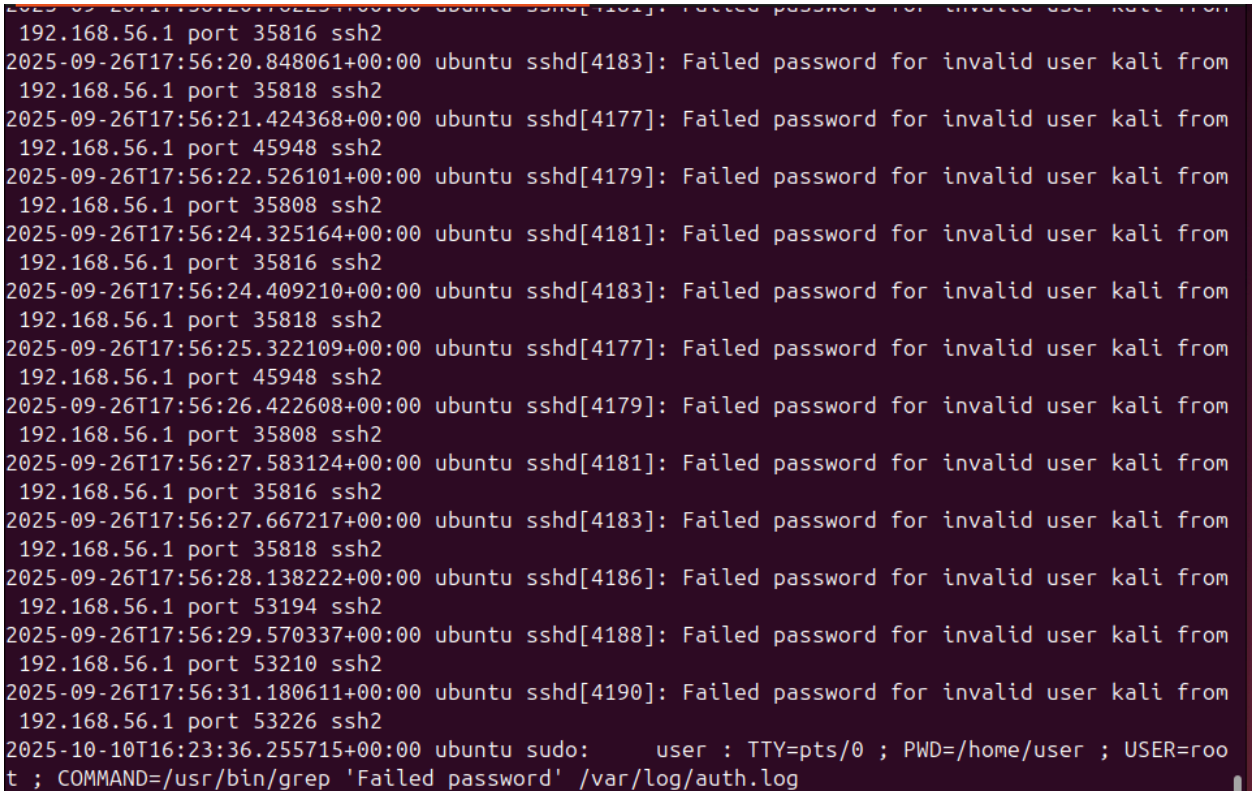
Part 1

1. Auth.log, syslog, cron.log
2.

```
user@ubuntu:~$ cat /etc/rsyslog.conf | grep -v '^#'



module(load="imuxsock") # provides support for local system logging



module(load="imklog" permitnonkernelfacility="on")


$RepeatedMsgReduction on

$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

$WorkDirectory /var/spool/rsyslog

$IncludeConfig /etc/rsyslog.d/*.conf
user@ubuntu:~$
```

Part 2

1. 
192.168.56.1 port 35816 ssh2
2025-09-26T17:56:20.848061+00:00 ubuntu sshd[4183]: Failed password for invalid user kali from
192.168.56.1 port 35818 ssh2
2025-09-26T17:56:21.424368+00:00 ubuntu sshd[4177]: Failed password for invalid user kali from
192.168.56.1 port 45948 ssh2
2025-09-26T17:56:22.526101+00:00 ubuntu sshd[4179]: Failed password for invalid user kali from
192.168.56.1 port 35808 ssh2
2025-09-26T17:56:24.325164+00:00 ubuntu sshd[4181]: Failed password for invalid user kali from
192.168.56.1 port 35816 ssh2
2025-09-26T17:56:24.409210+00:00 ubuntu sshd[4183]: Failed password for invalid user kali from
192.168.56.1 port 35818 ssh2
2025-09-26T17:56:25.322109+00:00 ubuntu sshd[4177]: Failed password for invalid user kali from
192.168.56.1 port 45948 ssh2
2025-09-26T17:56:26.422608+00:00 ubuntu sshd[4179]: Failed password for invalid user kali from
192.168.56.1 port 35808 ssh2
2025-09-26T17:56:27.583124+00:00 ubuntu sshd[4181]: Failed password for invalid user kali from
192.168.56.1 port 35816 ssh2
2025-09-26T17:56:27.667217+00:00 ubuntu sshd[4183]: Failed password for invalid user kali from
192.168.56.1 port 35818 ssh2
2025-09-26T17:56:28.138222+00:00 ubuntu sshd[4186]: Failed password for invalid user kali from
192.168.56.1 port 53194 ssh2
2025-09-26T17:56:29.570337+00:00 ubuntu sshd[4188]: Failed password for invalid user kali from
192.168.56.1 port 53210 ssh2
2025-09-26T17:56:31.180611+00:00 ubuntu sshd[4190]: Failed password for invalid user kali from
192.168.56.1 port 53226 ssh2
2025-10-10T16:23:36.255715+00:00 ubuntu sudo: user : TTY=pts/0 ; PWD=/home/user ; USER=roo
t ; COMMAND=/usr/bin/grep 'Failed password' /var/log/auth.log

2. 192.168.56.1

```
2025-09-26T16:47:34.639675+00:00 ubuntu sshd[4661]: Accepted password for alice from 192.168.5
6.4 port 44180 ssh2
2025-09-26T16:51:14.632449+00:00 ubuntu sshd[4947]: Accepted password for alice from 192.168.5
6.4 port 40870 ssh2
2025-09-26T16:53:55.603589+00:00 ubuntu sshd[5243]: Accepted password for bob from 192.168.56.
4 port 51242 ssh2
2025-09-26T16:54:56.761438+00:00 ubuntu sshd[5552]: Accepted password for charlie from 192.168
.56.4 port 44536 ssh2
2025-09-26T16:56:12.476778+00:00 ubuntu sshd[5872]: Accepted password for alice from 192.168.5
6.4 port 58448 ssh2
2025-09-26T16:56:20.041305+00:00 ubuntu sshd[6064]: Accepted password for bob from 192.168.56.
4 port 39748 ssh2
2025-09-26T16:56:23.771795+00:00 ubuntu sshd[6072]: Accepted password for charlie from 192.168
.56.4 port 39770 ssh2
2025-09-26T17:48:32.056978+00:00 ubuntu sshd[2645]: Accepted password for alice from 192.168.5
6.1 port 43668 ssh2
2025-09-26T17:48:41.636407+00:00 ubuntu sshd[2858]: Accepted password for bob from 192.168.56.
1 port 39348 ssh2
2025-09-26T17:48:43.918803+00:00 ubuntu sshd[3081]: Accepted password for charlie from 192.168
.56.1 port 39412 ssh2
2025-09-26T17:50:43.005901+00:00 ubuntu sshd[3348]: Accepted password for alice from 192.168.5
6.1 port 48126 ssh2
2025-09-26T17:53:01.368289+00:00 ubuntu sshd[3641]: Accepted password for bob from 192.168.56.
1 port 50074 ssh2
2025-09-26T17:53:59.563995+00:00 ubuntu sshd[3890]: Accepted password for charlie from 192.168
.56.1 port 53664 ssh2
2025-10-10T16:25:42.823729+00:00 ubuntu sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=roo
t ; COMMAND=/usr/bin/grep 'Accepted password' /var/log/auth.log
user@ubuntu:~$
```

3.

```
user@ubuntu:~$ sudo awk '/Failed password/{print $(NF-3)}' /var/log/auth.log | sort | uniq -c
| sort -nr | head
    980 192.168.56.4
    532 192.168.56.1
      2 '/Failed
      1 COMMAND=/usr/bin/grep
user@ubuntu:~$
```

```
user@ubuntu:~$ sudo grep "sudo" /var/log/auth.log | grep "COMMAND"
2025-09-26T07:32:03.963436+00:00 localhost sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=
root ; COMMAND=/usr/bin/apt update
2025-09-26T07:32:06.826502+00:00 localhost sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=
root ; COMMAND=/usr/bin/apt upgrade -y
2025-09-26T07:33:17.692186+00:00 localhost sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=
root ; COMMAND=/usr/bin/apt install neovim
2025-09-26T16:12:33.448515+00:00 ubuntu sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=roo
t ; COMMAND=/usr/bin/apt install net-tools
2025-09-26T16:13:41.710038+00:00 ubuntu sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=roo
t ; COMMAND=/usr/bin/systemctl status ssh
2025-09-26T16:13:50.881553+00:00 ubuntu sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=roo
t ; COMMAND=/usr/bin/systemctl start ssh
2025-09-26T16:14:02.900484+00:00 ubuntu sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=roo
t ; COMMAND=/usr/bin/systemctl status sshd
2025-09-26T16:14:27.773861+00:00 ubuntu sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=roo
t ; COMMAND=/usr/bin/apt update
2025-09-26T16:14:44.657574+00:00 ubuntu sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=roo
t ; COMMAND=/usr/bin/apt install openssh-server -y
2025-09-26T16:15:05.989315+00:00 ubuntu sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=roo
t ; COMMAND=/usr/bin/systemctl status ssh
2025-09-26T16:15:09.883006+00:00 ubuntu sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=roo
t ; COMMAND=/usr/bin/systemctl start ssh
2025-09-26T16:25:18.892242+00:00 ubuntu sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=roo
t ; COMMAND=/usr/bin/systemctl status ssh
2025-09-26T16:32:52.184992+00:00 ubuntu sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=roo
t ; COMMAND=/usr/sbin/useradd -m -s /bin/bash alice
```

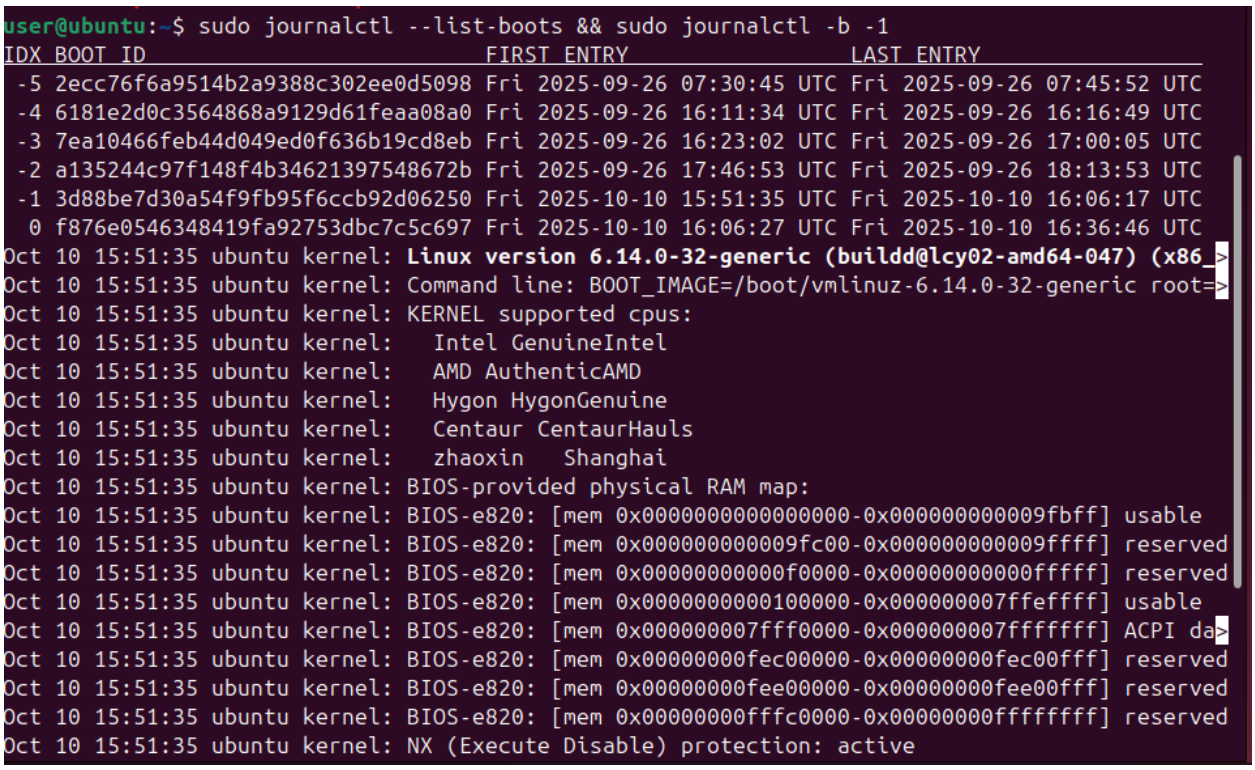
4.

5. no

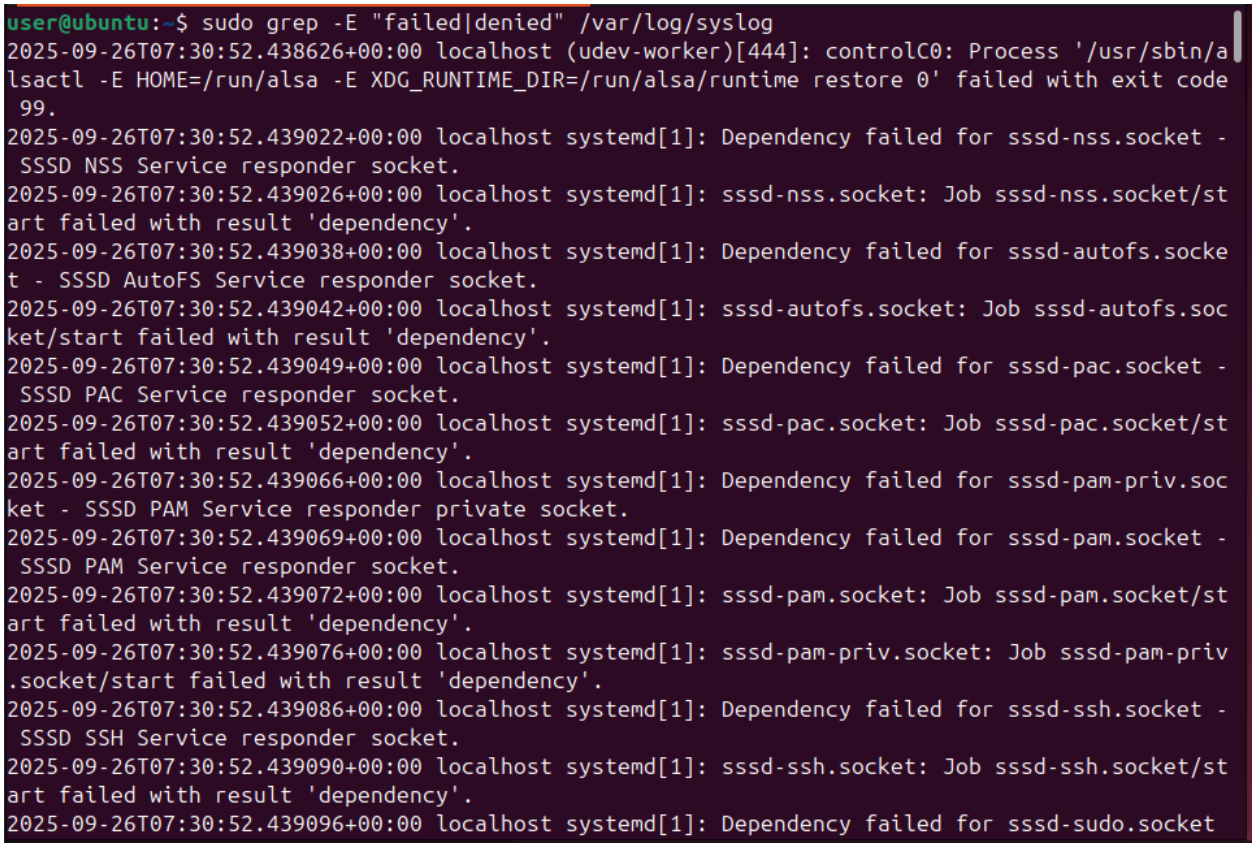
```
user@ubuntu:~$ sudo journalctl -b -1 && sudo tail -n 50 /var/log.syslog
Oct 10 15:51:35 ubuntu kernel: Linux version 6.14.0-32-generic (buildd@lcy02-amd64-047) (x86_>
Oct 10 15:51:35 ubuntu kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.14.0-32-generic root=>
Oct 10 15:51:35 ubuntu kernel: KERNEL supported cpus:
Oct 10 15:51:35 ubuntu kernel:   Intel GenuineIntel
Oct 10 15:51:35 ubuntu kernel:   AMD AuthenticAMD
Oct 10 15:51:35 ubuntu kernel:   Hygon HygonGenuine
Oct 10 15:51:35 ubuntu kernel:   Centaur CentaurHauls
Oct 10 15:51:35 ubuntu kernel:   zhaoxin   Shanghai
Oct 10 15:51:35 ubuntu kernel: BIOS-provided physical RAM map:
Oct 10 15:51:35 ubuntu kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Oct 10 15:51:35 ubuntu kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Oct 10 15:51:35 ubuntu kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Oct 10 15:51:35 ubuntu kernel: BIOS-e820: [mem 0x0000000000100000-0x000000007ffeffff] usable
Oct 10 15:51:35 ubuntu kernel: BIOS-e820: [mem 0x000000007fff0000-0x000000007fffffff] ACPI da>
Oct 10 15:51:35 ubuntu kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Oct 10 15:51:35 ubuntu kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Oct 10 15:51:35 ubuntu kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Oct 10 15:51:35 ubuntu kernel: NX (Execute Disable) protection: active
Oct 10 15:51:35 ubuntu kernel: APIC: Static calls initialized
Oct 10 15:51:35 ubuntu kernel: SMBIOS 2.5 present.
Oct 10 15:51:35 ubuntu kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01>
Oct 10 15:51:35 ubuntu kernel: DMI: Memory slots populated: 0/0
Oct 10 15:51:35 ubuntu kernel: Hypervisor detected: KVM
```

Part 3

1. No unexpected reboots



2. Sssd.service failure, probably with wrong configuration as it failed with result “dependency”



```
user@ubuntu:~$ sudo grep -E "failed|denied" /var/log/syslog
2025-09-26T07:30:52.438626+00:00 localhost (udev-worker)[444]: controlC0: Process '/usr/sbin/a
lsactl -E HOME=/run/alsa -E XDG_RUNTIME_DIR=/run/alsa/runtime restore 0' failed with exit code
 99.
2025-09-26T07:30:52.439022+00:00 localhost systemd[1]: Dependency failed for sssd-nss.socket -
 SSSD NSS Service responder socket.
2025-09-26T07:30:52.439026+00:00 localhost systemd[1]: sssd-nss.socket: Job sssd-nss.socket/st
art failed with result 'dependency'.
2025-09-26T07:30:52.439038+00:00 localhost systemd[1]: Dependency failed for sssd-autofs.socke
t - SSSD AutoFS Service responder socket.
2025-09-26T07:30:52.439042+00:00 localhost systemd[1]: sssd-autofs.socket: Job sssd-autofs.soc
ket/start failed with result 'dependency'.
2025-09-26T07:30:52.439049+00:00 localhost systemd[1]: Dependency failed for sssd-pac.socket -
 SSSD PAC Service responder socket.
2025-09-26T07:30:52.439052+00:00 localhost systemd[1]: sssd-pac.socket: Job sssd-pac.socket/st
art failed with result 'dependency'.
2025-09-26T07:30:52.439066+00:00 localhost systemd[1]: Dependency failed for sssd-pam-priv.soc
ket - SSSD PAM Service responder private socket.
2025-09-26T07:30:52.439069+00:00 localhost systemd[1]: Dependency failed for sssd-pam.socket -
 SSSD PAM Service responder socket.
2025-09-26T07:30:52.439072+00:00 localhost systemd[1]: sssd-pam.socket: Job sssd-pam.socket/st
art failed with result 'dependency'.
2025-09-26T07:30:52.439076+00:00 localhost systemd[1]: sssd-pam-priv.socket: Job sssd-pam-priv
.socket/start failed with result 'dependency'.
2025-09-26T07:30:52.439086+00:00 localhost systemd[1]: Dependency failed for sssd-ssh.socket -
 SSSD SSH Service responder socket.
2025-09-26T07:30:52.439090+00:00 localhost systemd[1]: sssd-ssh.socket: Job sssd-ssh.socket/st
art failed with result 'dependency'.
2025-09-26T07:30:52.439096+00:00 localhost systemd[1]: Dependency failed for sssd-sudo.socket
```

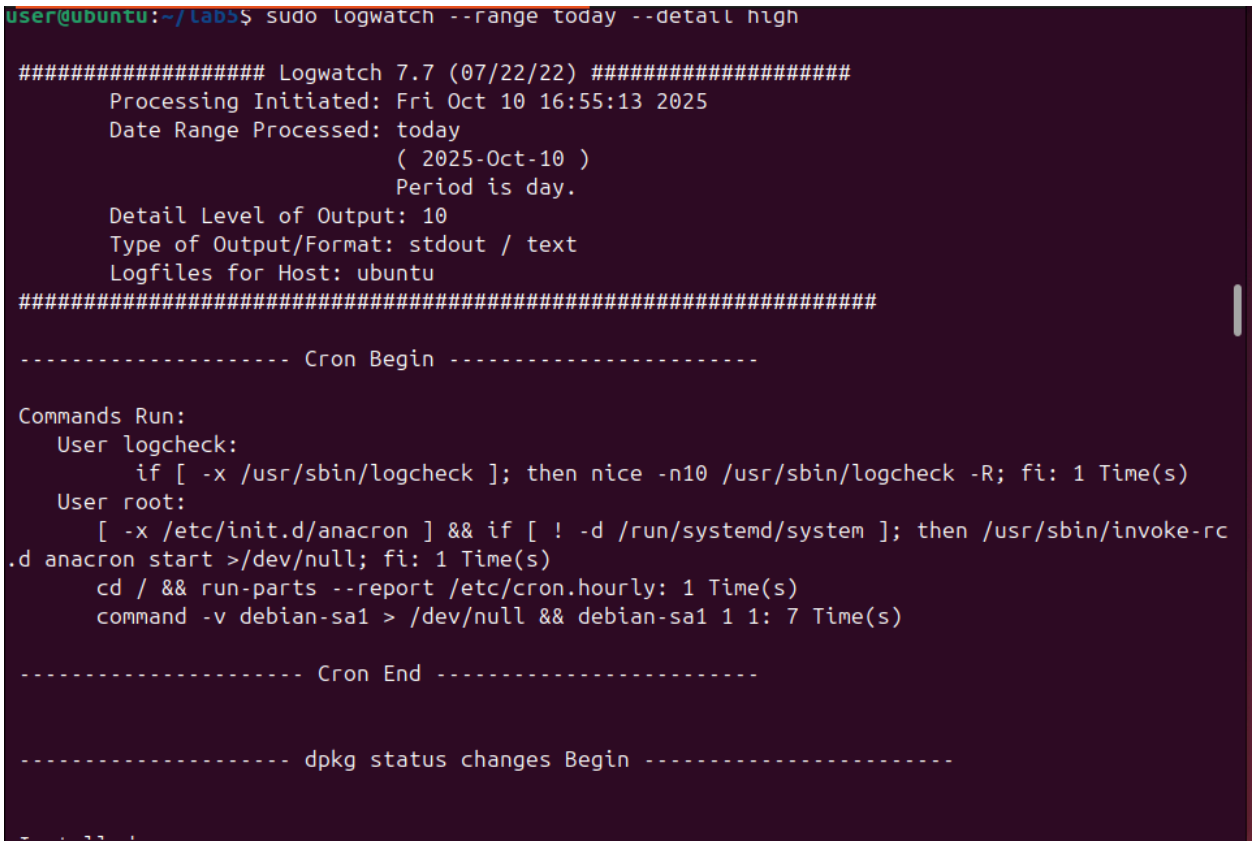
3. No password changed after system reboot

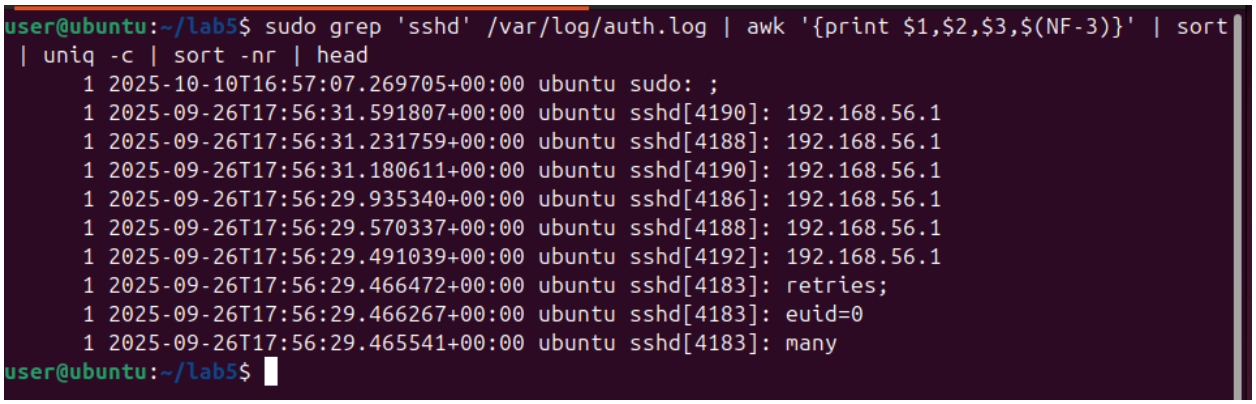
```
user@ubuntu:~$ sudo auditctl -w /etc/passwd -p war -k passwd_changes
user@ubuntu:~$ sudo ausearch -l passwd_changes
passwd_changes is an unsupported option
user@ubuntu:~$ sudo ausearch -k passwd_changes
----
time->Fri Oct 10 16:42:39 2025
type=PROCTITLE msg=audit(1760114559.108:473): proctitle=617564697463746C002D77002F6574632F7061
73737764002D7000776172002D6B007061737377645F6368616E676573
type=SYSCALL msg=audit(1760114559.108:473): arch=c000003e syscall=44 success=yes exit=1084 a0=
4 a1=7ffda91cf6c0 a2=43c a3=0 items=0 ppid=4474 pid=4475 auid=1000 uid=0 gid=0 euid=0 suid=0 f
suid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=4 comm="auditctl" exe="/usr/sbin/auditctl" subj=unco
nfined key=(null)
type=CONFIG_CHANGE msg=audit(1760114559.108:473): auid=1000 ses=4 subj=unconfined op=add_rule
key="passwd_changes" list=4 res=1
----
time->Fri Oct 10 16:42:51 2025
type=PROCTITLE msg=audit(1760114571.241:476): proctitle=7375646F006175736561726368002D6C007061
737377645F6368616E676573
type=PATH msg=audit(1760114571.241:476): item=0 name="/etc/passwd" inode=396261 dev=08:02 mode
=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_fr
ootid=0
type=CWD msg=audit(1760114571.241:476): cwd="/home/user"
type=SYSCALL msg=audit(1760114571.241:476): arch=c000003e syscall=257 success=yes exit=3 a0=ff
ffff9c a1=7ec216dcf320 a2=80000 a3=0 items=1 ppid=4068 pid=4479 auid=1000 uid=1000 gid=1000 eu
id=0 suid=0 fsuid=0 egid=1000 sgid=1000 fsgid=1000 tty=pts0 ses=4 comm="sudo" exe="/usr/bin/su
do" subj=unconfined key="passwd_changes"
----
time->Fri Oct 10 16:42:51 2025
type=PROCTITLE msg=audit(1760114571.244:477): proctitle=7375646F006175736561726368002D6C007061
```

Part 4

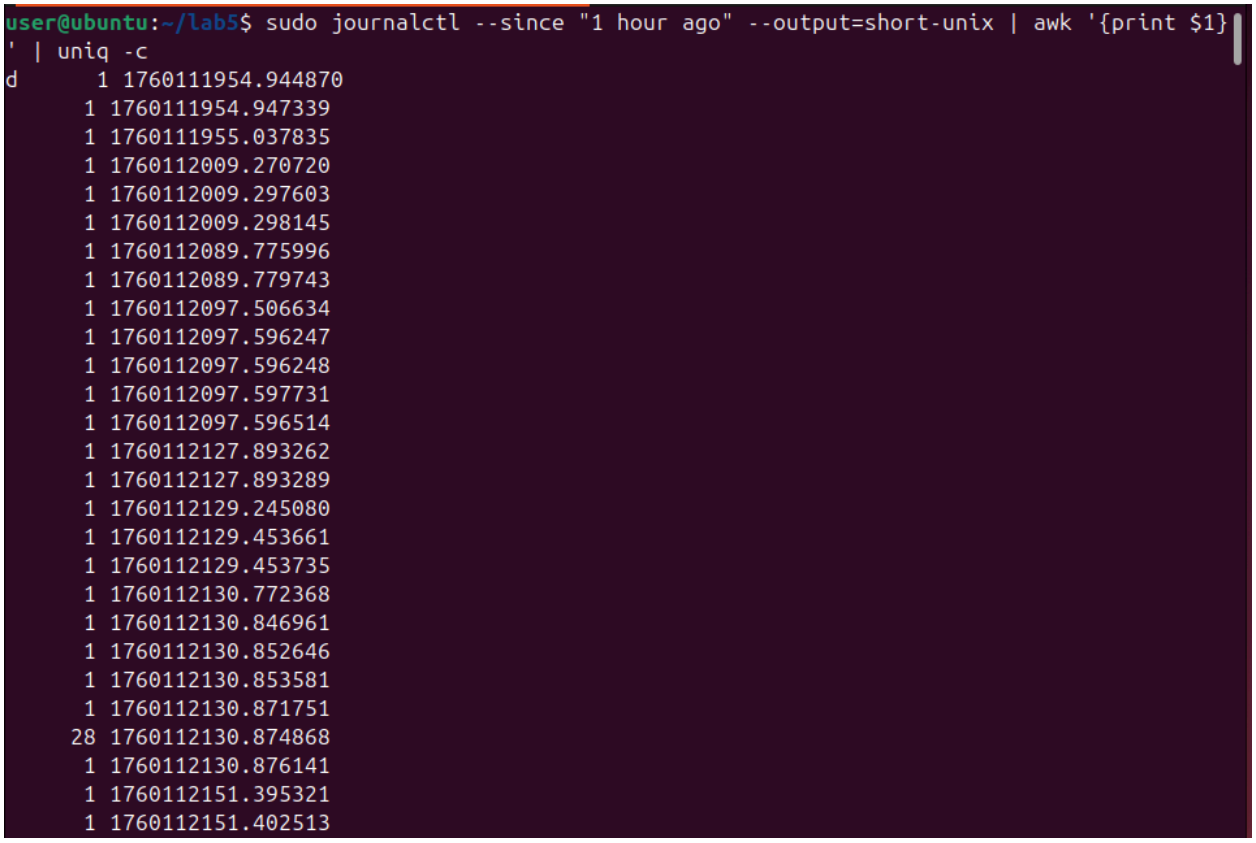
```
user@ubuntu:~/lab5$ sudo ./part4.sh
Failed Logins
    980 192.168.56.4
    532 192.168.56.1
      2 '/Failed
      1 COMMAND=/usr/bin/grep

Sucessful Logins
     10 192.168.56.4
      6 192.168.56.1
      1 COMMAND=/usr/bin/grep

Sudo Attempts
2025-09-26T07:32:03.963436+00:00 localhost sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=
root ; COMMAND=/usr/bin/apt update
2025-09-26T07:32:06.826502+00:00 localhost sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=
root ; COMMAND=/usr/bin/apt upgrade -y
2025-09-26T07:33:17.692186+00:00 localhost sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=
root ; COMMAND=/usr/bin/apt install neovim
2025-09-26T16:12:33.448515+00:00 ubuntu sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=roo
t ; COMMAND=/usr/bin/apt install net-tools
2025-09-26T16:13:41.710038+00:00 ubuntu sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=roo
t ; COMMAND=/usr/bin/systemctl status ssh
2025-09-26T16:13:50.881553+00:00 ubuntu sudo:     user : TTY=pts/0 ; PWD=/home/user ; USER=roo
t ; COMMAND=/usr/bin/systemctl start ssh
```

Part 5

1. 
user@ubuntu:~/lab5$ sudo logwatch --range today --detail high
################### Logwatch 7.7 (07/22/22) ####################
Processing Initiated: Fri Oct 10 16:55:13 2025
Date Range Processed: today
(2025-Oct-10)
Period is day.
Detail Level of Output: 10
Type of Output/Format: stdout / text
Logfiles for Host: ubuntu
##
---------- Cron Begin ----------
Commands Run:
User logcheck:
if [-x /usr/sbin/logcheck]; then nice -n10 /usr/sbin/logcheck -R; fi: 1 Time(s)
User root:
[-x /etc/init.d/anacron] && if [! -d /run/systemd/system]; then /usr/sbin/invoke-rc
.d anacron start >/dev/null; fi: 1 Time(s)
cd / && run-parts --report /etc/cron.hourly: 1 Time(s)
command -v debian-sa1 > /dev/null && debian-sa1 1 1: 7 Time(s)
---------- Cron End ----------
---------- dpkg status changes Begin ----------

2. 
user@ubuntu:~/lab5$ sudo grep 'sshd' /var/log/auth.log | awk '{print $1,$2,$3,$(NF-3)}' | sort
| uniq -c | sort -nr | head
1 2025-10-10T16:57:07.269705+00:00 ubuntu sudo: ;
1 2025-09-26T17:56:31.591807+00:00 ubuntu sshd[4190]: 192.168.56.1
1 2025-09-26T17:56:31.231759+00:00 ubuntu sshd[4188]: 192.168.56.1
1 2025-09-26T17:56:31.180611+00:00 ubuntu sshd[4190]: 192.168.56.1
1 2025-09-26T17:56:29.935340+00:00 ubuntu sshd[4186]: 192.168.56.1
1 2025-09-26T17:56:29.570337+00:00 ubuntu sshd[4188]: 192.168.56.1
1 2025-09-26T17:56:29.491039+00:00 ubuntu sshd[4192]: 192.168.56.1
1 2025-09-26T17:56:29.466472+00:00 ubuntu sshd[4183]: retries;
1 2025-09-26T17:56:29.466267+00:00 ubuntu sshd[4183]: euid=0
1 2025-09-26T17:56:29.465541+00:00 ubuntu sshd[4183]: many
user@ubuntu:~/lab5$

3.


user@ubuntu:~/lab5$ sudo journalctl --since "1 hour ago" --output=short-unix | awk '{print $1}
' | uniq -c
d 1 1760111954.944870
1 1760111954.947339
1 1760111955.037835
1 1760112009.270720
1 1760112009.297603
1 1760112009.298145
1 1760112089.775996
1 1760112089.779743
1 1760112097.506634
1 1760112097.596247
1 1760112097.596248
1 1760112097.597731
1 1760112097.596514
1 1760112127.893262
1 1760112127.893289
1 1760112129.245080
1 1760112129.453661
1 1760112129.453735
1 1760112130.772368
1 1760112130.846961
1 1760112130.852646
1 1760112130.853581
1 1760112130.871751
28 1760112130.874868
1 1760112130.876141
1 1760112151.395321
1 1760112151.402513

Incident Title:

Unauthorized SSH Login Attempts (Brute-force Attack)

Date/Time of Detection:

2025-10-10: 10:07

Detection Method:

Manual log review and command-line analysis:
`grep "Accepted password" /var/log/auth.log | awk '{print $(NF-3)}' | sort | uniq -c | sort -nr`
`grep "Failed password" /var/log/auth.log | awk '{print $(NF-3)}' | sort | uniq -c | sort -nr`

Incident Description

Analysis of the auth.log file revealed hundreds of failed SSH login attempts targeting the system's SSH daemon (sshd).
The attempts originated from multiple external IP addresses, indicating a brute-force or credential-stuffing attack aimed at guessing valid user credentials.

A small number of successful logins (with accepted passwords) were also observed, suggesting that at least one set of credentials may have been compromised.

Migration Steps

1. Immediate Containment: using firewall tools like ufw to block specific IPs , and terminate active sessions with pkill
2. Credential Security: Enforce stronger authentication policies to prevent brute force attacks, such as stronger password requirements
3. SSH Security: Only allow SSH from trusted IP addresses or via VPN, additionally disable password authentication completely and enforce using SSH keys only
4. Post-Incident Analysis: Review /var/log/* for any further suspicious activity, set up cron job indicating persistence.