Joseph Guzman

1/4/2020

<div align="center">Leviathan03</div>

This is the login info for this lab:

```
ssh server: leviathan.labs.overthewire.org
port: 2223
username: leviathan3
password: Ahdiemoo1j
```

In this lab you are again given an executable. It is named `level3`. This lab felt much simpler than the last couple labs. The executable prompts the user for a password. I used the `ltrace` command to try to figure out what it was doing. Below I should my terminal output. I ran the executable with ltrace and provided "asdf" as my password guess.

```
leviathan3@leviathan:~$ ltrace ./level3
__libc_start_main(0x8048618, 1, 0xffffdd44, 0x80486d0 <unfinished ...>
strcmp("h0no33", "kakaka")
= -1
printf("Enter the password> ")
= 20
fgets(Enter the password> asdf
"asdf\n", 256, 0xf7fc55a0)
= 0xffffdb50
strcmp("asdf\n", "snlprintf\n")
= -1
puts("bzzzzzzzzap. WRONG"bzzzzzzzzap. WRONG
)                                                    = 19
+++ exited (status 0) +++
```

You can clearly see with this output that my password guess is being compared with `snlprintf\n`. This means that `snlprintf\n` is the password. Below I show the output with this guess. After entering the correct password you're given a shell with leviathan4 permissions. I then cat the password file.

```
leviathan3@leviathan:~$ ./level3
```

```
Enter the password> snlprintf
[You've got shell]!
$ cat /etc/leviathan_pass/leviathan4
vuH0coox6m
$
leviathan3@leviathan:~$ ./level3
Enter the password> snlprintf
[You've got shell]!
$ whoami
leviathan4
$ cat /etc/leviathan_pass/leviathan4
vuH0coox6m
$
```

This is the login info for the next lab:

```
ssh server: leviathan.labs.overthewire.org
port: 2223
username: leviathan4
password: vuH0coox6m
```