Linux Server Hardening & Secure Configuration

Tools

- **Primary:** Ubuntu Server / Kali Linux
- **Alternatives:** Lynis, CIS Benchmarks

1 Review Default System Settings

```
cat /etc/passwd
systemctl list-units --type=service
ss -tuln
dpkg -l
```

```
┌──(kali㉿kali)-[~]
└─$ cat /etc/passwd

root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbi
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/no
systemd-network:x:998:998:systemd Network Management:
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhc
systemd-timesync:x:992:992:systemd Time Synchronizati
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
tss:x:102:104:TPM software stack,,,:/var/lib/tpm:/bi
strongswan:x:103:65534::/var/lib/strongswan:/usr/sbi
tcpdump:x:104:105::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/
avahi:x:106:108:Avahi mDNS daemon,,,:/run/avahi-daemo
nm-openvpn:x:107:109:NetworkManager OpenVPN,,,:/var/
speech-dispatcher:x:108:29:Speech Dispatcher,,,:/run/
```

```
┌──(kali㉿kali)-[~]
└─$ systemctl list-units --type=service

  UNIT                                  LOAD   ACTIVE SUB     DESCRIPTION
  accounts-daemon.service               loaded active running Accounts Service
  colord.service                        loaded active running Manage, Install and Generate Color Profiles
  console-setup.service                 loaded active exited  Set console font and keymap
  cron.service                          loaded active running Regular background program processing daemon
  dbus.service                          loaded active running D-Bus System Message Bus
  getty@tty1.service                    loaded active running Getty on tty1
  haveged.service                       loaded active running Entropy Daemon based on the HAVEGE algorithm
  ifupdown-pre.service                  loaded active exited  Helper to synchronize boot up for ifupdown
  keyboard-setup.service                loaded active exited  Set the console keyboard layout
  kmod-static-nodes.service             loaded active exited  Create List of Static Device Nodes
  lightdm.service                       loaded active running Light Display Manager
  ModemManager.service                  loaded active running Modem Manager
  networking.service                    loaded active exited  Raise network interfaces
```

```
┌──(kali㉿kali)-[~]
└─$ ss -tuln
# or
netstat -tuln

Netid            State             Recv-Q            Send-Q                        Local Address:Port                        Peer Address:Port
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

```
┌──(kali㉿kali)-[~]
└─$ dpkg -l

Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name                                  Version                                  Architecture Description
+++-=====================================-========================================-============-=============================================
ii  7zip                                  25.01+dfsg-3                             amd64        7-Zip file archive
ii  accountsservice                       23.13.9-8                                amd64        query and manipula
ii  acl                                   2.3.2-2+b1                               amd64        access control lis
ii  adduser                               3.153                                    all          add and remove use
ii  adwaita-icon-theme                    49.0-1                                   all          default icon theme
ii  aircrack-ng                           1:1.7+git20230807.4bf83f1a-2+b1          amd64        wireless WEP/WPA c
```

2 Manage Users and Privileges

```
awk -F: '$7 ~ /bash|sh/ {print $1}' /etc/passwd
sudo deluser username
sudo cat /etc/sudoers
sudo usermod -aG sudo username
```

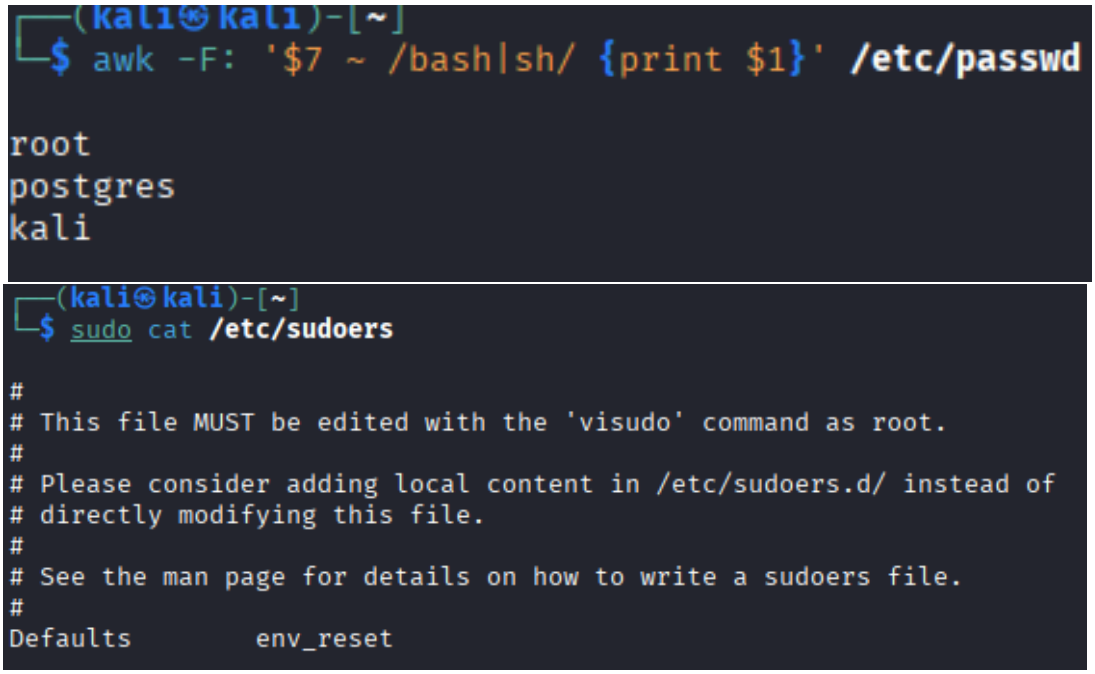

Figure 2: Screenshot of user management and sudo configuration

3 Secure SSH Configuration

```
sudo nano /etc/ssh/sshd_config
PermitRootLogin no
PasswordAuthentication no
PubkeyAuthentication yes
sudo systemctl restart ssh
ssh-keygen
ssh-copy-id user@server-ip
```

```
  GNU nano 8.6

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
```

```
┌──(kali㉿kali)-[~]
└─$ ssh-keygen
ssh-copy-id user@server-ip

Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/kali/.ssh/id_ed25519): kali
Enter passphrase for "kali" (empty for no passphrase):
Enter same passphrase again:
Passphrases do not match.  Try again.
Enter passphrase for "kali" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in kali
Your public key has been saved in kali.pub
The key fingerprint is:
SHA256:ZoGlWWrpswEP/Z4MRRhXJI417ozqsm5DtWRruSFyFEM kali@kali
The key's randomart image is:
+--[ED25519 256]--+
| .E   .oOoo      |
|  o  ../ o       |
|   oo X =        |
|  . +* * .       |
| . + +B S        |
|. + *. X .       |
| + o.o. +        |
|  +..            |
| oo+.            |
+----[SHA256]-----+
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed:
```


Figure 3: Screenshot of SSH hardening configuration

4 Update and Patch System

```
sudo apt update
sudo apt upgrade
sudo apt install unattended-upgrades
sudo dpkg-reconfigure unattended-upgrades
```

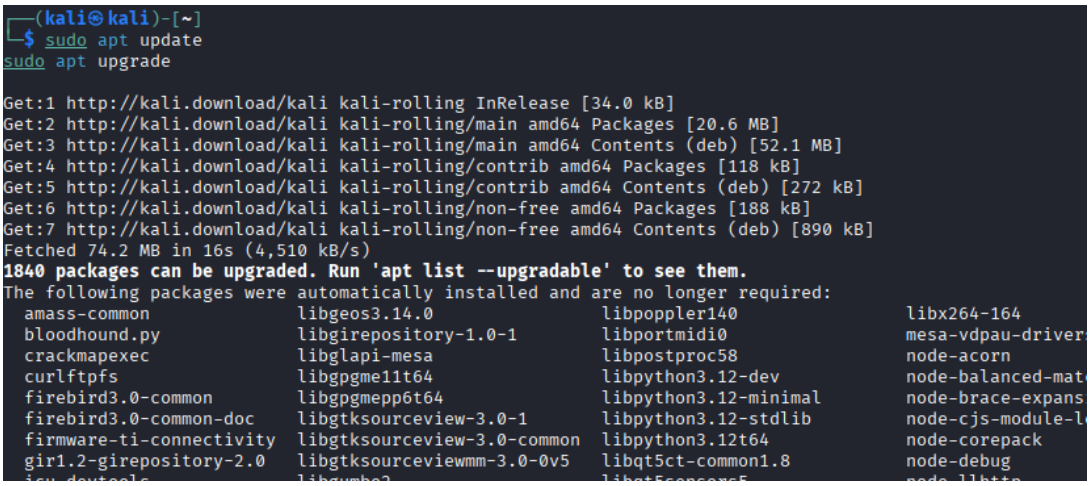

Figure 4: Screenshot showing system update process

5 Configure Firewall

```
sudo ufw enable
sudo ufw allow ssh
sudo ufw allow 80/tcp
sudo ufw status
```

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw enable

Firewall is active and enabled on system startup
```

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow ssh

Rule added
Rule added (v6)
```

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow 80/tcp

Rule added
Rule added (v6)
```

```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status

Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
80                         ALLOW       Anywhere
21                         DENY        Anywhere
1000:2000/tcp              ALLOW       Anywhere
23                         DENY        Anywhere
Anywhere                   DENY        192.168.1.100
Anywhere                   DENY        192.168.1.0/24
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
80 (v6)                    ALLOW       Anywhere (v6)
21 (v6)                    DENY        Anywhere (v6)
1000:2000/tcp (v6)         ALLOW       Anywhere (v6)
23 (v6)                    DENY        Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
```


Figure 5: Screenshot of UFW firewall configuration

6 Disable Unnecessary Services

```
systemctl list-unit-files --type=service
sudo systemctl stop servicename
sudo systemctl disable servicename
```

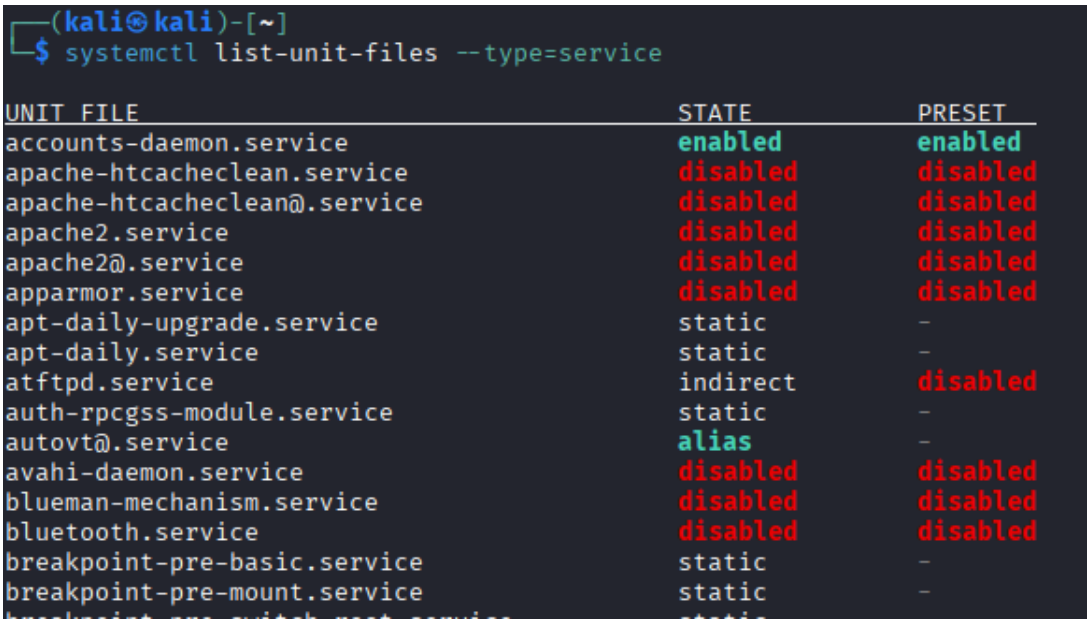

Figure 6: Screenshot showing service management

7 Secure File Permissions

```
ls -l /etc/shadow
ls -l /etc/passwd
sudo chmod 600 /etc/shadow
sudo chmod 644 /etc/passwd
find / -perm -o+w
```

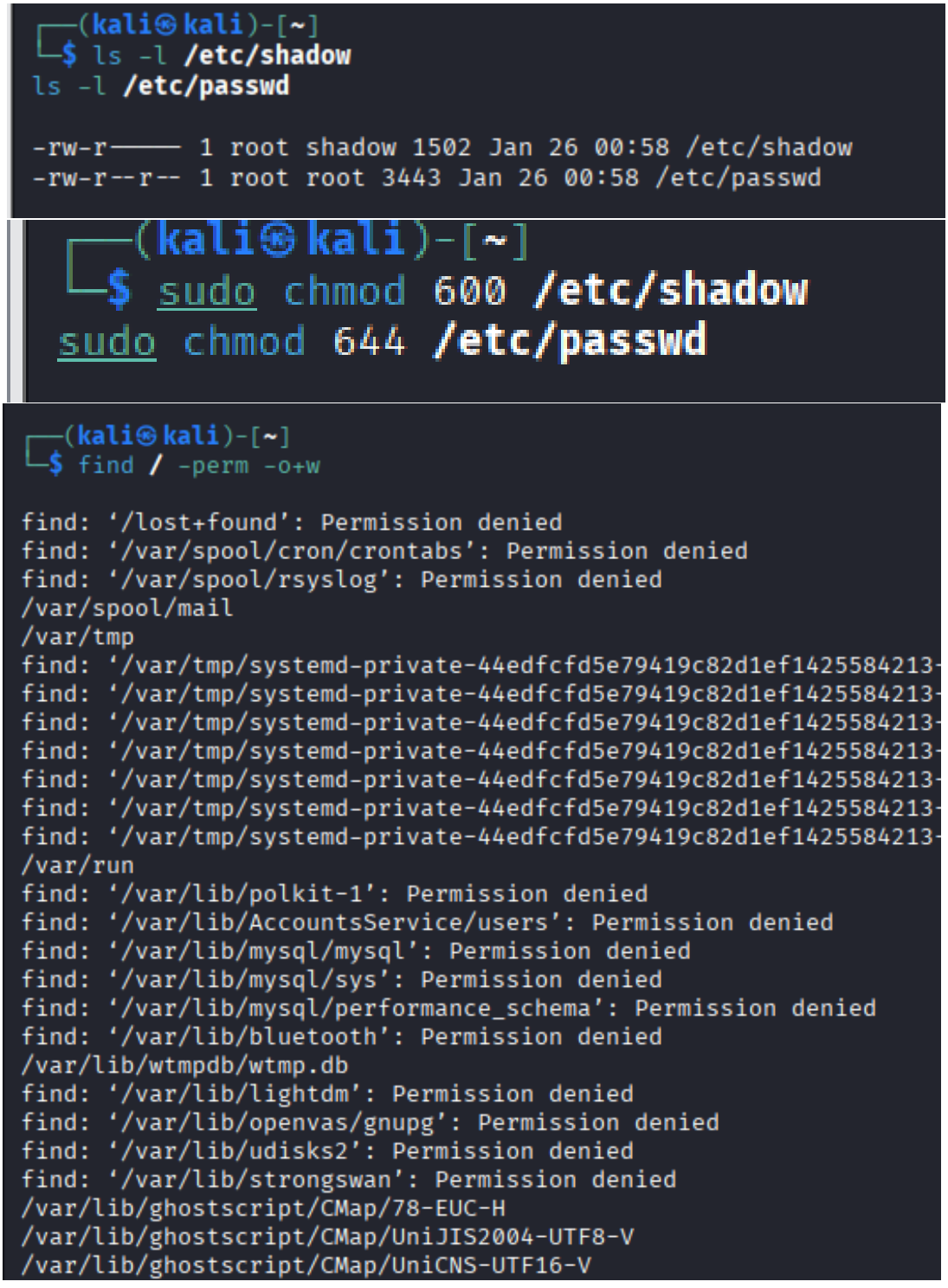

Figure 7: Screenshot of file permission verification

8 Review System Logs

```
sudo cat /var/log/auth.log
sudo journalctl
sudo grep "Failed password" /var/log/auth.log
```

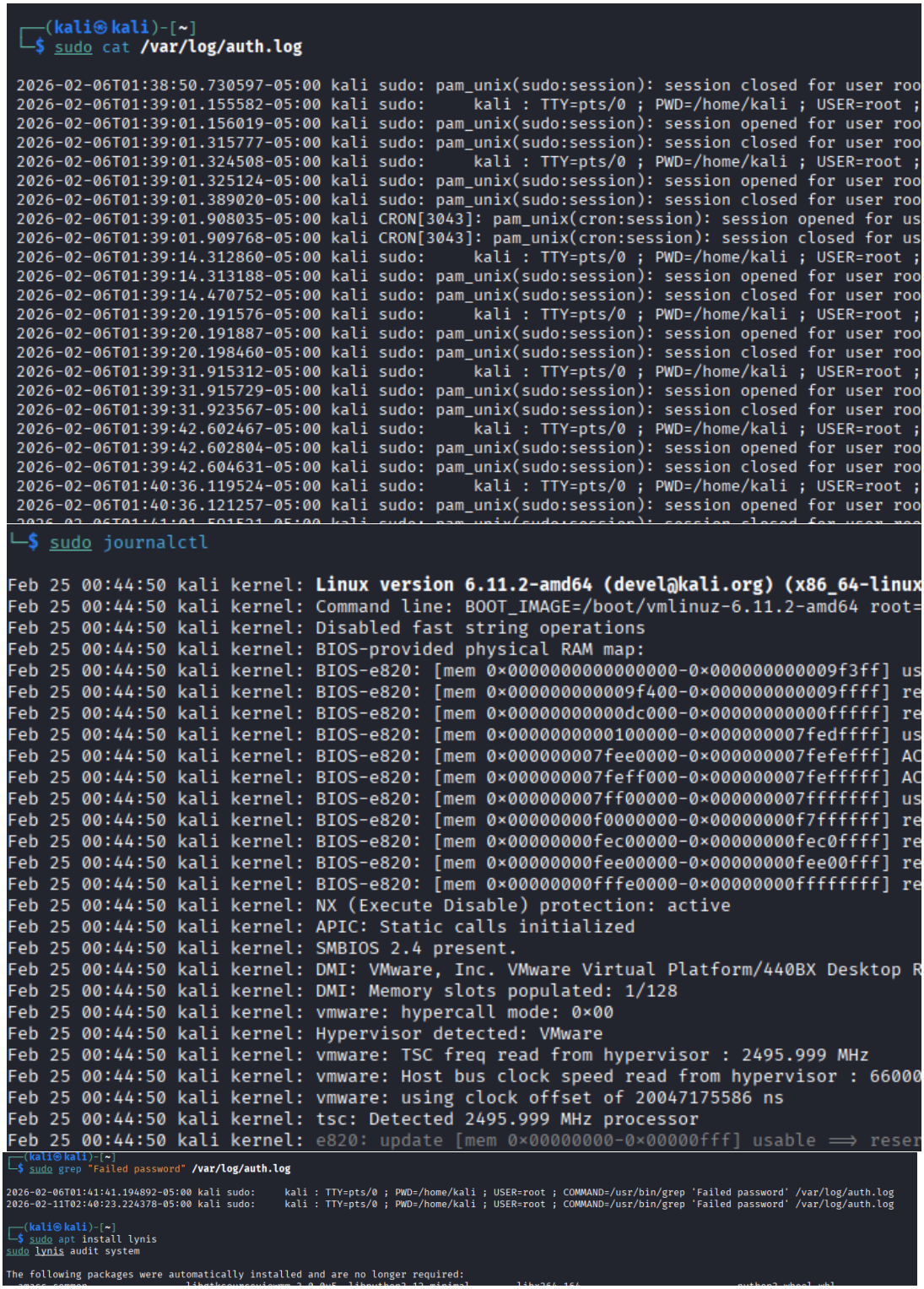

Figure 8: Screenshot of log monitoring

9 Optional Security Audit with Lynis

```
sudo apt install lynis
sudo lynis audit system
```

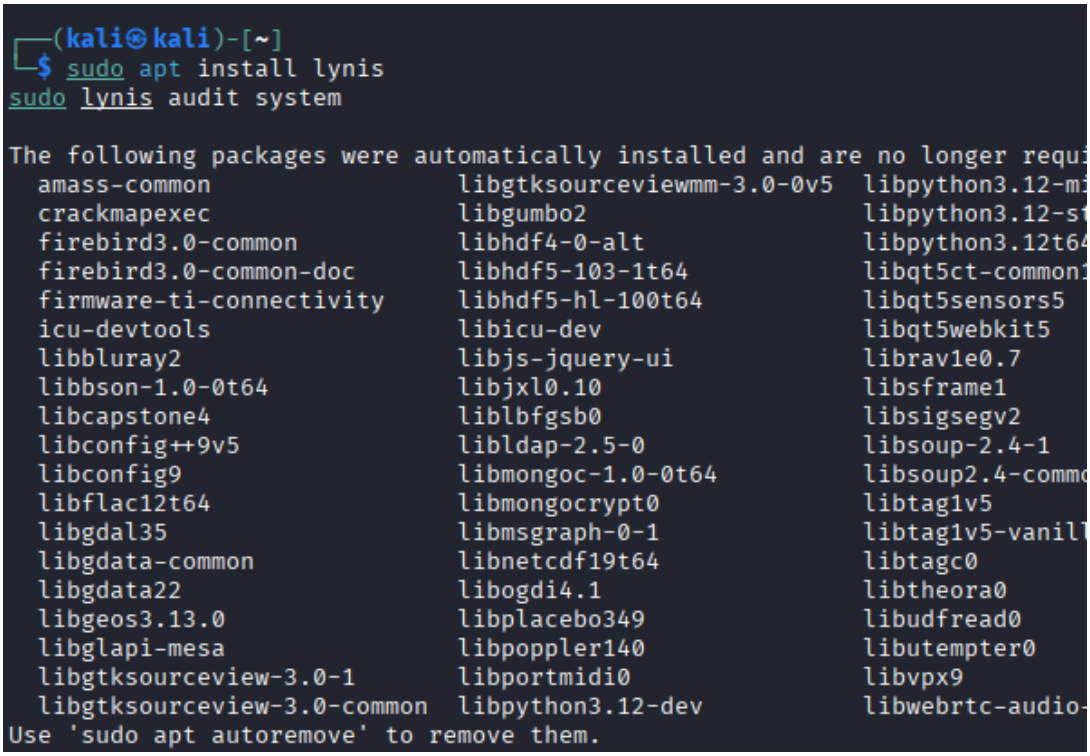

Figure 9: Screenshot of Lynis security audit results

10 Conclusion

Linux server hardening strengthens system security by reducing attack surface, controlling privileges, securing remote access, keeping systems updated, restricting network traffic, protecting sensitive files, and monitoring logs. Applying these practices significantly improves server resilience.