



SIEM Project (End-to-End Implementation): Real-Time Attack Monitoring Using Splunk Cloud + Ubuntu Server + Kali Linux

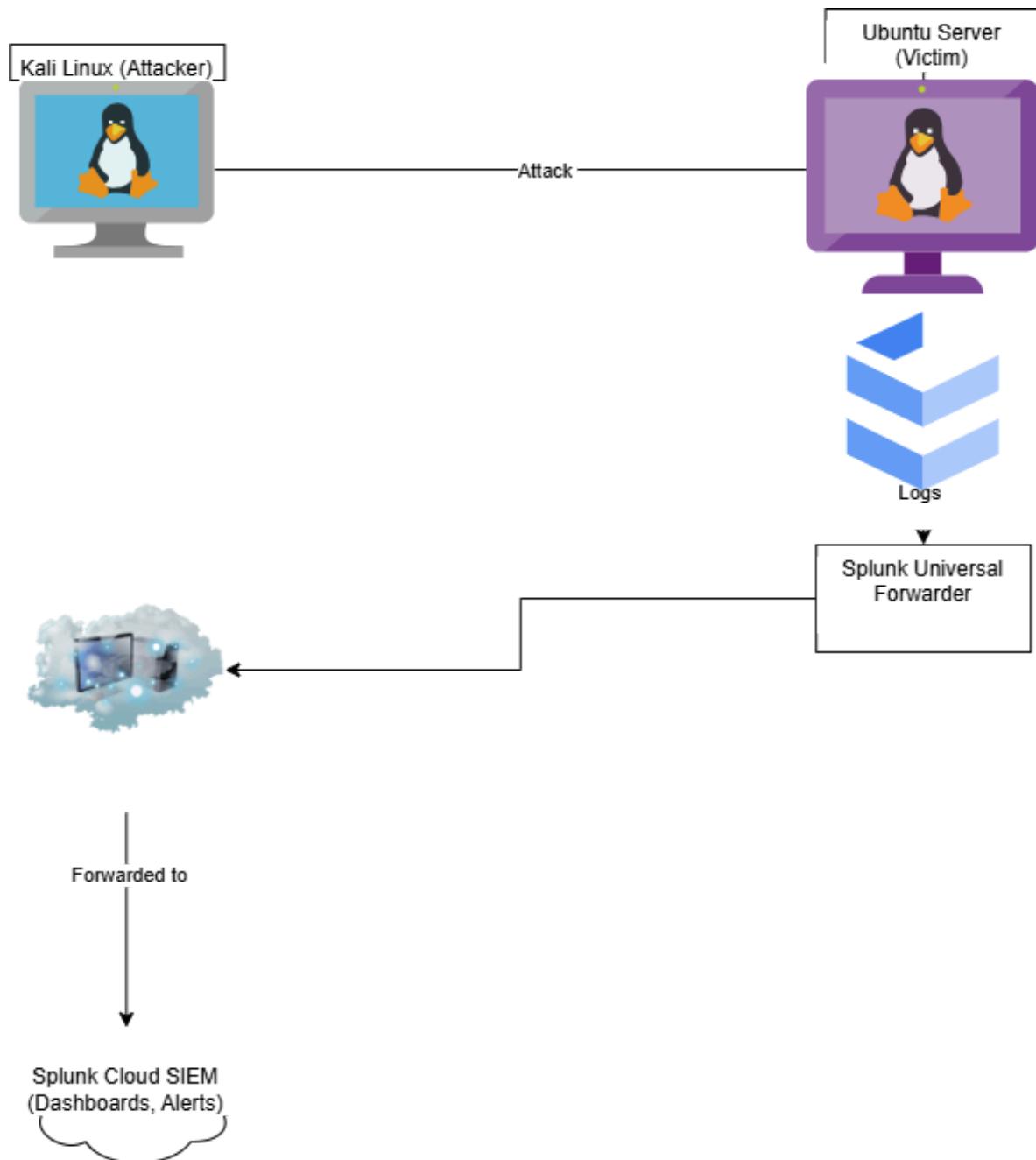


Introduction

In this project, I built a complete **end-to-end SIEM (Security Information and Event Monitoring) lab** where:

- **Ubuntu Server** acts as the monitored victim machine
- **Kali Linux** acts as the attacker
- **Splunk Cloud** acts as the SIEM platform
- I forward **system logs, audit logs, firewall logs, SSH logs** from Ubuntu to Splunk
- I perform **real cyber-attacks** (nmap scan, SSH brute force, suspicious commands)
- I visualize everything inside **custom Splunk dashboards**

/red/ Lab Architecture



Step 1 — Ubuntu Server Preparation

✓ Update & upgrade

```
sudo apt update && sudo apt upgrade -y
```

✓ Install required packages

```
sudo apt install ufw audited netfilter-persistent iptables-persistent -y
```

✓ Enable UFW firewall

```
sudo ufw enable
```

```
sudo ufw logging full
```

✓ Add iptables LOG rule (to detect Nmap)

```
sudo iptables -A INPUT -j LOG --log-prefix "iptables:  
sudo netfilter-persistent save
```



- This ensures kernel logs will show SRC/DST during scans

Step 2 — Install & Configure Splunk Universal Forwarder

✓ Install Forwarder on Ubuntu (wget + dpkg)

```
lab@lab:~$ cd /tmp/
lab@lab:/tmp$ wget -O splunkforwarder.deb "wget -O splunkforwarder-10.0.1-c486717c322b-linux-amd64.deb "https://download.splunk.com/products/universalforwarder/releases/10.0.1/linux/splunkforwarder-10.0.1-c486717c322b-linux-amd64.deb"
> ^C
lab@lab:/tmp$ wget -O splunkforwarder.deb "wget -O splunkforwarder-10.0.1-c486717c322b-linux-amd64.deb "https://download.splunk.com/products/universalforwarder/releases/10.0.1/linux/splunkforwarder-10.0.1-c486717c322b-linux-amd64.deb"
> ^C
lab@lab:/tmp$ wget -O splunkforwarder.deb "https://download.splunk.com/products/universalforwarder/releases/10.0.1/linux/splunkforwarder-10.0.1-c486717c322b-linux-amd64.deb"
--2025-11-13 09:08:45-- https://download.splunk.com/products/universalforwarder/releases/10.0.1/linux/splunkforwarder-10.0.1-c486717c322b-linux-amd64.deb
Resolving download.splunk.com (download.splunk.com) ... 18.67.233.65, 18.67.233.40, 18.67.233.18, ...
Connecting to download.splunk.com (download.splunk.com)|18.67.233.65|:443... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 71299870 (68M) [binary/octet-stream]
Saving to: 'splunkforwarder.deb'

splunkforwarder.deb      71%[=====] 48.37M 3.48MB/s eta 6s
splunkforwarder.deb      100%[=====] 68.00M 3.56MB/s   in 19s

2025-11-13 09:09:04 (3.57 MB/s) - 'splunkforwarder.deb' saved [71299870/71299870]

lab@lab:/tmp$ sudo dpkg -i splunkforwarder.deb
[sudo] password for lab:
Selecting previously unselected package splunkforwarder.
(Reading database ... 87035 files and directories currently installed.)
Preparing to unpack splunkforwarder.deb ...
verifying that this system has all the commands we will require to perform the preflight step
no need to run the splunk-preflight upgrade check
Unpacking splunkforwarder (10.0.1) ...
Setting up splunkforwarder (10.0.1) ...
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.
lab@lab:/tmp$ sudo /opt/splunkforwarder/bin/splunk start --accept-license --answer-yes
Warning: Attempting to revert the SPLUNK HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, 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: spl_admin
```

```
Splunk software must create an administrator account during startup. Otherwise, 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: spl_admin
Password must contain at least:
  * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file ...
Important: splunk will start under systemd as user: splunkfwd
The unit file has been created.

Splunk> Winning the War on Error
Checking prerequisites ...
  Checking mgmt port [8089]: open
    Creating: /opt/splunkforwarder/var/lib/splunk
    Creating: /opt/splunkforwarder/var/run/splunk
    Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
    Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
    Creating: /opt/splunkforwarder/var/run/splunk/upload
    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'.
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-10.0.1-c486717c322b-linux-amd64-manifest'
  All installed files intact.
  Done
All preliminary checks passed.

Starting splunk server daemon (splunkd) ...
Done

lab@lab:/tmp$ sudo /opt/splunkforwarder/bin/splunk start --accept-license --answer-yes^C
lab@lab:/tmp$ sudo /opt/splunkforwarder/bin/splunk enable boot-start[]
```

✓ Configure receiving index & token

Add new index

Name: lab

Index data type: Events

Max raw data size: 100 MB

Searchable retention (days): 365

Cancel Save

✓ Configure log forwarding

File: /opt/splunkforwarder/etc/system/local/inputs.conf

The screenshot shows a terminal window with two tabs. The active tab displays the contents of the file /opt/splunkforwarder/etc/system/local/inputs.conf. The configuration file contains several sections for monitoring system logs:

```
host = ubuntu-agent
index = lab
# Syslog - Debian/Ubuntu uses /var/log/syslog
# Syslog - Debian/Ubuntu uses /var/log/syslog
[monitor:///var/log/syslog]
disabled = 0
sourcetype = syslog
index = lab<SOURCE>_<SOURCE_REALTIME>
CRCSSalt = <SOURCE>_<SOURCE_REALTIME>
# Auth logs (SSH/sudo)
# Auth logs (SSH/sudo) [th.log]
[monitor:///var/log/auth.log]
disabled = 0
sourcetype = linux_secure
index = lab<SOURCE>_<SOURCE_REALTIME>
CRCSSalt = <SOURCE>_<SOURCE_REALTIME>
# Dpkg/Apt logs for package activity
# Dpkg/Apt logs for package activity
[monitor:///var/log/apt/history.log]
disabled = 0
sourcetype = debian_apt
index = lab
# Kernel messages
# Kernel messages [log/kern.log]
[monitor:///var/log/kern.log]
disabled = 0
sourcetype = kernel
index = lab
# Monitor any webserver logs (if present)
# Monitor any webserver logs (if present)
[monitor:///var/log/apache2/access.log]
disabled = 0
sourcetype = access_combined
index = lab
[monitor:///var/log/apache2/error.log]
[monitor:///var/log/apache2/error.log]
disabled = 0
sourcetype = apache_error
index = lab
# Monitor user home shell history (optional, cariable per user)
# Monitor user home shell history (optional, cariable per user)
[monitor:///home/ubuntu/.bash_history]
disabled = 0
sourcetype = bash_history
index = lab
EOF
```

The terminal prompt at the bottom is lab@lab:/opt/splunkforwarder/bin\$.

✓ Restart Universal Forwarder

sudo /opt/splunkforwarder/bin/splunk restart

📌 Step 3 — Enable audit d (Detect Commands, Privilege Escalation)

✓ Add custom audit rules

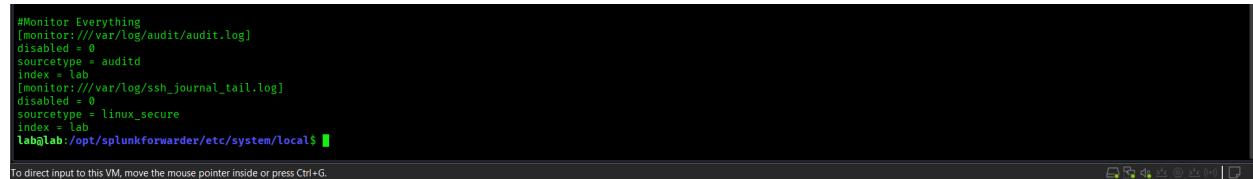
To improve detection i have add this

a) Install auditd and monitor `/var/log/audit/audit.log`

```
sudo apt-get install -y auditd
sudo systemctl enable --now auditd
# optionally add an execve rule (noisy) - edit with caution
# sudo auditctl -a exit,always -F arch=b64 -S execve
```

Then add this to `inputs.conf` or create a new monitor:

```
[monitor:///var/log/audit/audit.log]
disabled = 0
sourcetype = auditd
index = lab
```



The screenshot shows a terminal window with the following content:

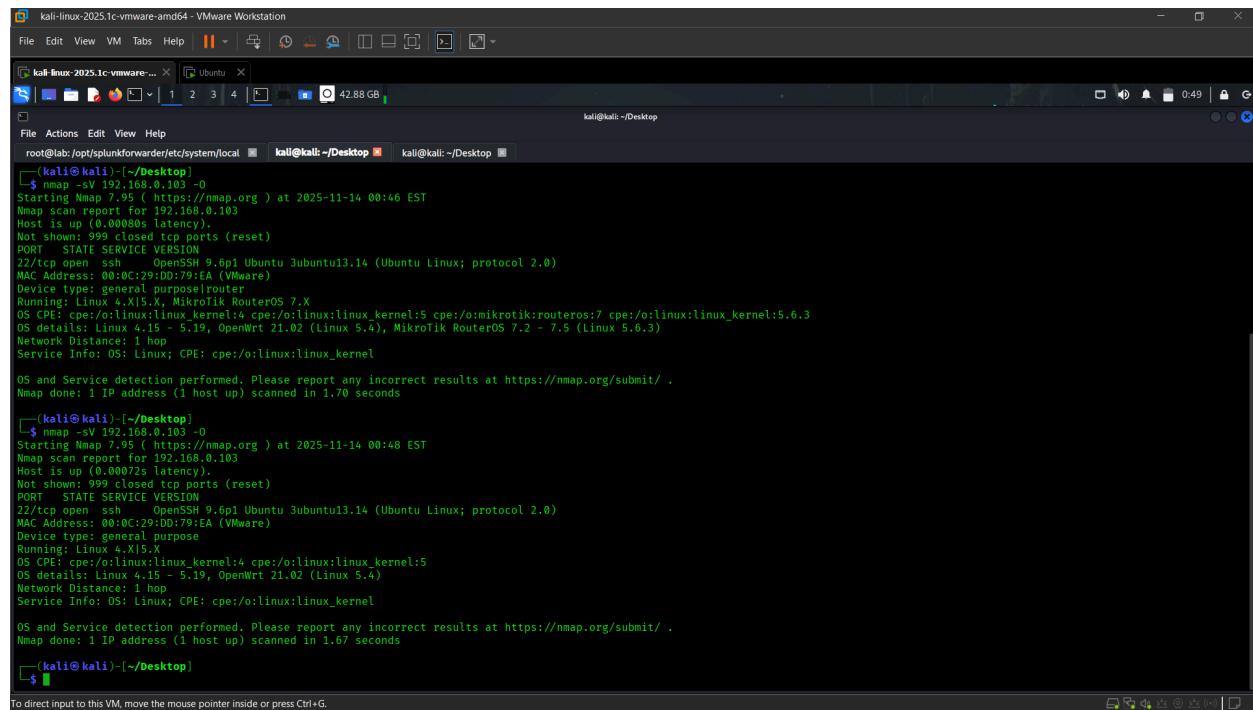
```
#Monitor Everything
[monitor:///var/log/audit/audit.log]
disabled = 0
sourcetype = auditd
index = lab
[monitor:///var/log/ssh_journal_tail.log]
disabled = 0
sourcetype = linux_secure
index = lab
lab@lab:/opt/splunkforwarder/etc/system/local$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Step 4 — Attacker Machine (Kali Linux) Setup

✓ Nmap Scan

nmap -sV <ubuntu-ip>



```
kali@kali:~/Desktop$ nmap -sV 192.168.0.103 -O
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-14 00:46 EST
Nmap scan report for 192.168.0.103
Host is up (0.00080s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 9.6p1 Ubuntu 13.14 (Ubuntu Linux; protocol 2.0)
MAC Address: 00:0C:29:D0:D7:EA (VMware)
Device type: general purpose/router
Running: Linux 4.X, MikroTik RouterOS 7.2
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:mikrotik:routers:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.4 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds

kali@kali:~/Desktop$ nmap -sV 192.168.0.103 -O
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-14 00:48 EST
Nmap scan report for 192.168.0.103
Host is up (0.00072s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 9.6p1 Ubuntu 13.14 (Ubuntu Linux; protocol 2.0)
MAC Address: 00:0C:29:D0:D7:EA (VMware)
Device type: general purpose
Running: Linux 4.X, X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds
```

✓ SSH Brute Force (Manual test)

ssh lab@<ubuntu-ip>

Enter wrong password multiple times

```
(kali㉿kali)-[~/Desktop]
$ ssh lab@192.168.0.103
lab@192.168.0.103's password:
Permission denied, please try again.
lab@192.168.0.103's password:
Permission denied, please try again.
lab@192.168.0.103's password:
lab@192.168.0.103: Permission denied (publickey,password).
```

Step 5 — Splunk Search Queries (SPL)

index=lab

7,806 events (11/12/25 9:00:00.000 AM to 11/13/25 9:40:34.000 AM) No Event Sampling

Events (7,806) Patterns Statistics Visualization

Timeline format Zoom Out + Zoom to Selection Deselect

1 hour per column

sourcetype

4 Values, 100% of events

Values	Count	%
syslog	4,399	56.354%
kernel	3,249	41.622%
linux_secure	158	1.92%
debian_apt	8	0.102%

Selected Yes No

Reports Top values by time Rare values

Events with this field

Values Count %

syslog 4,399 56.354%
kernel 3,249 41.622%
linux_secure 158 1.92%
debian_apt 8 0.102%

tat-collect.service - system activity accounting tool.
| sourcetype = syslog
ct.service: Deactivated successfully.
| sourcetype = syslog
tat-collect.service - system activity accounting tool...
| sourcetype = syslog
:session): session closed for user root
@/log/auth.log | sourcetype = linux_secure
ommand -v debian-sa1 > /dev/null && debian-sa1 1 1)
g | sourcetype = syslog

11/13/25 2025-11-13T09:35:01.028518+00:00 lab CRON(2773): pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
9:35:01.028 AM https://prd-p-00k63.splunkcloud.com/en-US/app/search/search?q=search%20index%3Dlab&display.page=search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=-24h%40h&latest=now&display.events.fields=%5B%22host%22,%22source%22,%22sourcetype%22,%22pid%22,%22p...
https://prd-p-00k63.splunkcloud.com/en-US/app/search/search?q=search index%3Dlab&display.page=search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=-24h%40h&latest=now&display.events.fields=%5B%22host%22,%22source%22,%22sourcetype%22,%22pid%22,%22p...

Detect Nmap Port Scans

```
index=lab (sourcetype=kernel OR sourcetype=syslog) "SRC="
| rex "SRC=(?<src_ip>[0-9\.]+)"
| rex "DST=(?<dest_ip>[0-9\.]+)"
| stats count BY src_ip dest_ip
| sort - count
```

index=lab (sourcetype=kernel OR sourcetype=syslog) "SRC="
| rex "SRC=(?<src_ip>[0-9\.]+)"
| rex "DST=(?<dest_ip>[0-9\.]+)"
| stats count BY src_ip dest_ip
| sort - count

1,199,074 events (before 11/22/25 2:28:13.000 PM) No Event Sampling

Events (1,199,074) Patterns Statistics (38) Visualization

🔍 SSH Brute Force Attempts

```
index=lab sourcetype=linux_secure "Failed password"  
| rex "from (?<src_ip>[0-9\.]*)"  
| stats count BY src_ip
```

The screenshot shows a Splunk search interface. At the top, there are tabs for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The Search tab is selected. Below the tabs, the title "New Search" is displayed. The search bar contains the command: `index=lab sourcetype=linux_secure "Failed password"
| rex "from (?<src_ip>[0-9\.]*)"
| stats count BY src_ip`. Below the search bar, it says **✓ 1,371 events** (before 11/22/25 2:29:05.000 PM) and No Event Sampling. There are four tabs below the search bar: Events (1,371), Patterns, Statistics (2), and Visualization. The Statistics tab is selected. Underneath are buttons for Show: 100 Per Page, Format, and Preview: On. The main area displays a table with one column labeled "src_ip". The table lists two rows: 192.168.0.102 and 192.168.0.104.

🔍 Successful Logins

```
index=lab sourcetype=linux_secure "Accepted password"  
| rex "from (?<src_ip>[0-9\.]*) for (?<user>\S+)"  
| stats count BY src_ip user
```

The screenshot shows a Splunk search interface. At the top, there are tabs for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The Search tab is selected. Below the tabs, the title "New Search" is displayed. The search bar contains the command: `index=lab sourcetype=linux_secure "Accepted password"
| rex "from (?<src_ip>[0-9\.]*) for (?<user>\S+)"
| stats count BY src_ip user`. Below the search bar, it says **✓ 12 events** (before 11/22/25 2:29:48.000 PM) and No Event Sampling. There are four tabs below the search bar: Events (12), Patterns, Statistics (12), and Visualization. The Statistics tab is selected. The main area displays a table with two columns: "src_ip" and "user". The table lists 12 rows, each showing a source IP and a user name.



Suspicious Commands (auditd EXECVE)

```
index=lab sourcetype=auditd type=EXECVE  
| rex "a0=(?<cmd>[^"]+)"  
| stats count BY cmd
```

New Search

```
index=lab sourcetype=auditd type=EXECVE  
| rex "a0=(?<cmd>[^\" ]+)"  
| stats count BY cmd
```

✓ 17,965 events (before 11/22/25 2:30:26.000 PM)

No Event Sampling ▾



Privilege Escalation Attempts

```
index=lab sourcetype=auditd ("sudo" OR "setuid")  
| stats count BY exe uid gid  
| sort - count
```

New Search

```
index=lab sourcetype=auditd ("sudo" OR "setuid")  
| stats count BY exe uid gid  
| sort - count|
```

✓ 541 events (before 11/22/25 2:47:09.000 PM)

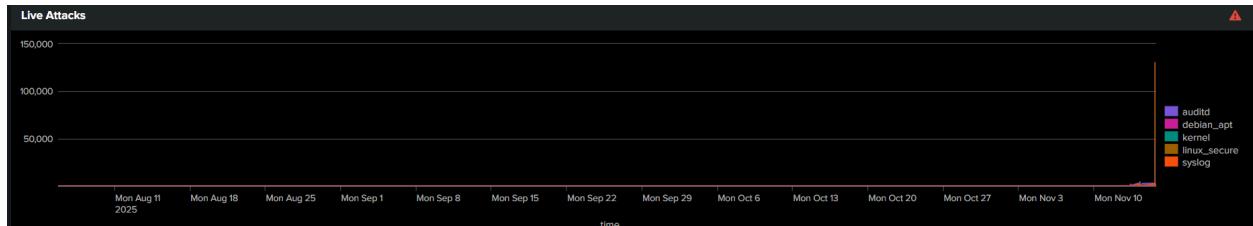
No Event Sampling ▾

📌 Step 6 — Build the Splunk Dashboard

✓ Dashboard Panels:

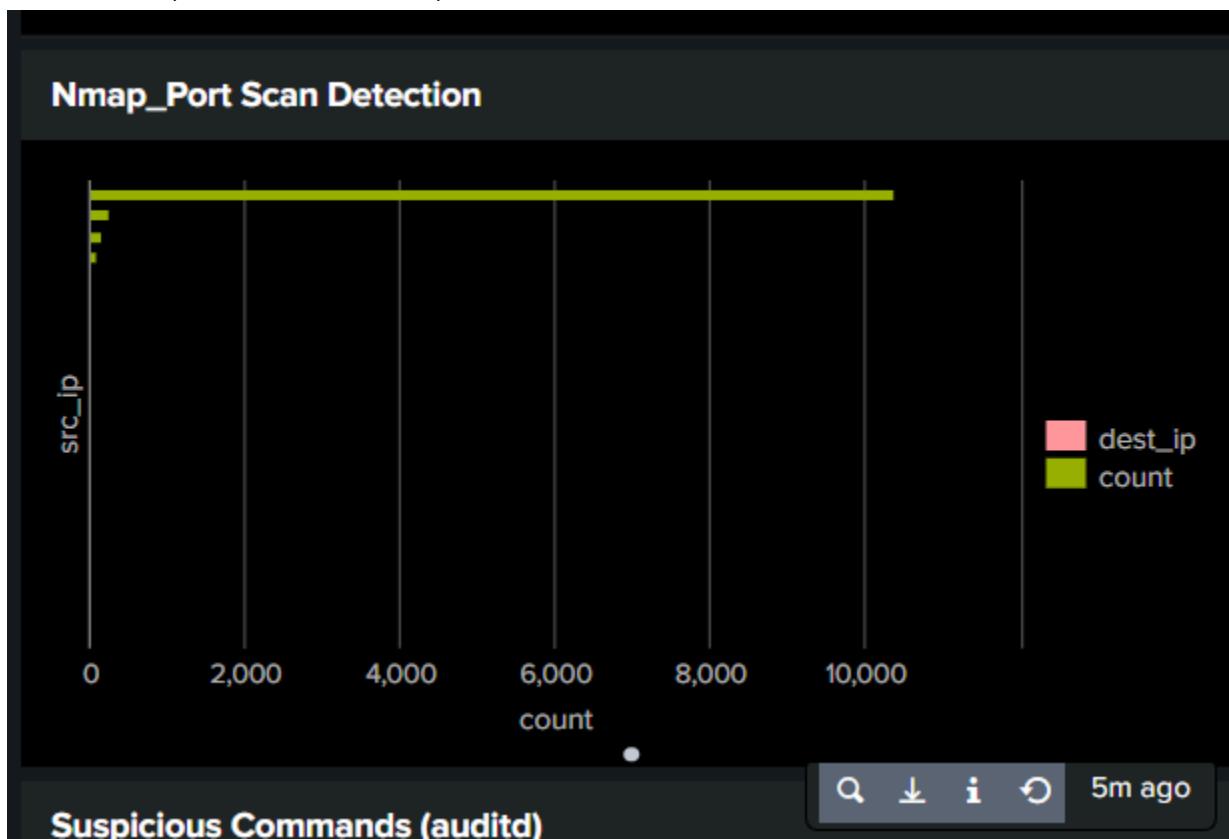
1. Live Attacks Timeline

index=lab | timechart span=1m count BY sourcetype



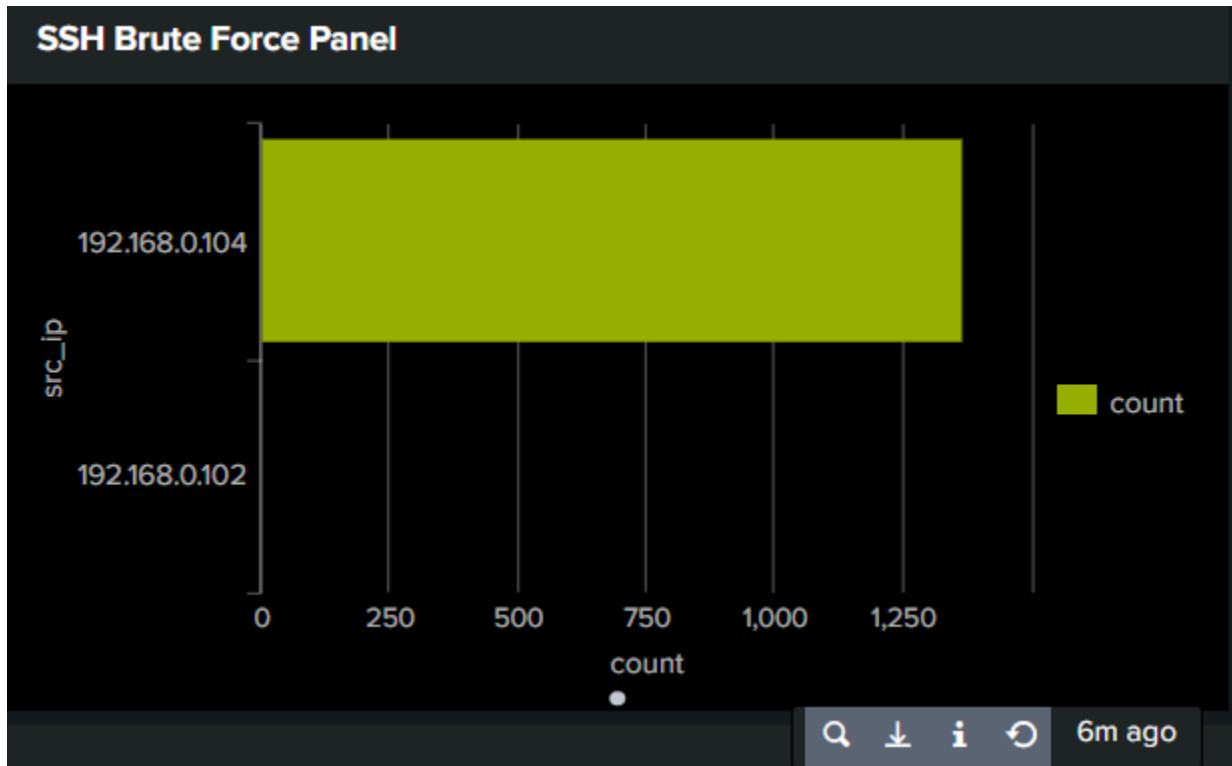
2. Nmap / Port Scan Detection

→ Bar chart (X-axis = Attacker IP)



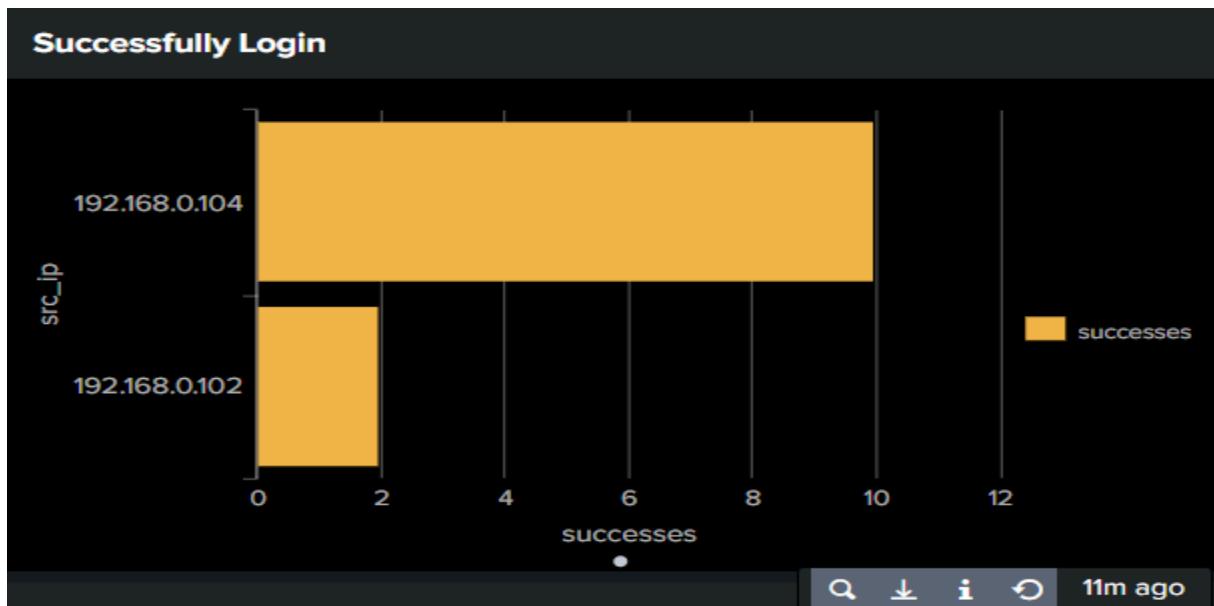
3. SSH Brute Force Panel

→ Column chart (X-axis = src_ip)



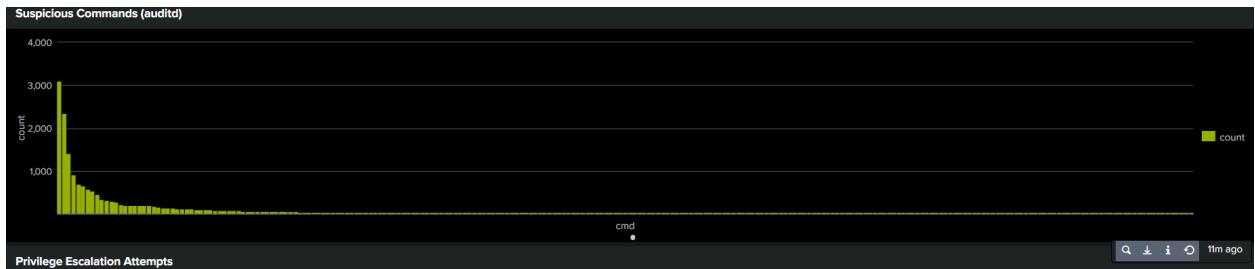
4. Successful Logins

→ Column chart



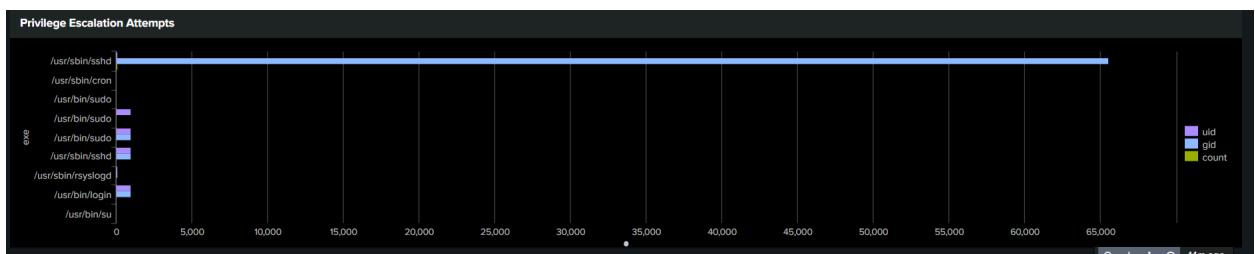
5. Suspicious Commands (auditd)

→ Horizontal bar chart



6. Privilege Escalation Attempts

→ Horizontal bar chart



Step 7 — Final Dashboard Screenshot



Step 9 Result Summary (What This Project Demonstrates)

- ✓ Real-time monitoring of Linux host
- ✓ Detection of real cyber-attacks
- ✓ Log forwarding using Splunk Universal Forwarder
- ✓ Processing of system logs, auth logs, kernel logs, audit logs
- ✓ Visualization of attacks in Splunk dashboards
- ✓ Offense detection:
 - Nmap scans
 - SSH brute force
 - Successful SSH intrusions
 - Suspicious commands
- ✓ Fully functional SIEM use-case simulation

Conclusion

This project successfully demonstrates a **realistic SIEM implementation** from scratch, covering:

- log ingestion
- attack simulation
- threat detection
- visualization
- alerting

It showcases practical SOC skills that are directly applicable in real-world environments.