Jared Ren
Race condition lab writeup
2/28/20

Task1)
Before

```
mysql:x:125:132:MySQL Server,,,:/nonexistent:/bin/false
user1:x:1001:1001::/home/user1:
```

After

```
user1:x:1001:1001::/home/user1:
test:U6aMy0wojraho:0:0:test:/root:/bin/bash

[03/02/20]seed@VM:~/lab_4v2$
```

Task2)
Successful attack.

```
No permission
No permission
STOP... The passwd file has been changed
[03/02/20]seed@VM:~/lab4$
```

The result

```
bind:x:124:131::/var/cache/bind:/bin/false
mysql:x:125:132:MySQL Server,,,:/nonexistent:/bin/false
user1:x:1001:1001::/home/user1:

test:U6aMy0wojraho:0:0:test:/root:/bin/bash[03/02/20]seed@VM:~/lab4$
```

Task3)

The attack was unsuccessful. The edit makes it so the user can only access files accessible to the user.

Task4)

The attack was unsuccessful. The command enables symbolic link protection, patching the vulnerability in symbolic links.

7.1
Yes the program has a race condition vulnerability.

7.2
Yes, None of the four countermeasures are in place in regards to this new program.

7.6
Yes it has a TOCTTOU race condition vulnerability. There is a window in between when we open the file and when we check it, meaning we can feed the program input that redirects to an attacking program.