

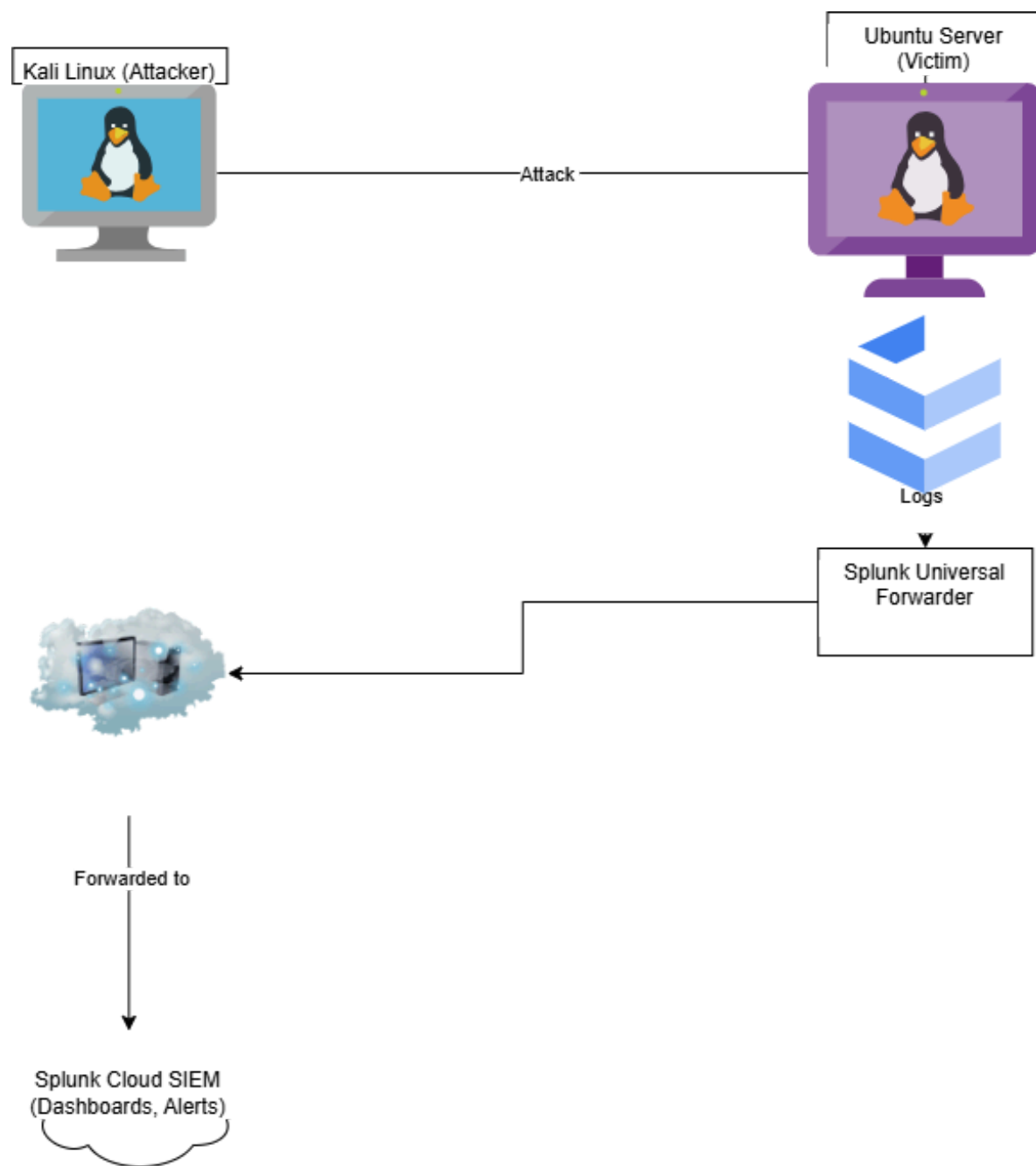
 **SIEM Project (End-to-End  
Implementation): Real-Time Attack  
Monitoring Using Splunk Cloud + Ubuntu  
Server + Kali Linux**

## Introduction

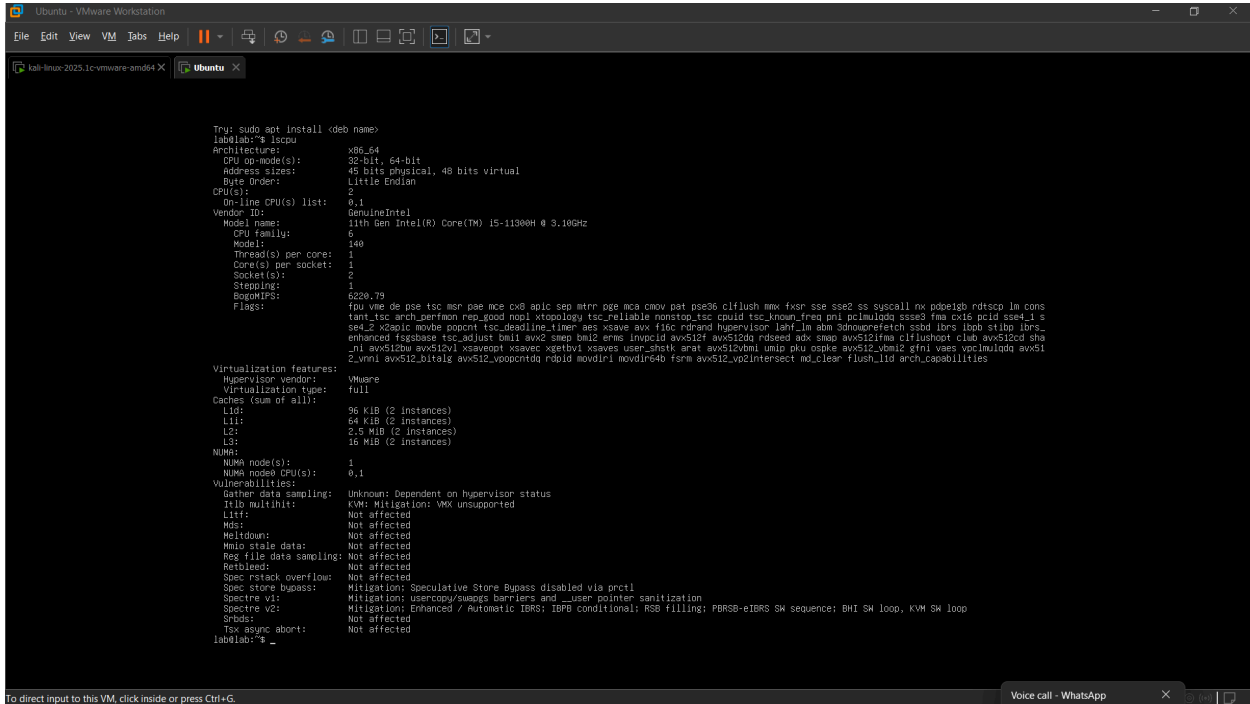
In this project, I built a complete **end-to-end SIEM (Security Information and Event Monitoring) lab** where:

- **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**

## Lab Architecture



## Step 1 — Ubuntu Server Preparation



```
Tru: sudo apt install <deb name>
labelab:~$ lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Address sizes:          48 bits physical, 48 bits virtual
Byte Order:             Little Endian
CPU(s):                 2
On-line CPU(s) list:    0,1
Vendor ID:              GenuineIntel
Model name:             11th Gen Intel(R) Core(TM) i5-11300H @ 3.10GHz
CPU family:             6
Model:                 140
Thread(s) per core:     1
Core(s) per socket:     1
Socket(s):              2
Stepping:               1
BogoMIPS:               6229.79
Flags:                  fpu vme de pse tsc mtr pae mce cx8 apic sep mtrr pge nca cmov pat pse36 clflush mmx fxsr sse sse2 ss syscall nx pdpe1gb rdtscp lm constant_tsc arch_perfmon rep_good nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand hypervisor lahf_lm abm 3dnowprefetch ssbd ibrs ibpb stibp lbrs_...
Virtualization features:
  Hypervisor vendor:    VMware
  Virtualization type:  full
Caches (sum of all):
  L1d:                  36 KiB (2 instances)
  L1i:                  64 KiB (2 instances)
  L2:                   2.5 MiB (2 instances)
  L3:                   16 MiB (2 instances)
NUMA:
  NUMA node(s):         1
  NUMA node0 CPU(s):    0,1
Vulnerabilities:
  Gather data sampling:  Unknown: Dependent on hypervisor status
  Itlb multihit:        KVM: Mitigation: VMX unsupported
  L1tf:                 Not affected
  Mds:                  Not affected
  Meltdown:             Not affected
  Mmio stale data:      Not affected
  Reg file data sampling: Not affected
  Retbleed:             Not affected
  Spec rstack overflow: Not affected
  Spec store bypass:    Mitigation: Speculative Store Bypass disabled via prctl
  Spectre v1:           Mitigation: usercopy/swapgs barriers and __user pointer sanitization
  Spectre v2:           Mitigation: Enhanced / Automatic IBRS; IBPB conditional; RSB filling; FBRSB-eIBRS SW sequence; BHI SW loop, KVM SW loop
  Srbds:                Not affected
  Tsx async abort:      Not affected
labelab:~$ _
```

### Update & upgrade

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

### Install required packages

`sudo apt install ufw auditd 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 ...
verify that this system has all the commands we will require to perform the preflight step
no need to run the splunk-preinstall 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/dimnccache
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

Indexes reside in flat files on the Splunk

Type	Category
Events	Regular
Events	Regular
Events	Regular
Events	Regular
Events	Regular

Add new index

×

\*Name

lab

\*Index data type

☒ Events ☐ Metrics

\*Max raw data size

100

MB

Maximum amount of raw data (uncompressed) the index can contain. The minimum allowable size is 100MB. Enter "0" for no data size limit.

\*Searchable retention (days)

365

↑

↓

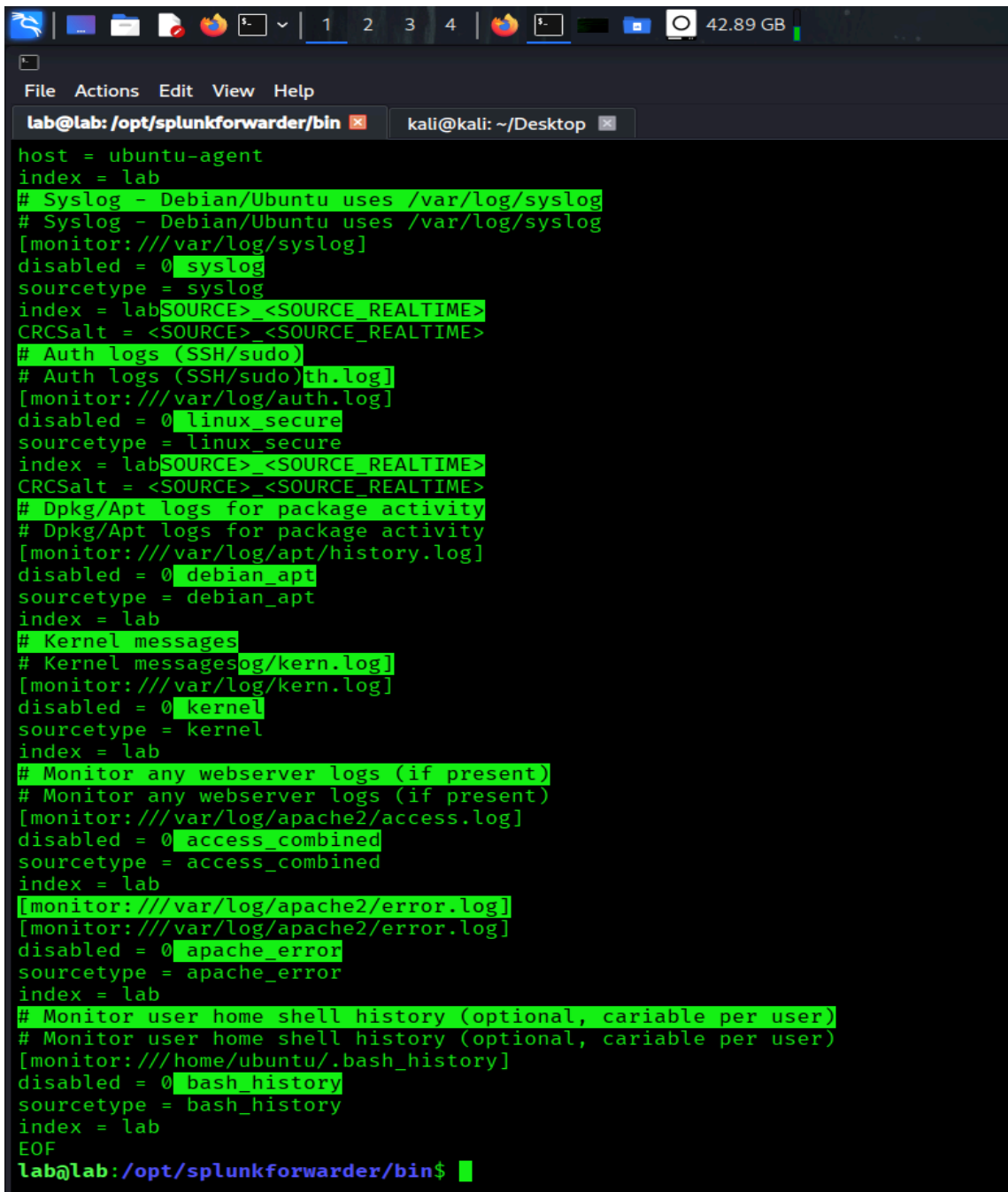
The number of days your data remains in active searchable storage (DDAS).

Cancel

Save

## ✓ Configure log forwarding

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



```
lab@lab: /opt/splunkforwarder/bin | kali@kali: ~/Desktop | 42.89 GB
File Actions Edit View Help
lab@lab: /opt/splunkforwarder/bin | kali@kali: ~/Desktop | 42.89 GB
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 syslog
sourcetype = syslog
index = labSOURCE>_<SOURCE_REALTIME>
CRCSalt = <SOURCE>_<SOURCE_REALTIME>
# Auth logs (SSH/sudo)
# Auth logs (SSH/sudo)th.log]
[monitor:///var/log/auth.log]
disabled = 0 linux_secure
sourcetype = linux_secure
index = labSOURCE>_<SOURCE_REALTIME>
CRCSalt = <SOURCE>_<SOURCE_REALTIME>
# Dpkg/Apt logs for package activity
# Dpkg/Apt logs for package activity
[monitor:///var/log/apt/history.log]
disabled = 0 debian_apt
sourcetype = debian_apt
index = lab
# Kernel messages
# Kernel messagesog/kern.log]
[monitor:///var/log/kern.log]
disabled = 0 kernel
sourcetype = kernel
index = lab
# Monitor any webserver logs (if present)
# Monitor any webserver logs (if present)
[monitor:///var/log/apache2/access.log]
disabled = 0 access_combined
sourcetype = access_combined
index = lab
[monitor:///var/log/apache2/error.log]
[monitor:///var/log/apache2/error.log]
disabled = 0 apache_error
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 bash_history
sourcetype = bash_history
index = lab
EOF
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

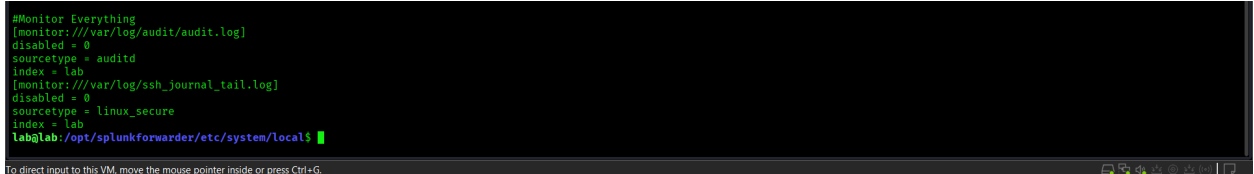
To improve detection i have add this

#### 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
```



```
#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.



```
nmap -sV <ubuntu-ip>
```

The screenshot displays a Kali Linux virtual machine environment. The top menu bar includes File, Edit, View, VM, Tabs, and Help. Below the menu is a toolbar with icons for file operations and VM controls. The main window shows a terminal window titled 'kali@kali: ~/Desktop'. The terminal output shows two Nmap scans performed on the IP address 192.168.0.103. Both scans successfully identified the host as a MikroTik RouterOS 7.5. The terminal text is as follows:

```

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 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
MAC Address: 08:0C:29:DD:79:EA (VMware)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:6 cpe:/o:mikrotik:routeros: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 - 7.5 (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 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
MAC Address: 08:0C:29:DD:79:EA (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:6 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

kali@kali:~/Desktop
$

```

The bottom status bar of the VM window indicates 'To direct input to this VM, move the mouse pointer inside or press Ctrl+G.'

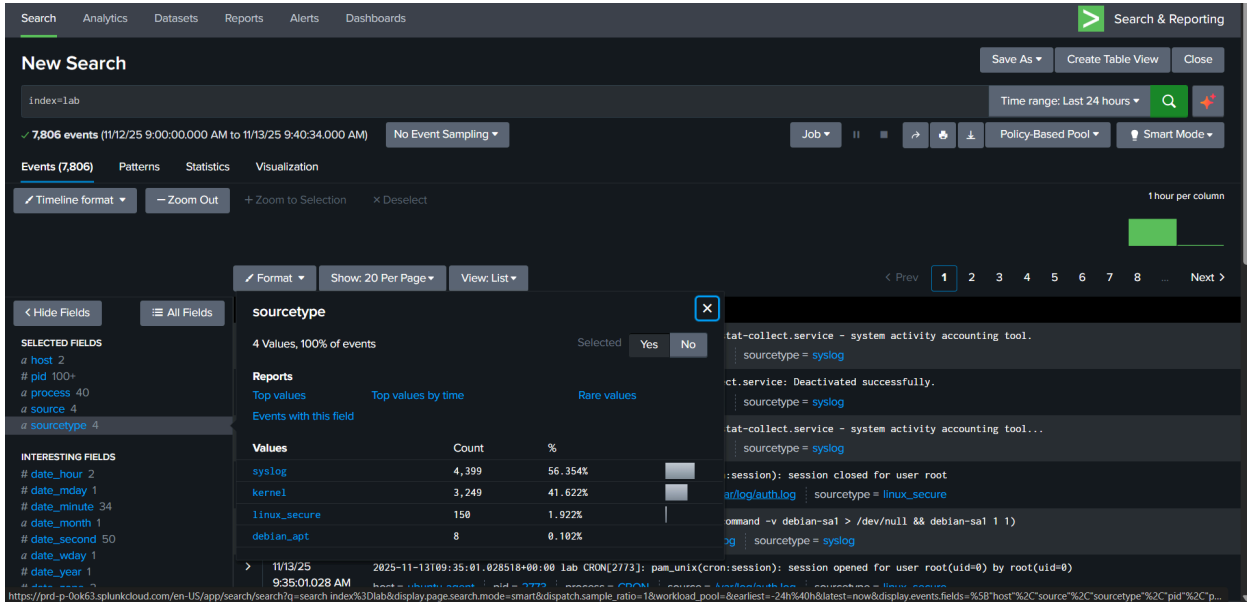


```
ssh lab@<ubuntu-ip>
```

## # Enter wrong password multiple times

```
└─(kali㉿kali)-[~/Desktop]
└─$ ssh lab@192.168.0.103
lab@192.168.0.103's password:
sPermission 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)



The screenshot shows the Splunk Search interface. At the top, there's a navigation bar with tabs for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The 'Search' tab is active. Below the navigation bar, there's a 'New Search' section. The search bar contains 'index=lab'. The time range is set to 'Last 24 hours'. The search results show 7,806 events. The interface includes a sidebar with field lists, a main search bar, and a results table.

**Search Query:** `index=lab`

**Results:** 7,806 events (11/12/25 9:00:00.000 AM to 11/13/25 9:40:34.000 AM)

**Fields:**

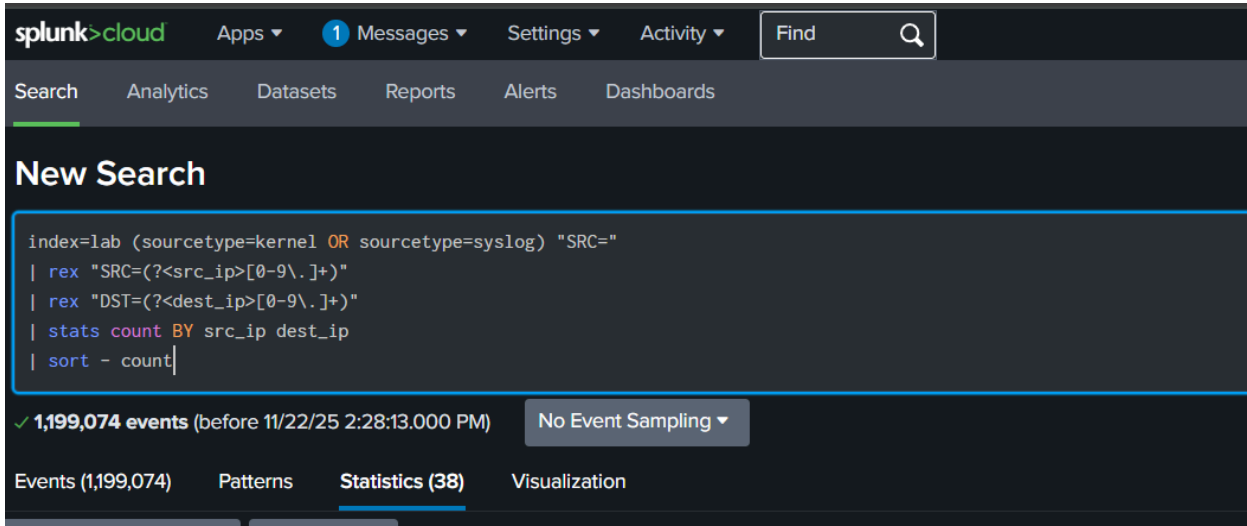
- SELECTED FIELDS: host 2, pid 100+, process 40, source 4, sourcetype 4
- INTERESTING FIELDS: date\_hour 2, date\_mday 1, date\_minute 34, date\_month 1, date\_second 50, date\_wday 1, date\_year 1

**Table:**

Values	Count	%
syslog	4,399	56.354%
kernel	3,249	41.622%
linux_secure	150	1.922%
debian_apt	8	0.102%

## 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
```



The screenshot shows the Splunk Search interface. At the top, there's a navigation bar with tabs for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The 'Search' tab is active. Below the navigation bar, there's a 'New Search' section. The search bar contains the query: `index=lab (sourcetype=kernel OR sourcetype=syslog) "SRC="`. The time range is set to 'before 11/22/25 2:28:13.000 PM'. The search results show 1,199,074 events. The interface includes a sidebar with field lists, a main search bar, and a results table.

**Search Query:** `index=lab (sourcetype=kernel OR sourcetype=syslog) "SRC="`

**Results:** 1,199,074 events (before 11/22/25 2:28:13.000 PM)

**Fields:**

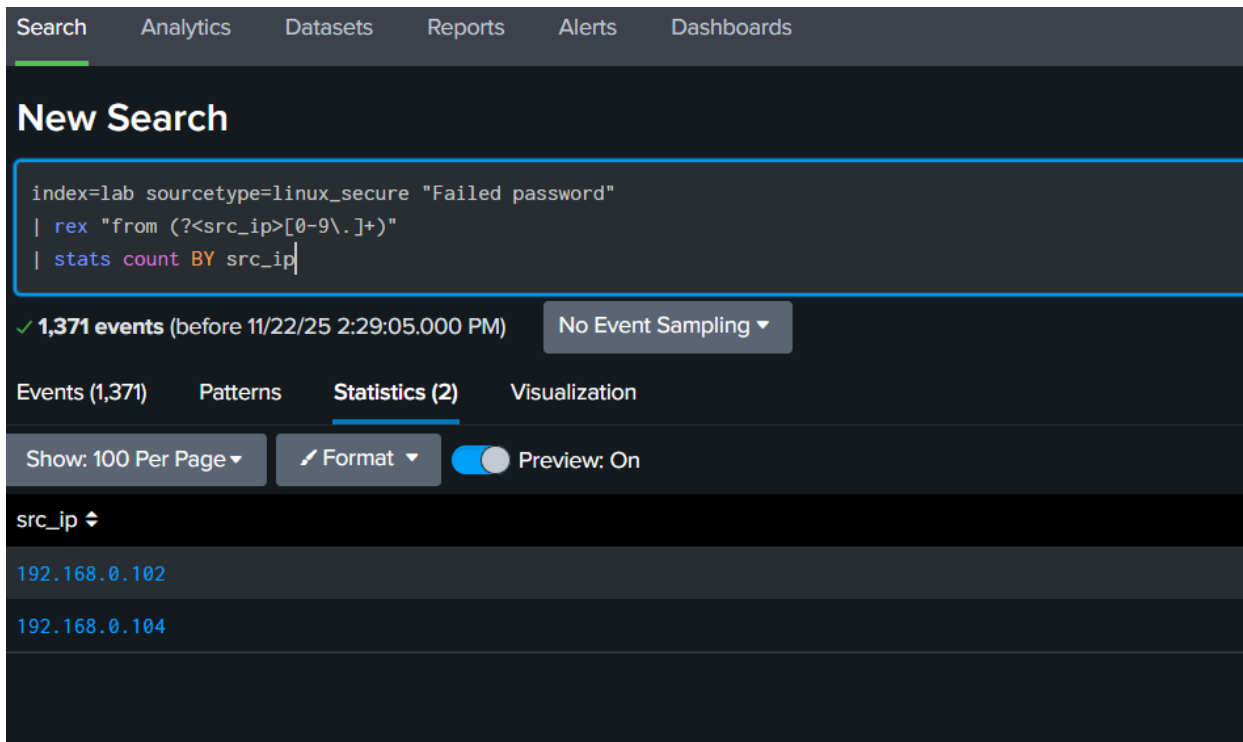
- SELECTED FIELDS: host 2, pid 100+, process 40, source 4, sourcetype 4
- INTERESTING FIELDS: date\_hour 2, date\_mday 1, date\_minute 34, date\_month 1, date\_second 50, date\_wday 1, date\_year 1

**Table:**

Values	Count	%
syslog	4,399	56.354%
kernel	3,249	41.622%
linux_secure	150	1.922%
debian_apt	8	0.102%

## SSH Brute Force Attempts

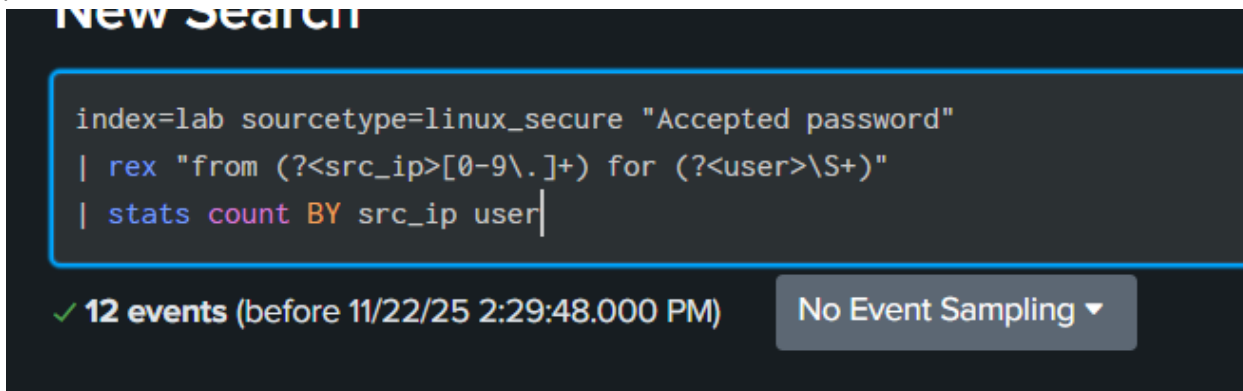
```
index=lab sourcetype=linux_secure "Failed password"  
| rex "from (?<src_ip>[0-9\.]++)"  
| stats count BY src_ip
```



The screenshot shows the Splunk Search interface. At the top, there are tabs for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The Search tab is active. Below the tabs, the search query is displayed in a text box: `index=lab sourcetype=linux_secure "Failed password"`, `| rex "from (?<src_ip>[0-9\.]++)"`, and `| stats count BY src_ip`. Below the query box, it shows **1,371 events** (before 11/22/25 2:29:05.000 PM) and a **No Event Sampling** dropdown. Below this, there are tabs for Events (1,371), Patterns, **Statistics (2)**, and Visualization. The Statistics tab is active. Below the tabs, there are controls for **Show: 100 Per Page**, **Format** (dropdown), and **Preview: On** (toggle). Below these controls, the search results are displayed as a table with the column **src\_ip**. The results show two unique IP addresses: **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 the Splunk Search interface. At the top, there are tabs for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The Search tab is active. Below the tabs, the search query is displayed in a text box: `index=lab sourcetype=linux_secure "Accepted password"`, `| rex "from (?<src_ip>[0-9\.]++) for (?<user>\S+)"`, and `| stats count BY src_ip user`. Below the query box, it shows **12 events** (before 11/22/25 2:29:48.000 PM) and a **No Event Sampling** dropdown.



## 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)

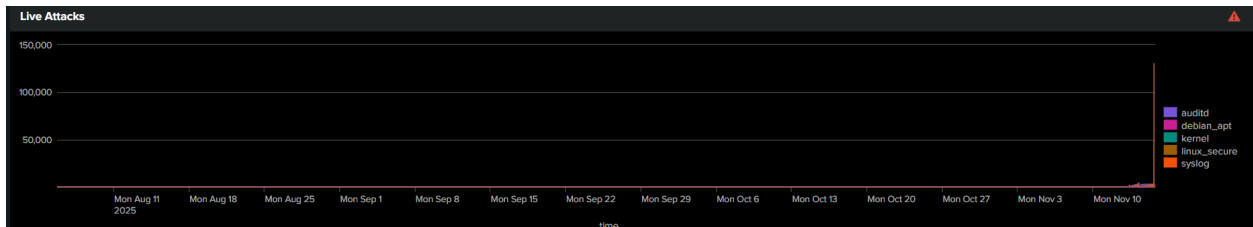
No Event Sampling ▼

## 📌 Step 6 — Build the Splunk Dashboard

### ✓ Dashboard Panels:

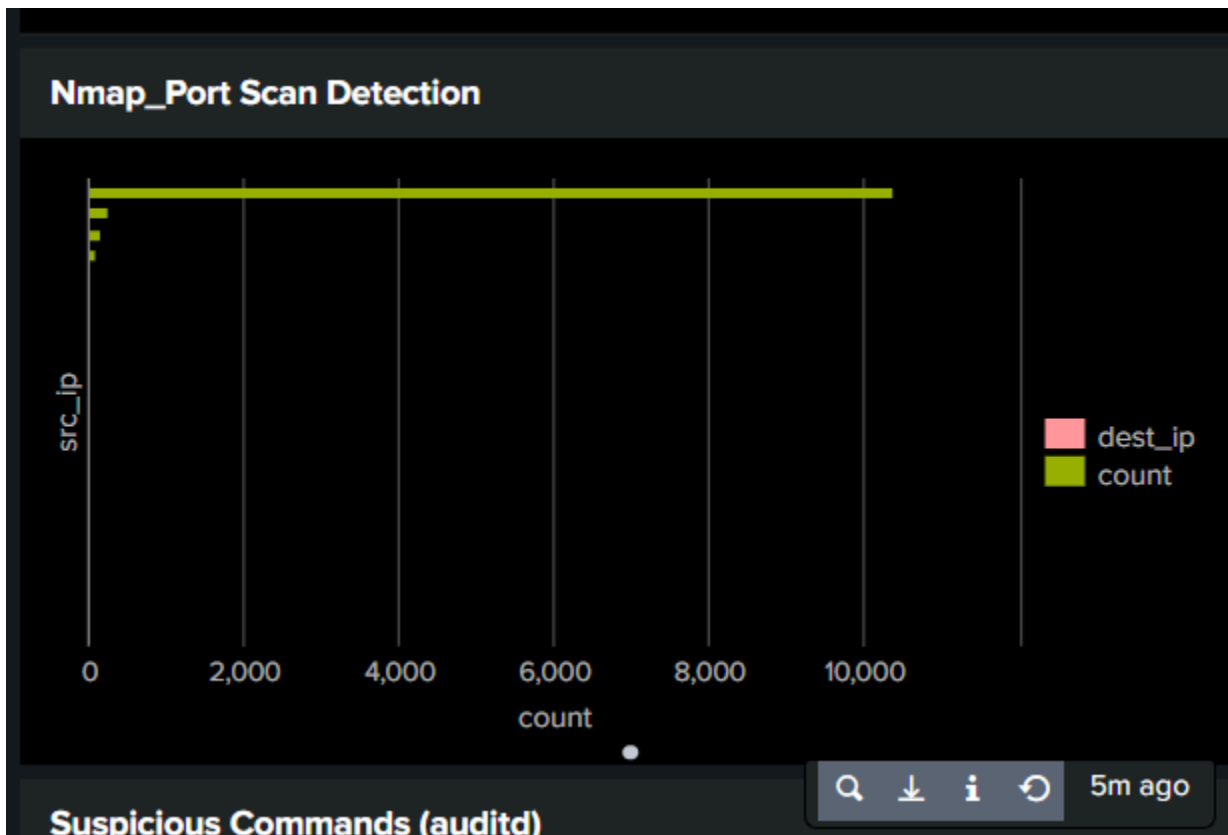
#### 1. Live Attacks Timeline

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



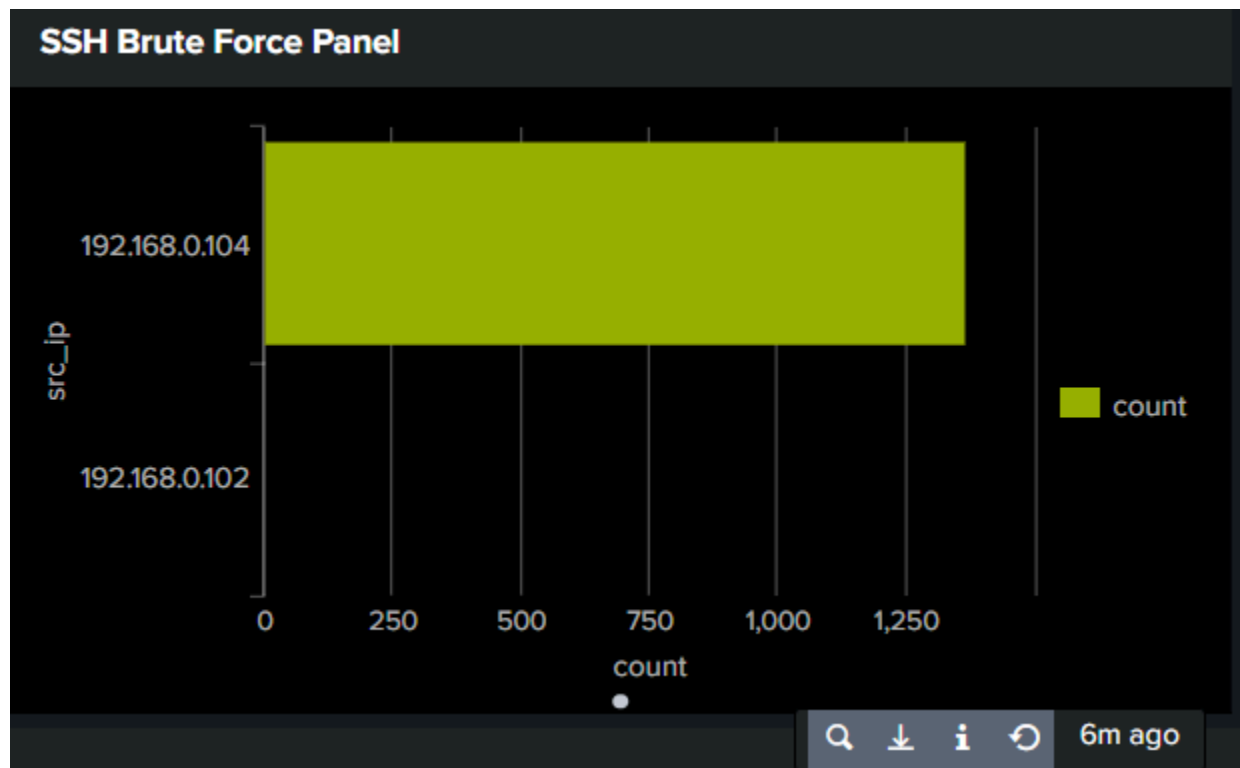
#### 2. Nmap / Port Scan Detection

→ Bar chart (X-axis = Attacker IP)



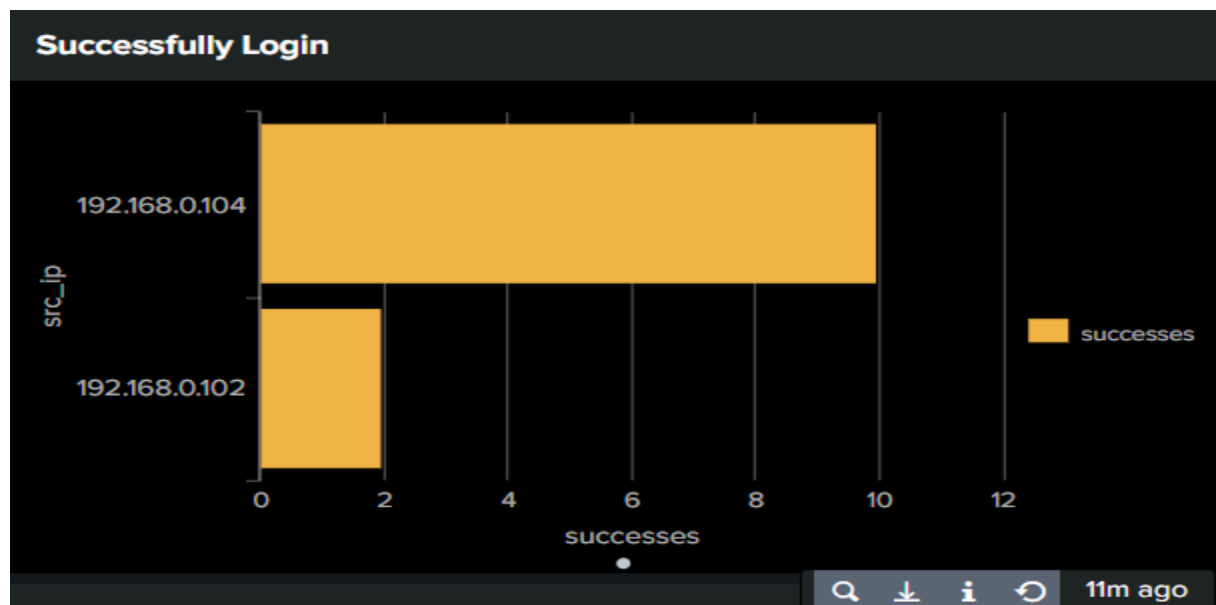
### 3. SSH Brute Force Panel

→ Column chart (X-axis = src\_ip)



### 4. Successful Logins

→ Column chart



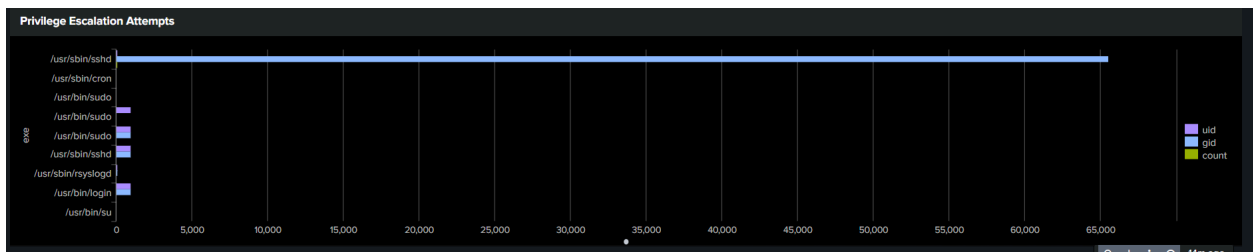
## 5. Suspicious Commands (auditd)

→ 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.