

# **CSE3501-Information Security Analysis and Audit**

**Lab 9+10**

## **Digital Assignment-2**

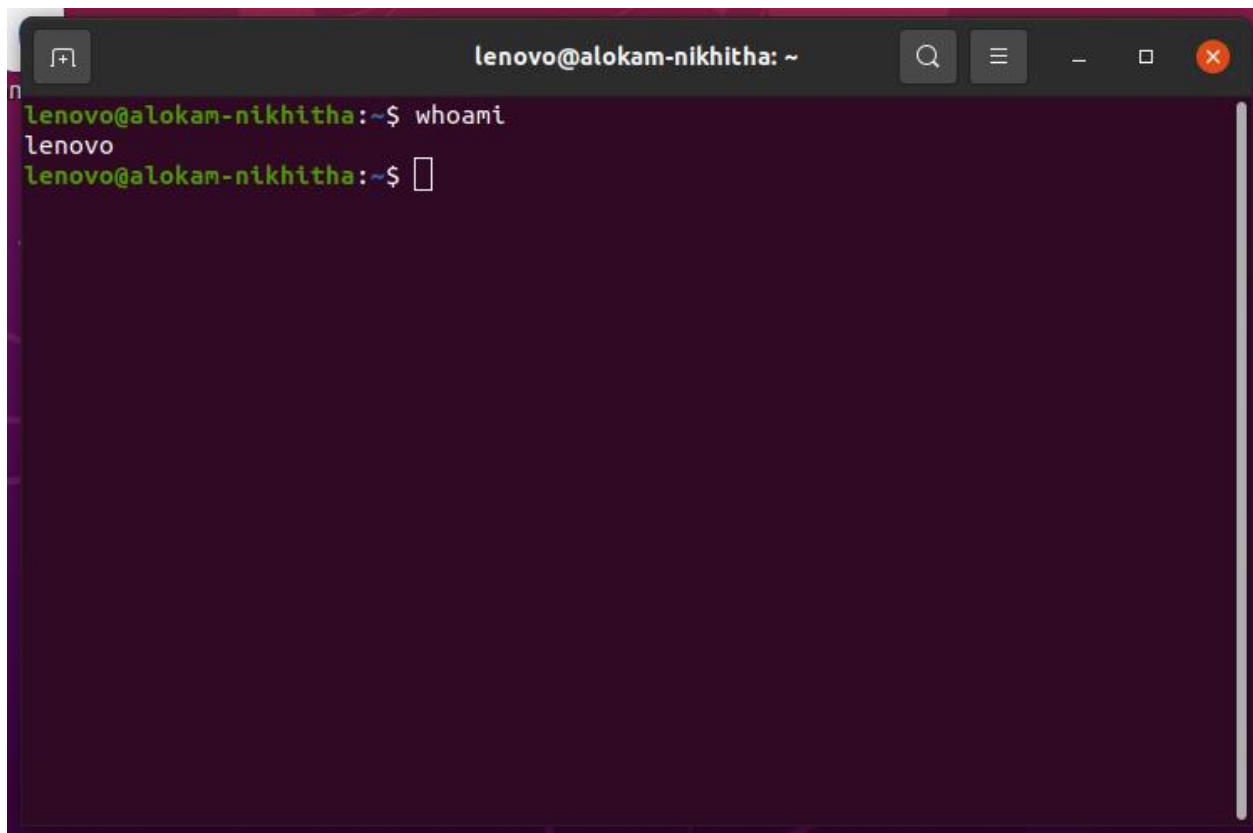
**Submitted by: Alokam Nikhitha**

**Reg No:19BCE2555**

# Privilege Escalation in Linux OS using sudo command on terminal.

## whoami:

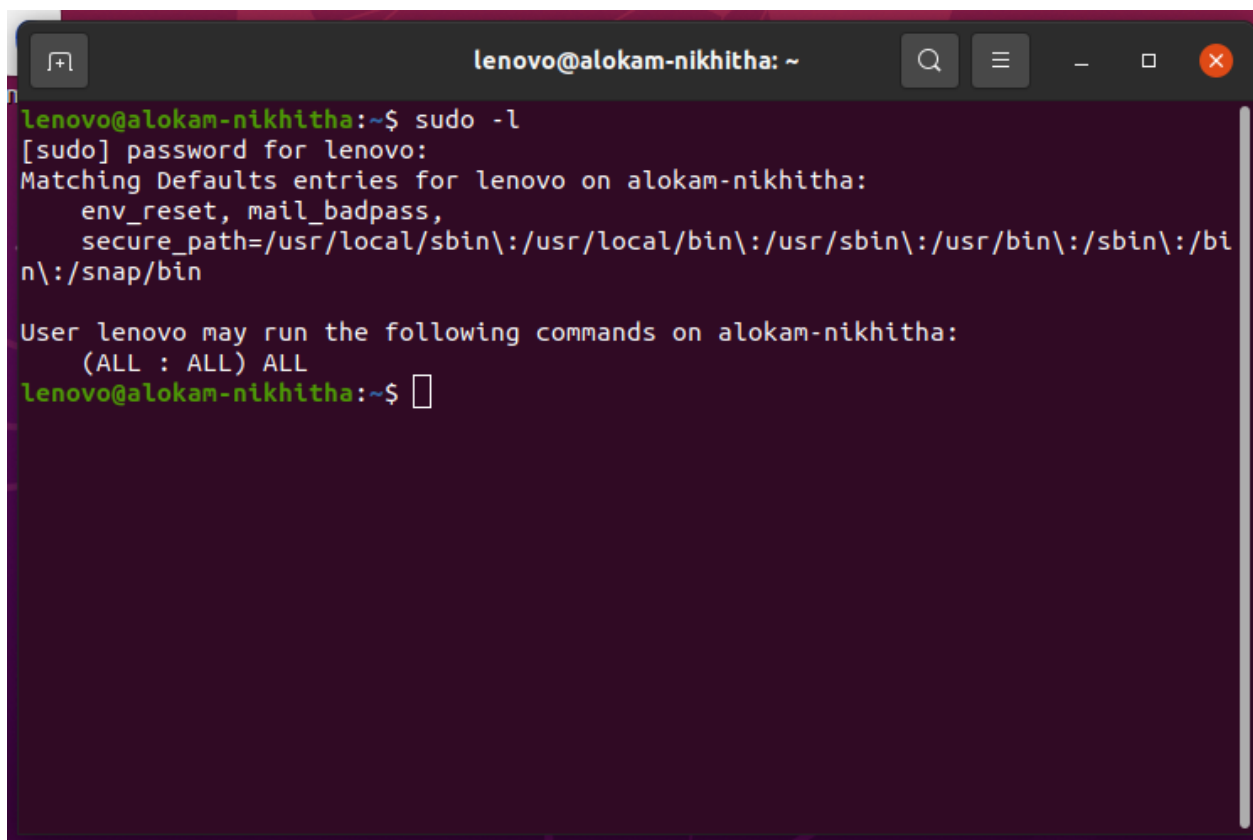
returns the user Details

A terminal window with a dark purple background. The title bar at the top reads 'lenovo@alokam-nikhitha: ~'. The terminal shows the command 'whoami' being entered at the prompt 'lenovo@alokam-nikhitha:~\$'. The output 'lenovo' is displayed on the next line. The prompt 'lenovo@alokam-nikhitha:~\$' is shown again with a cursor, indicating the command has finished execution.

```
lenovo@alokam-nikhitha:~$ whoami
lenovo
lenovo@alokam-nikhitha:~$
```

## sudo -l:

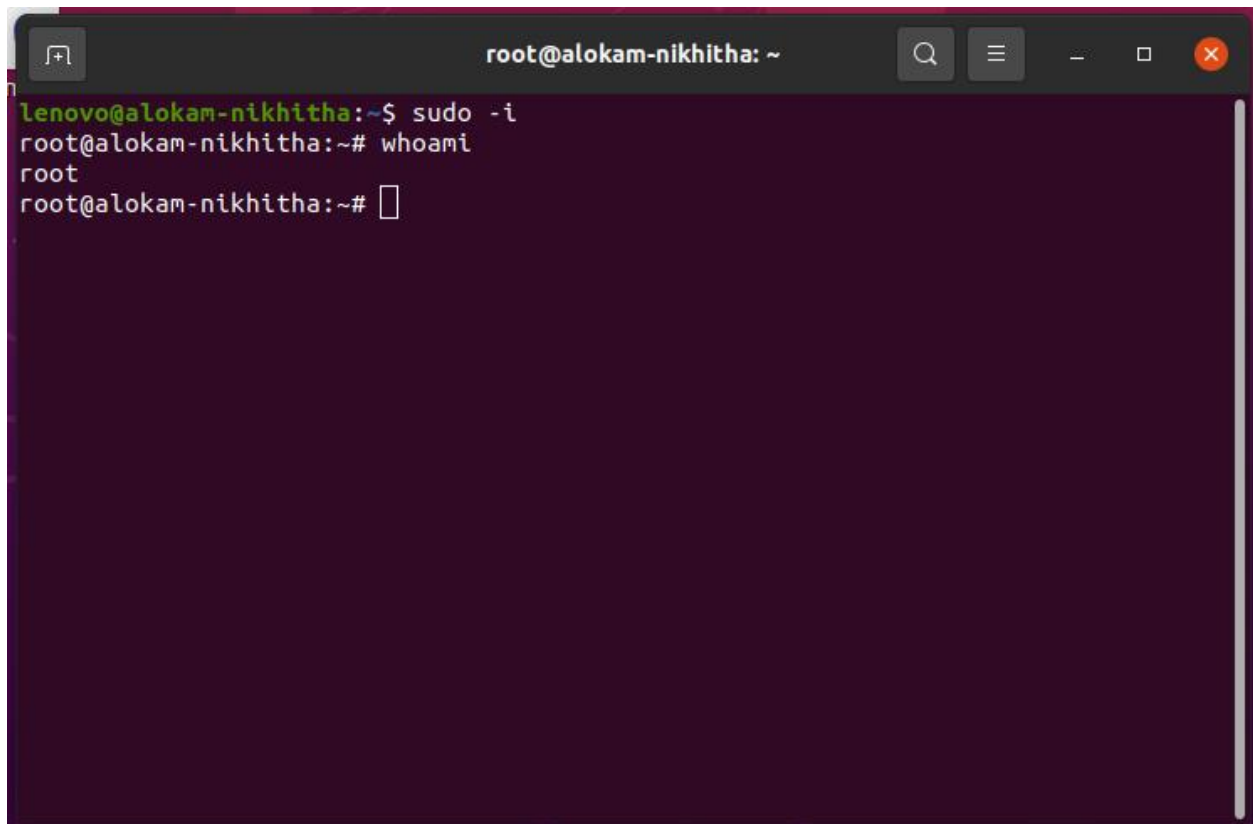
returns list of commands the user can use or the user even has a permission to use the sudo command.

A terminal window titled 'lenovo@alokam-nikhitha: ~' with standard window controls. The terminal shows the command 'sudo -l' being executed. It prompts for a password, then displays matching defaults for the user 'lenovo', including environment variables and secure paths. Finally, it lists the commands the user is allowed to run, which is '(ALL : ALL) ALL'.

```
lenovo@alokam-nikhitha:~$ sudo -l
[sudo] password for lenovo:
Matching Defaults entries for lenovo on alokam-nikhitha:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User lenovo may run the following commands on alokam-nikhitha:
    (ALL : ALL) ALL
lenovo@alokam-nikhitha:~$
```

**sudo -i** command to get to the root user which has higher privileges than the user dgn, to confirm that the user is changed check it using **whoami** command. Thus, Privilege Escalation is achieved.



```
root@alokam-nikhitha: ~
lenovo@alokam-nikhitha:~$ sudo -i
root@alokam-nikhitha:~# whoami
root
root@alokam-nikhitha:~#
```