

l_2

Connor Taffe

April 1, 2016

1 Task 1

Task one is just to fill the proper line in `exploit.c`:

```
/* You need to fill the buffer with appropriate contents here */  
memcpy(buffer, shellcode, sizeof(shellcode));
```

The following three figures show me editing and running the programs.

2 Task 2

Address randomization has no effect on the stack addressed relative to the stack. The stack grows linearly regardless unless you are compiling with split stacks, which in such a small area like a frame, would not cause issues.

3 Task 3

Stack Guard causes the stack smashing to be detected at runtime.

```

[04/01/2016 13:17] seed@ubuntu:~$ sudo su root
[sudo] password for seed:
[04/01/2016 13:18] root@ubuntu:/home/seed# sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
[04/01/2016 13:18] root@ubuntu:/home/seed# ls
Desktop          Music              Pictures
Documents        openssl-1.0.1      Public
Downloads        openssl_1.0.1-4ubuntu5.11.debian.tar.gz  Templates
elggData         openssl_1.0.1-4ubuntu5.11.dsc             Videos
examples.desktop openssl_1.0.1.orig.tar.gz
[04/01/2016 13:18] root@ubuntu:/home/seed# mkdir l2
[04/01/2016 13:18] root@ubuntu:/home/seed# cd l2
[04/01/2016 13:18] root@ubuntu:/home/seed/l2# ls
[04/01/2016 13:18] root@ubuntu:/home/seed/l2# wget http://www.cis.syr.edu/~wedu/seed/Labs/Vulnerability/Buffer_Overflow/files/call_shellcode.c
--2016-04-01 13:18:55-- http://www.cis.syr.edu/~wedu/seed/Labs/Vulnerability/Buffer_Overflow/files/call_shellcode.c
Resolving www.cis.syr.edu (www.cis.syr.edu)... 128.230.208.76
Connecting to www.cis.syr.edu (www.cis.syr.edu)|128.230.208.76|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 951 [text/x-c]
Saving to: `call_shellcode.c'

100%[=====] 951          --.-K/s   in 0s

2016-04-01 13:18:55 (2.06 MB/s) - `call_shellcode.c' saved [951/951]

[04/01/2016 13:18] root@ubuntu:/home/seed/l2# wget http://www.cis.syr.edu/~wedu/seed/Labs/Vulnerability/Buffer_Overflow/files/stack.c
--2016-04-01 13:19:06-- http://www.cis.syr.edu/~wedu/seed/Labs/Vulnerability/Buffer_Overflow/files/stack.c
Resolving www.cis.syr.edu (www.cis.syr.edu)... 128.230.208.76
Connecting to www.cis.syr.edu (www.cis.syr.edu)|128.230.208.76|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 554 [text/x-c]
Saving to: `stack.c'

100%[=====] 554          --.-K/s   in 0s

```

Figure 1: Disabling memory layout randomization

```

fer_Overflow/files/exploit.c
Resolving www.cis.syr.edu (www.cis.syr.edu)... 128.230.208.76
Connecting to www.cis.syr.edu (www.cis.syr.edu)|128.230.208.76|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1260 (1.2K) [text/x-c]
Saving to: `exploit.c'

100%[=====>] 1,260      --.-K/s   in 0s

2016-04-01 13:19:57 (7.06 MB/s) - `exploit.c' saved [1260/1260]

[04/01/2016 13:19] root@ubuntu:/home/seed/l2# ls
call_shellcode.c exploit.c stack.c
[04/01/2016 13:19] root@ubuntu:/home/seed/l2# vim call_shellcode.c
[04/01/2016 13:21] root@ubuntu:/home/seed/l2# gcc -z execstack -o call_shellcode
call_shellcode.c
[04/01/2016 13:21] root@ubuntu:/home/seed/l2# ./call_shellcode
#
[04/01/2016 13:22] root@ubuntu:/home/seed/l2# exit
exit
[04/01/2016 13:22] seed@ubuntu:~$ sudo su root
[04/01/2016 13:22] root@ubuntu:/home/seed# gcc -o stack -z execstack -fno-stack-p
rotector stack.c
gcc: error: stack.c: No such file or directory
gcc: fatal error: no input files
compilation terminated.
[04/01/2016 13:22] root@ubuntu:/home/seed# ls
Desktop  examples.desktop  openssl_1.0.1-4ubuntu5.11.debian.tar.gz  Public
Documents  l2                openssl_1.0.1-4ubuntu5.11.dsc             Templates
Downloads  Music             openssl_1.0.1.orig.tar.gz                 Videos
elggData  openssl-1.0.1     Pictures
[04/01/2016 13:22] root@ubuntu:/home/seed# cd l2
[04/01/2016 13:23] root@ubuntu:/home/seed/l2# ls
call_shellcode call_shellcode.c exploit.c stack.c
[04/01/2016 13:23] root@ubuntu:/home/seed/l2# gcc -o stack -z execstack -fno-stac
k-protector stack.c
[04/01/2016 13:23] root@ubuntu:/home/seed/l2# ls
call_shellcode call_shellcode.c exploit.c stack stack.c

```

Figure 2: Running call_shellcode.c

```

Documents  l2          openssl_1.0.1-4ubuntu5.11.dsc          Templates
Downloads  Music        openssl_1.0.1.orig.tar.gz          Videos
elggData   openssl-1.0.1      Pictures

[04/01/2016 13:22] root@ubuntu:/home/seed# cd l2
[04/01/2016 13:23] root@ubuntu:/home/seed/l2# ls
call_shellcode  call_shellcode.c  exploit.c  stack.c
[04/01/2016 13:23] root@ubuntu:/home/seed/l2# gcc -o stack -z execstack -fno-stack-protector stack.c
[04/01/2016 13:23] root@ubuntu:/home/seed/l2# ls
call_shellcode  call_shellcode.c  exploit.c  stack  stack.c
[04/01/2016 13:23] root@ubuntu:/home/seed/l2# chmod 4755 stack
[04/01/2016 13:23] root@ubuntu:/home/seed/l2# exit
exit
[04/01/2016 13:23] seed@ubuntu:~$ cd l2
[04/01/2016 13:23] seed@ubuntu:~/l2$ ls
call_shellcode  call_shellcode.c  exploit.c  stack  stack.c
[04/01/2016 13:23] seed@ubuntu:~/l2$ ./stack
Segmentation fault (core dumped)
[04/01/2016 13:24] seed@ubuntu:~/l2$ vim stack.c
[04/01/2016 13:24] seed@ubuntu:~/l2$ vim exploit.c
[04/01/2016 13:25] seed@ubuntu:~/l2$ ls
call_shellcode  call_shellcode.c  exploit.c  stack  stack.c
[04/01/2016 13:25] seed@ubuntu:~/l2$ sudo su
[04/01/2016 13:25] root@ubuntu:/home/seed/l2# vim exploit.c
[04/01/2016 13:26] root@ubuntu:/home/seed/l2# gcc -o exploit exploit.c
exploit.c: In function 'main':
exploit.c:30:20: error: 'shellcode' undeclared (first use in this function)
exploit.c:30:20: note: each undeclared identifier is reported only once for each
function it appears in
[04/01/2016 13:26] root@ubuntu:/home/seed/l2# vim exploit.c
[04/01/2016 13:26] root@ubuntu:/home/seed/l2# gcc -o exploit exploit.c
[04/01/2016 13:26] root@ubuntu:/home/seed/l2# ./exploit
[04/01/2016 13:26] root@ubuntu:/home/seed/l2# ./stack
#
[04/01/2016 13:26] root@ubuntu:/home/seed/l2# /sbin/sysctl -w kernel.randomize_va_space=2
kernel.randomize_va_space = 2
[04/01/2016 13:30] root@ubuntu:/home/seed/l2# ./stack

```

Figure 3: Successfully running exploit.c and stack.c

```

[04/01/2016 13:23] root@ubuntu:/home/seed/l2# chmod 4755 stack
[04/01/2016 13:23] root@ubuntu:/home/seed/l2# exit
exit
[04/01/2016 13:23] seed@ubuntu:~$ cd l2
[04/01/2016 13:23] seed@ubuntu:~/l2$ ls
call_shellcode  call_shellcode.c  exploit.c  stack  stack.c
[04/01/2016 13:23] seed@ubuntu:~/l2$ ./stack
Segmentation fault (core dumped)
[04/01/2016 13:24] seed@ubuntu:~/l2$ vim stack.c
[04/01/2016 13:24] seed@ubuntu:~/l2$ vim exploit.c
[04/01/2016 13:25] seed@ubuntu:~/l2$ ls
call_shellcode  call_shellcode.c  exploit.c  stack  stack.c
[04/01/2016 13:25] seed@ubuntu:~/l2$ sudo su
[04/01/2016 13:25] root@ubuntu:/home/seed/l2# vim exploit.c
[04/01/2016 13:26] root@ubuntu:/home/seed/l2# gcc -o exploit exploit.c
exploit.c: In function 'main':
exploit.c:30:20: error: 'shellcode' undeclared (first use in this function)
exploit.c:30:20: note: each undeclared identifier is reported only once for each
function it appears in
[04/01/2016 13:26] root@ubuntu:/home/seed/l2# vim exploit.c
[04/01/2016 13:26] root@ubuntu:/home/seed/l2# gcc -o exploit exploit.c
[04/01/2016 13:26] root@ubuntu:/home/seed/l2# ./exploit
[04/01/2016 13:26] root@ubuntu:/home/seed/l2# ./stack
#
[04/01/2016 13:26] root@ubuntu:/home/seed/l2# /sbin/sysctl -w kernel.randomize_v
a_space=2
kernel.randomize_va_space = 2
[04/01/2016 13:30] root@ubuntu:/home/seed/l2# ./stack
#
[04/01/2016 13:31] root@ubuntu:/home/seed/l2# ./stack
#
[04/01/2016 13:31] root@ubuntu:/home/seed/l2# ./stack
#
[04/01/2016 13:31] root@ubuntu:/home/seed/l2# gcc -o stack -z execstack stack.c
[04/01/2016 13:34] root@ubuntu:/home/seed/l2# ./stack
*** stack smashing detected ***: ./stack terminated
Segmentation fault (core dumped)
[04/01/2016 13:34] root@ubuntu:/home/seed/l2# █

```

Figure 4: Turning on memory layout randomization, running program, compiling with stack smash detection, running program yet again