CSCI:530 – Security Systems
Lab 3: Authorization – Due Date: October 4^{th,} 2024
Name: Anne Sai Venkata Naga Saketh
USC Email: annes@usc.edu
USC ID: 3725520208

Question 1:

Above you wrote predictions in the grids for both the baseline "before" case and the modified "after" case following creation of an ACL. Then you tested them. Maybe all your predictions were right, maybe not. Now, go ahead and change the predictions (in the tables above), as needed, to reflect the actual empirical outcomes you saw. "Yes" or "No" should appear in each cell. In each, under "yes" or "no," write the very brief reason for that outcome. Do this for both of the grids appearing above.

baseline case:

	bill	mary	joe
strategies	Yes	No	No
salaries	No	Yes	No
workschedule	Yes	Yes	Yes

Reason:

The file permissions that we have set are as follows,

1. chmod 644
- The owner has the read-and-write permissions
- Group has Read-only permission
- Others have Read-only permission

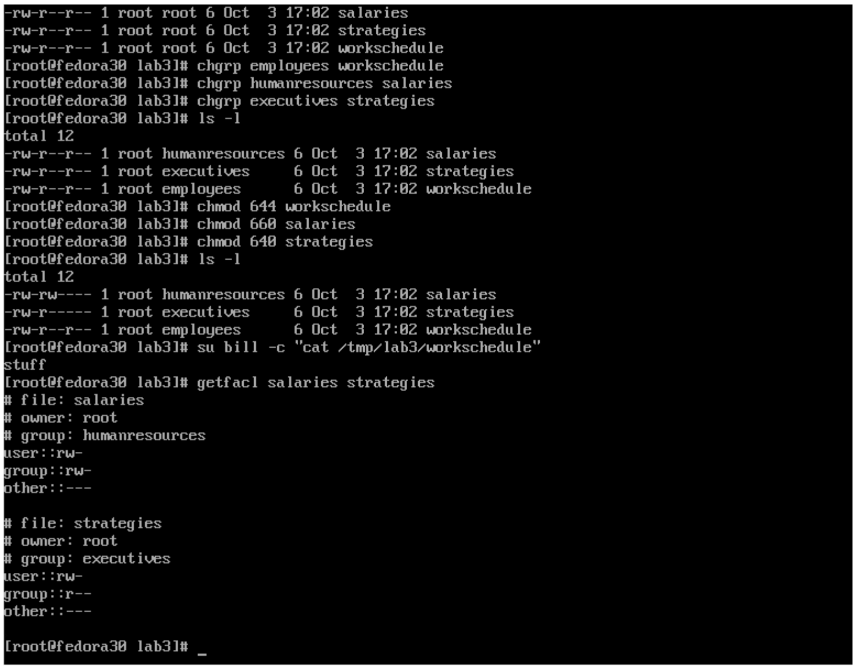
So, in this case, everyone can read the contents of the file.

2. chmod 640
- Owner has read and write permissions
- Group has read-only permission
- Others have No permissions

So, in this case, only the group and the owner of the file can read the contents of the file.

3. chmod 660
- Owner has read and write permissions
- Group has read and write permissions
- Others have No permissions

Hence, similar to the above condition (since we are not concerned about write permissions), the owner of the file and the group have the permissions to read the contents of the file.



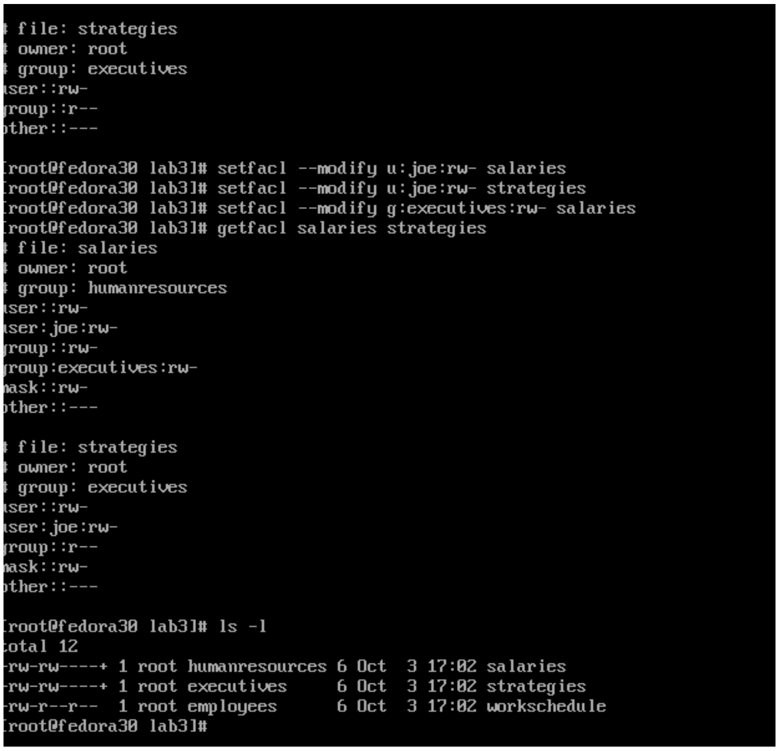
```
-rw-r--r-- 1 root root 6 Oct  3 17:02 salaries
-rw-r--r-- 1 root root 6 Oct  3 17:02 strategies
-rw-r--r-- 1 root root 6 Oct  3 17:02 workschedule
[root@fedora30 lab3]# chgrp employees workschedule
[root@fedora30 lab3]# chgrp humanresources salaries
[root@fedora30 lab3]# chgrp executives strategies
[root@fedora30 lab3]# ls -l
total 12
-rw-r--r-- 1 root humanresources 6 Oct  3 17:02 salaries
-rw-r--r-- 1 root executives     6 Oct  3 17:02 strategies
-rw-r--r-- 1 root employees      6 Oct  3 17:02 workschedule
[root@fedora30 lab3]# chmod 644 workschedule
[root@fedora30 lab3]# chmod 660 salaries
[root@fedora30 lab3]# chmod 640 strategies
[root@fedora30 lab3]# ls -l
total 12
-rw-rw---- 1 root humanresources 6 Oct  3 17:02 salaries
-rw-r----- 1 root executives     6 Oct  3 17:02 strategies
-rw-r--r-- 1 root employees      6 Oct  3 17:02 workschedule
[root@fedora30 lab3]# su bill -c "cat /tmp/lab3/workschedule"
stuff
[root@fedora30 lab3]# getfacl salaries strategies
# file: salaries
# owner: root
# group: humanresources
user::rw-
group::rw-
other::---

# file: strategies
# owner: root
# group: executives
user::rw-
group::r--
other::---

[root@fedora30 lab3]# _
```

modified case:

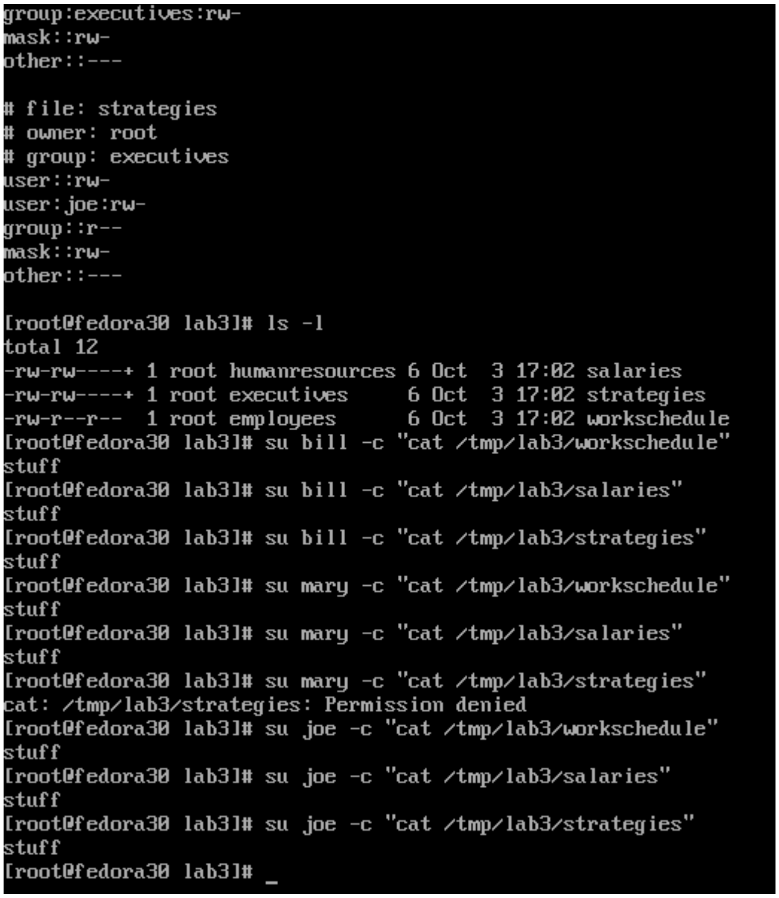
	bill	mary	joe
strategies	Yes	No	Yes
salaries	Yes	Yes	Yes
workschedule	Yes	Yes	Yes

In this case, we are modifying the permissions of Joe to access (read and write) the salaries and strategies file which he did not have access to earlier during the baseline step.

As well, we are modifying the permissions of the executives group to read and write the salaries file. The executives group contains the user Bill, so he should be able to access the salaries file, which he was not able to access earlier.



```
# file: strategies
# owner: root
# group: executives
user::rw-
group::r--
other::---

[root@fedora30 lab3]# setfacl --modify u:joe:rw- salaries
[root@fedora30 lab3]# setfacl --modify u:joe:rw- strategies
[root@fedora30 lab3]# setfacl --modify g:executives:rw- salaries
[root@fedora30 lab3]# getfacl salaries strategies
# file: salaries
# owner: root
# group: humanresources
user::rw-
user:joe:rw-
group::rw-
group:executives:rw-
mask::rw-
other::---

# file: strategies
# owner: root
# group: executives
user::rw-
user:joe:rw-
group::r--
mask::rw-
other::---

[root@fedora30 lab3]# ls -l
total 12
-rw-rw----+ 1 root humanresources 6 Oct  3 17:02 salaries
-rw-rw----+ 1 root executives     6 Oct  3 17:02 strategies
-rw-r--r--  1 root employees      6 Oct  3 17:02 workschedule
[root@fedora30 lab3]#
```



```
group:executives:rw-
mask::rw-
other::---

# file: strategies
# owner: root
# group: executives
user::rw-
user:joe:rw-
group::r--
mask::rw-
other::---

[root@fedora30 lab3]# ls -l
total 12
-rw-rw----+ 1 root humanresources 6 Oct  3 17:02 salaries
-rw-rw----+ 1 root executives     6 Oct  3 17:02 strategies
-rw-r--r--  1 root employees      6 Oct  3 17:02 workschedule
[root@fedora30 lab3]# su bill -c "cat /tmp/lab3/workschedule"
stuff
[root@fedora30 lab3]# su bill -c "cat /tmp/lab3/salaries"
stuff
[root@fedora30 lab3]# su bill -c "cat /tmp/lab3/strategies"
stuff
[root@fedora30 lab3]# su mary -c "cat /tmp/lab3/workschedule"
stuff
[root@fedora30 lab3]# su mary -c "cat /tmp/lab3/salaries"
stuff
[root@fedora30 lab3]# su mary -c "cat /tmp/lab3/strategies"
cat: /tmp/lab3/strategies: Permission denied
[root@fedora30 lab3]# su joe -c "cat /tmp/lab3/workschedule"
stuff
[root@fedora30 lab3]# su joe -c "cat /tmp/lab3/salaries"
stuff
[root@fedora30 lab3]# su joe -c "cat /tmp/lab3/strategies"
stuff
[root@fedora30 lab3]# _
```

Question 2:

When you assigned identical passwords to bill, mary, and joe, different content appeared for each user in the /etc/shadow file where passwords are stored. Why?

Reason: The main reason we see different passwords for all three users, even though we give the same password ‘password’ for all three users is that the ‘passwd’ command combines the plain text along with some salt (random character data) and then it is hashed using the hashing algorithms like MD5 or SHA-512 and then stored.