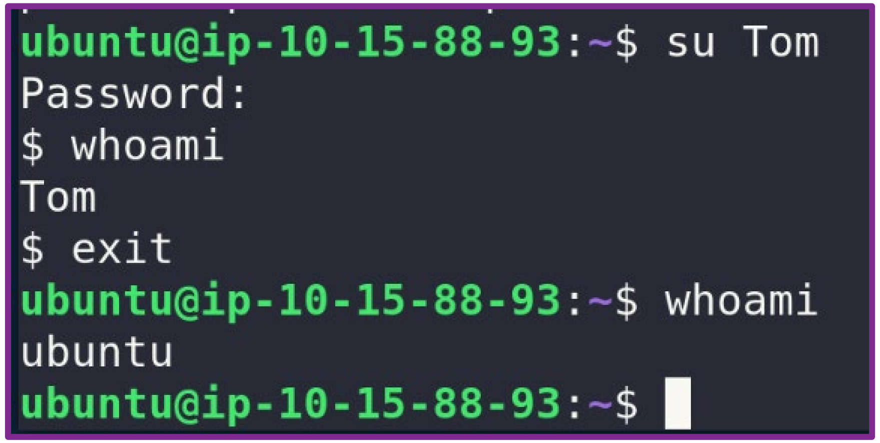
Intro to Linux

2.4.2 - Executing Commands as Another User

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Accessing Files and Executing Commands as Other Users

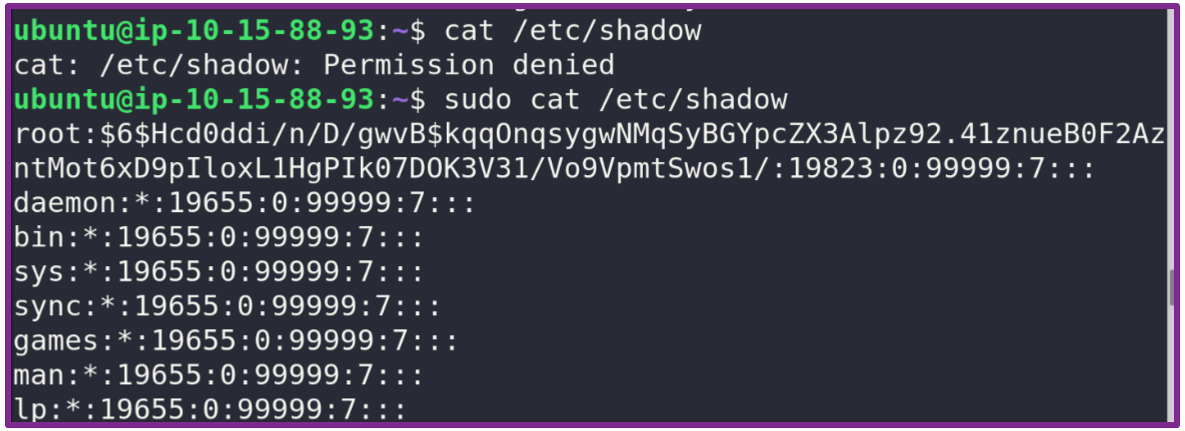
- In some cases, files may need to be accessed by other users within a system or commands may need to be executed through the root user when performing administrative tasks
- The **`su –`** command, where the – is the username, allows a user to login as another in order to access certain files or permissions
- Commands can be executed by running **`su <username> -c <command>`**
- Typing **`exit`** will return the user to the original account



```
ubuntu@ip-10-15-88-93:~$ su Tom
Password:
$ whoami
Tom
$ exit
ubuntu@ip-10-15-88-93:~$ whoami
ubuntu
ubuntu@ip-10-15-88-93:~$ 
```

Running Commands with Sudo

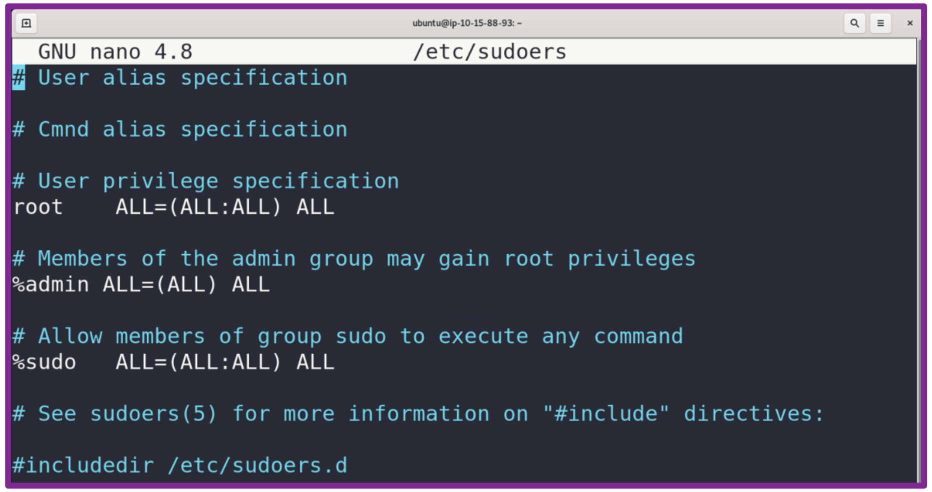
- Allowing multiple users to have admin credentials poses a security threat to the system
- The **`sudo`** command allows a user to run a command with admin privileges without having to login as the root user
- The command would be preceded with **`sudo`** as seen here



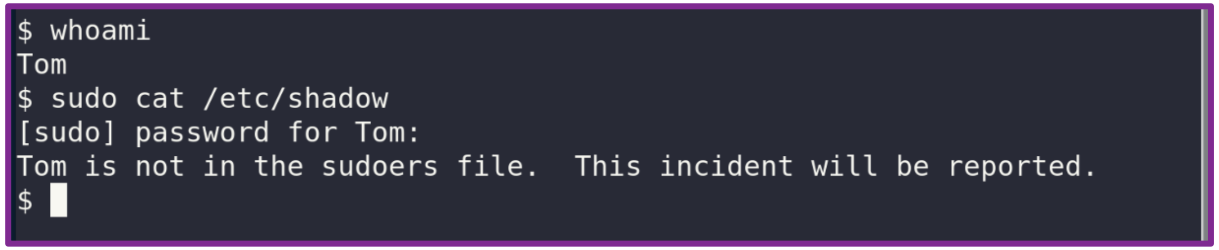
```
ubuntu@ip-10-15-88-93:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
ubuntu@ip-10-15-88-93:~$ sudo cat /etc/shadow
root:$6$Hcd0ddi/n/D/gwvB$kqqOnqsygwNMqSyBGYpcZX3Alpz92.41znueB0F2Az
ntMot6xD9pIloxL1HgPIk07DOK3V31/Vo9VpmtSwos1/:19823:0:99999:7:::
daemon:*:19655:0:99999:7:::
bin:*:19655:0:99999:7:::
sys:*:19655:0:99999:7:::
sync:*:19655:0:99999:7:::
games:*:19655:0:99999:7:::
man:*:19655:0:99999:7:::
lp:*:19655:0:99999:7:::
```

Sudoers File

- Not just any user can use the sudo command
- As a security feature of Linux systems, the user must be listed in the sudoers file, located at /etc/sudoers
- If not listed, the user will not be allowed to use sudo and the incident is logged



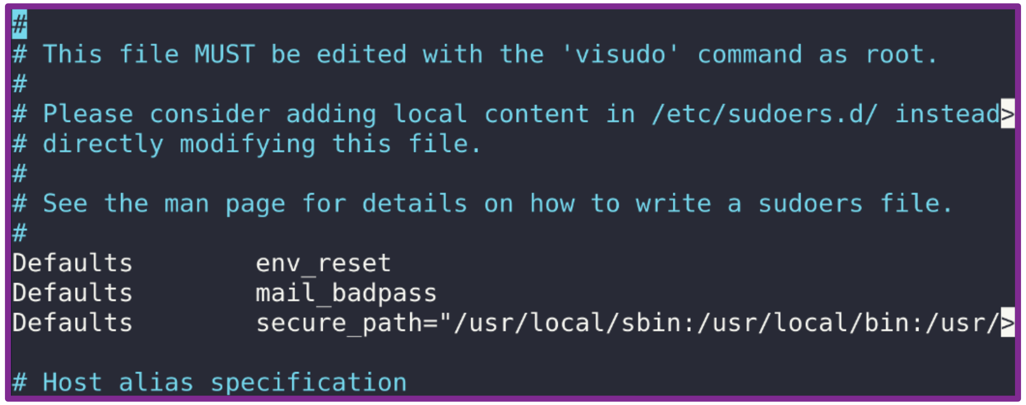
```
  GNU nano 4.8                         /etc/sudoers
# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```



```
$ whoami
Tom
$ sudo cat /etc/shadow
[sudo] password for Tom:
Tom is not in the sudoers file.  This incident will be reported.
$ 
```

Editing the Sudoers File

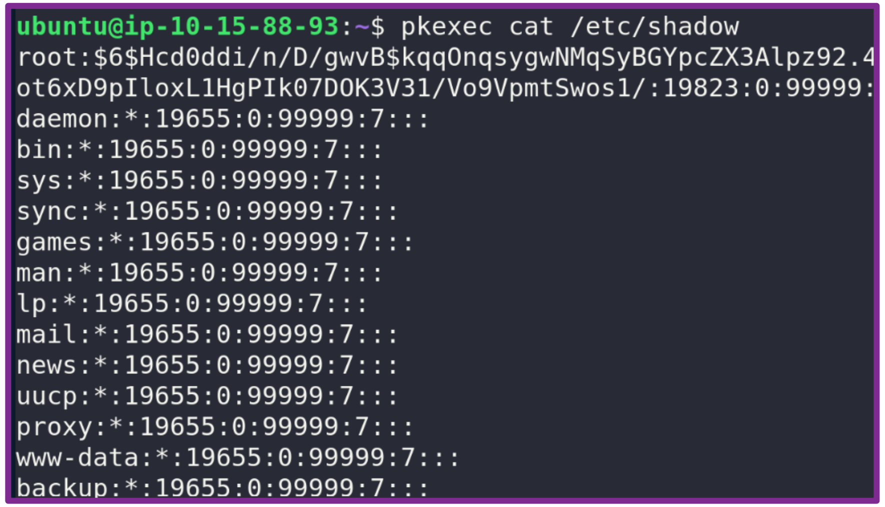
- Editing the sudoers file requires root access and some additional security precautions
- Issues can arise if the sudoers file is open or edited by multiple people
- Typically, the sudoers file is open using the visudo editor which does a check to see if the file is open by another user
- If it is open already then, the file is opened as read-only



```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead>
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/>

# Host alias specification
```

PolicyKit

- Also referred to as PolKit
- Allows fine tuning of administrative privileges such as mounting drives, changing systems, installing software, and more
- When a task is performed, PolicyKit will check it against the rules in place to determine if the user has sufficient rights
- **`pkexec`** is common command allowing a user to execute commands as the root user



```
ubuntu@ip-10-15-88-93:~$ pkexec cat /etc/shadow
root:$6$Hcd0ddi/n/D/gwvB$kqqOnqsygwNMqSyBGYpcZX3Alpz92.4
ot6xD9pIloxL1HgPIk07DOK3V31/Vo9VpmtSwos1/:19823:0:99999:
daemon:*:19655:0:99999:7:::
bin:*:19655:0:99999:7:::
sys:*:19655:0:99999:7:::
sync:*:19655:0:99999:7:::
games:*:19655:0:99999:7:::
man:*:19655:0:99999:7:::
lp:*:19655:0:99999:7:::
mail:*:19655:0:99999:7:::
news:*:19655:0:99999:7:::
uucp:*:19655:0:99999:7:::
proxy:*:19655:0:99999:7:::
www-data:*:19655:0:99999:7:::
backup:*:19655:0:99999:7:::
```