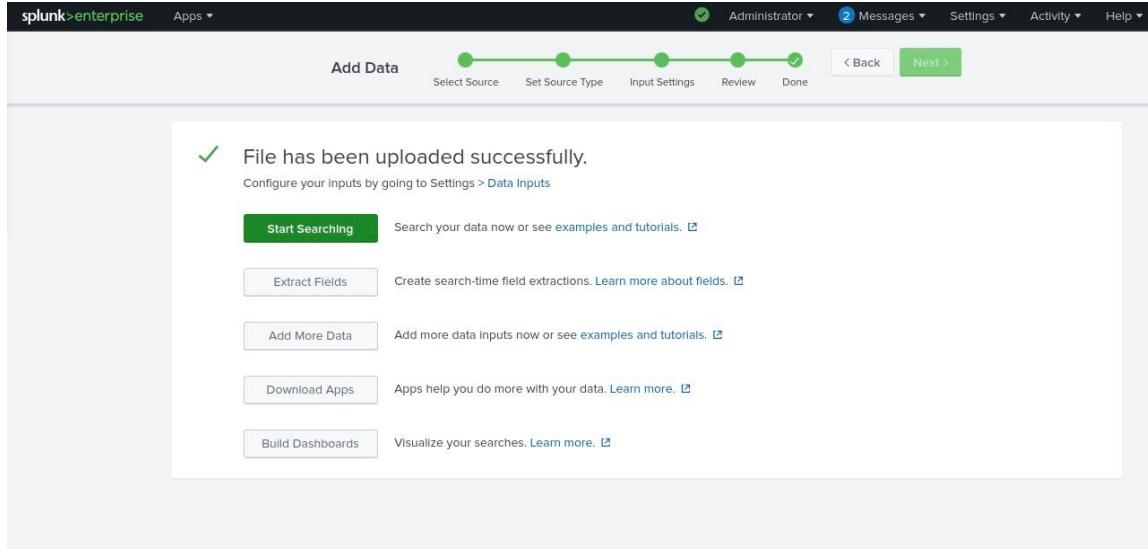
```
vagrant@metasploitable3-ub1404:~$ sudo /opt/splunkforwarder/bin/splunk enable boot-start
Error calling execve(): No such file or directory
Error launching command: No such file or directory
Adding system startup for /etc/init.d/splunk ...
/etc/rc0.d/K20splunk -> ../init.d/splunk
/etc/rc1.d/K20splunk -> ../init.d/splunk
/etc/rc6.d/K20splunk -> ../init.d/splunk
/etc/rc2.d/S20splunk -> ../init.d/splunk
/etc/rc3.d/S20splunk -> ../init.d/splunk
/etc/rc4.d/S20splunk -> ../init.d/splunk
/etc/rc5.d/S20splunk -> ../init.d/splunk
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
vagrant@metasploitable3-ub1404:~$ sudo /opt/splunkforwarder/bin/splunk list forwarder-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Active forwards:
    None
Configured but inactive forwards:
        10.0.2.15:9997
vagrant@metasploitable3-ub1404:~$ _
```

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:Rpy8shmBT8uIiqZeMsZCG6N5gHXDNSWQ0tEgSgF7t/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: [REDACTED]

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

The screenshot shows a Kali Linux terminal window at the top, displaying a log of network traffic captured by Wireshark. The log includes numerous HTTP requests and responses, such as logins to 'splunk>enterprise' and file downloads from 'butcherup-shopping.com'. Below the terminal is the Splunk Enterprise web interface, featuring a dark-themed dashboard. The dashboard includes sections for 'Hello, Administrator', 'Common tasks' (Add data, Search your data, Visualize your data, Manage alerts, Add team members, Manage permissions, Configure mobile devices), and links for Bookmarks, Dashboard, Search history, Recently viewed, Created by you, Shared with you, and Splunk recommended (14). The top right of the interface shows user information (Administrator) and navigation links.



Statistics Visualization		
<input type="button" value="Zoom Out"/> + Zoom to Selection <input type="button" value="X Deselect"/> 1 hour per column		
<input type="button" value="List"/>	<input type="button" value="Format"/>	<input type="button" value="20 Per Page"/>
All Fields	i	Time Event
	>	May 01 02:49:18 kali sudo[106126]: pam_unix(sudo:session): session opened for user root(uid=0) by m4h910(uid=1000)
	>	2:49:18.000 AM host=kali source=/var/log/system-journal.log sourcetype=system-journal-too_small
	>	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
	>	May 01 02:45:01 kali CRON[103340]: pam_unix(cron:session): session closed for user root
	>	2:45:01.000 AM host=kali source=/var/log/system-journal.log sourcetype=system-journal-too_small
	>	May 01 02:45:01 kali CRON[103342]: (root) CMD (command -v debian-sal > /dev/null && debian-sal 1 1)
	>	host=kali source=/var/log/system-journal.log sourcetype=system-journal-too_small
	>	May 01 02:45:01 kali CRON[103340]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
	>	2:45:01.000 AM host=kali source=/var/log/system-journal.log sourcetype=system-journal-too_small
	>	May 01 02:44:38 kali sudo[102998]: pam_unix(sudo:session): session closed for user root
	>	2:44:38.000 AM host=kali source=/var/log/system-journal.log sourcetype=system-journal-too_small
	>	May 01 02:44:37 kali sudo[102998]: pam_unix(sudo:session): session opened for user root(uid=0) by m4h910(uid=1000)
	>	2:44:37.000 AM host=kali source=/var/log/system-journal.log sourcetype=system-journal-too_small
	>	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
	>	May 01 02:44:22 kali sudo[102792]: pam_unix(sudo:session): session closed for user root
	>	2:44:22.000 AM host=kali source=/var/log/system-journal.log sourcetype=system-journal-too_small
	>	May 01 02:44:21 kali sudo[102792]: pam_unix(sudo:session): session opened for user root(uid=0) by m4h910(uid=1000)
	>	2:44:21.000 AM host=kali source=/var/log/system-journal.log sourcetype=system-journal-too_small

The image displays two side-by-side screenshots of the Splunk Enterprise web interface. Both screenshots show a search results page with a dark theme.

Screenshot 1 (Top):

- Search Bar:** `index="main" sourcetype="auth" | top limit=20 host`
- Results Summary:** ✓ 153 events (4/30/25 3:00:00.000 AM to 5/1/25 3:45:45.000 AM) | No Event Sampling
- Statistics:** Statistics (1) | Events, Patterns, Statistics (1), Visualization
- Data Preview:** 20 Per Page | Format, Preview
- Host Data:**

host	count	percent
kali	153	100.000000

Screenshot 2 (Bottom):

- Search Bar:** `index="main" sourcetype="auth" | eval status=if(searchmatch("Failed password"), "Failed Login", if(searchmatch("Accepted password"), "Successful Login", if(searchmatch("invalid user"), "Invalid User", "Other"))) | stats count by status`
- Results Summary:** ✓ 110 events (4/30/25 10:00:00.000 PM to 5/1/25 10:27:34.000 PM) | No Event Sampling
- Statistics:** Statistics (2) | Events, Patterns, Statistics (2), Visualization
- Status Data:**

status	count
Other	104
Successful Login	6

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.