

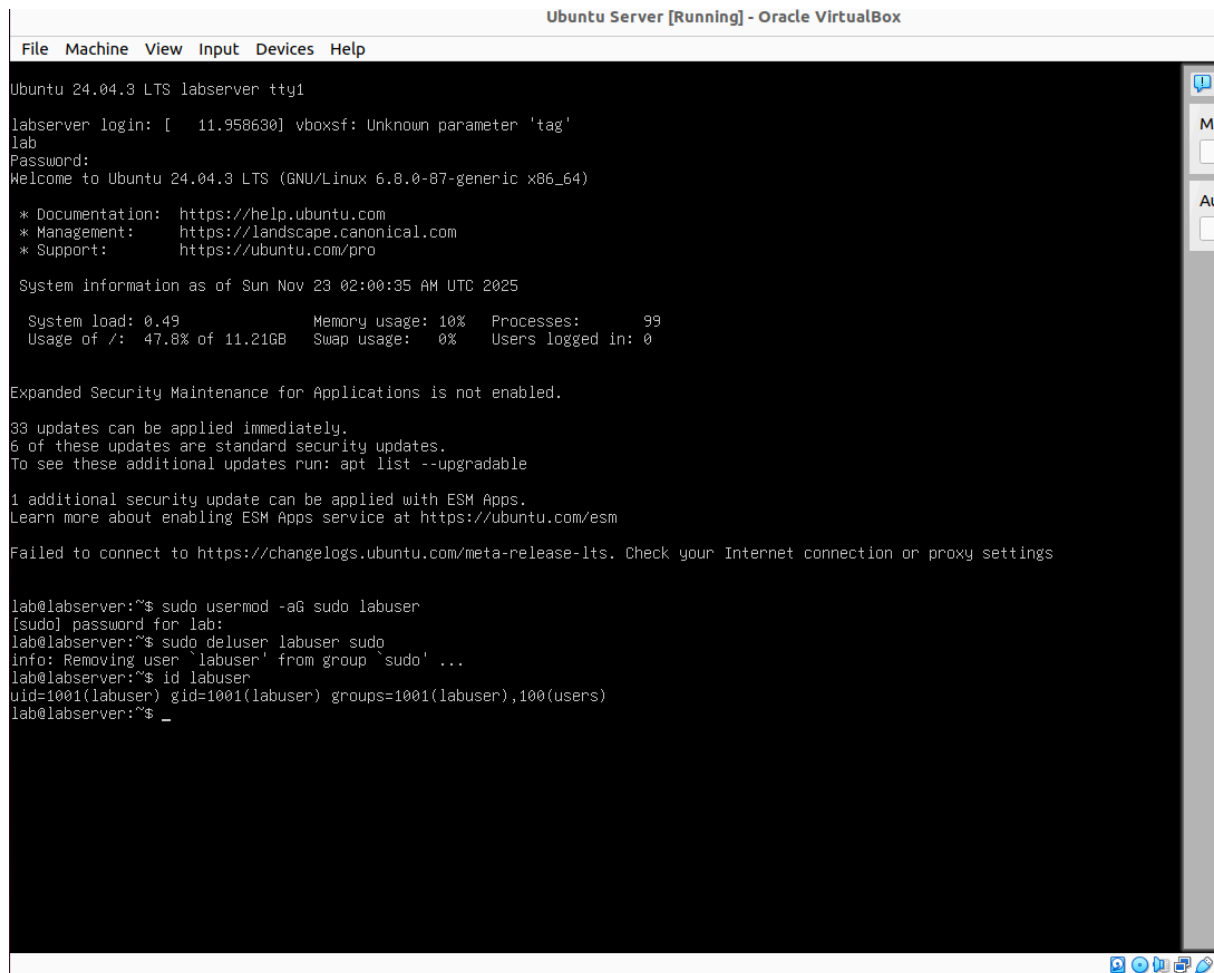
Linux Privilege Escalation

I made a user named labuser for the lab.

```
sudo adduser labuser
```

```
sudo usermod -aG sudo labuser
```

```
sudo deluser labuser sudo
```



```
Ubuntu Server [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Ubuntu 24.04.3 LTS labserver tty1
labserver login: [ 11.958630] vboxsf: Unknown parameter 'tag'
lab
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Sun Nov 23 02:00:35 AM UTC 2025

  System load: 0.49           Memory usage: 10%   Processes:    99
  Usage of /:  47.8% of 11.21GB Swap usage:   0%   Users logged in: 0

Expanded Security Maintenance for Applications is not enabled.

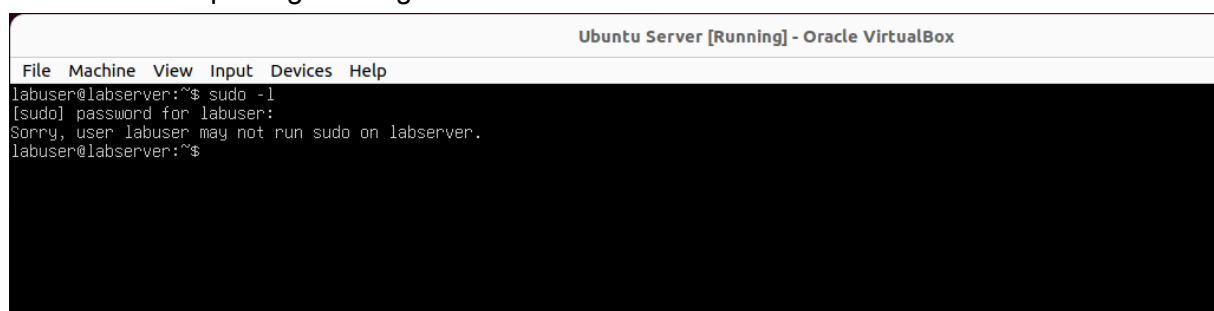
33 updates can be applied immediately.
6 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

1 additional security update can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

lab@labserver:~$ sudo usermod -aG sudo labuser
[sudo] password for lab:
lab@labserver:~$ sudo deluser labuser sudo
info: Removing user `labuser' from group `sudo' ...
lab@labserver:~$ id labuser
uid=1001(labuser) gid=1001(labuser) groups=1001(labuser),100(users)
lab@labserver:~$ _
```

I checked sudo privileges using sudo -l



```
Ubuntu Server [Running] - Oracle VirtualBox
File Machine View Input Devices Help

labuser@labserver:~$ sudo -l
[sudo] password for labuser:
Sorry, user labuser may not run sudo on labserver.
labuser@labserver:~$
```

User labuser cannot run any sudo commands.

Then, I checked the OS, kernel, and environment.

```
Ubuntu Server [Running] - Oracle VirtualBox
File Machine View Input Devices Help
labuser@labserver:~$ sudo -l
[sudo] password for labuser:
Sorry, user labuser may not run sudo on labserver.
labuser@labserver:~$ whoami
labuser
labuser@labserver:~$ hostname
labserver
labuser@labserver:~$ uname -a
Linux labserver 6.8.0-87-generic #88-Ubuntu SMP PREEMPT_DYNAMIC Sat Oct 11 09:28:41 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
labuser@labserver:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 24.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.3 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
labuser@labserver:~$
```

This showed the OS version and kernel build. This is recent and unlikely vulnerable to known kernel exploits.

I checked the PATH.

```
labuser@labserver:~$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
labuser@labserver:~$
```

A misconfigured PATH which is writable directories before system paths can allow PATH hijacking. The path was correctly ordered and had no writable directories.

SUID binaries

```
labuser@labserver:~$ find / -perm -4000 -type f 2>/dev/null
/opt/VBoxGuestAdditions-7.2.0/bin/VBoxDRMClient
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/fusermount3
/usr/bin/umount
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
labuser@labserver:~$
```

SUID binaries run as the file owner(root). No unusual or dangerous SUID binaries were found.

Cron jobs

```
Ubuntu Server [Running] - Oracle VirtualBox

File Machine View Input Devices Help

labuser@labserver:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
# You can also override PATH, but by default, newer versions inherit it from the environment
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# * * * * * user-name command to be executed
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.daily; }
47 6 * * 7 root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.weekly; }
52 6 1 * * root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.monthly; }
#

labuser@labserver:~$ ls -la /etc/cron.d
total 20
drwxr-xr-x  2 root root 4096 Aug  5 17:14 .
drwxr-xr-x 110 root root 4096 Nov 23 02:00 ..
-rw-r--r--  1 root root  201 Apr  8 2024 e2scrub_all
-rw-r--r--  1 root root  102 Aug  5 17:14 .placeholder
-rw-r--r--  1 root root  396 Aug  5 17:14 sysstat
labuser@labserver:~$ _
```

Cron tasks run automatically; if root runs a writable script, that becomes a privilege escalation vector. All cron entries are default and non-writable, so no cron-based escalation path exists.

Next, I used linpeas which is a script which will search for all possible paths to escalate privileges on Linux hosts on Kali.

I downloaded linpeas on Kali, hosted with `python3 -m http.server 8000`, so ubuntu server could download linpeas.

```
labuser@labserver:/tmp$ wget http://192.168.56.101:8000/linpeas.sh -O linpeas.sh
labuser@labserver:/tmp$ chmod +x linpeas.sh
labuser@labserver:/tmp$ ls -l
total 980
-rwxrwxr-x 1 labuser labuser 971926 Nov 15 15:04 linpeas.sh
drwx----- 2 root root 4096 Nov 15 08:26 snap-private-tmp
drwx----- 3 root root 4096 Nov 15 08:26 systemd-private-c734f7c33cbb4b6e8c965cf838f34717-ModemManager.service-JczYGs
drwx----- 3 root root 4096 Nov 15 08:26 systemd-private-c734f7c33cbb4b6e8c965cf838f34717-polkit.service-0T2Eag
drwx----- 3 root root 4096 Nov 15 08:26 systemd-private-c734f7c33cbb4b6e8c965cf838f34717-systemd-logind.service-77Hsv7
drwx----- 3 root root 4096 Nov 15 08:26 systemd-private-c734f7c33cbb4b6e8c965cf838f34717-systemd-resolved.service-vdVan9
drwx----- 3 root root 4096 Nov 23 02:24 systemd-private-c734f7c33cbb4b6e8c965cf838f34717-upower.service-kaT01V
drwx----- 2 labuser labuser 4096 Nov 23 02:59 tmux-1001
labuser@labserver:/tmp$ _
```

[illegible]

```

File Machine View Input Devices Help
lab@labserver:~$ sudo cp /bin/bash /usr/local/bin/rootbash
[sudo] password for lab:
lab@labserver:~$ sudo chmod 4755 /usr/local/bin/rootbash
lab@labserver:~$ ls -ls /usr/local/bin/rootbash
1416 -rwsr-xr-x 1 root root 1446024 Nov 24 02:59 /usr/local/bin/rootbash
lab@labserver:~$

```

```
-rwsr-xr-x 1 root root 1.4M Nov 24 02:59 ESC[1;31m/usr/local/bin/rootbash (Unknown SUID binary!)ESC[0m
```

After adding the SUID misconfiguration on the Ubuntu server, the second linpeas scan correctly flagged `/usr/local/bin/rootbash` as an 'Unknown SUID binary.' Linpeas highlights this type of file because it is not part of the standard OS installation and it runs with elevated privileges due to the SUID bit. Any non-privileged user can execute the file and immediately obtain a root shell. This confirms that the SUID configuration represents an intentional privilege-escalation vulnerability.