GB200 writeup DEFCON CTF quals

In the challenge "Grab Bag" 200 find a server running on port 6000 and which give us the key: "Never \ $ olv3d!". When we used to connect the port and send any character we got the following output:

```
000111222333444555000111222333444555000111222333444555
```

After that the system expected a post and responded with another similar row of numbers or a bad message message. The analysis found:

1. The numbers were only from 0 to 5.

2. The error message is generated every 4 numbers, so that the system was 4 expected numbers. So we had combinations from 0000 to 5555.

3. If not return a correct sequence is then alleged generated an error.

The solution:

After trying different things I tried every combination of numbers like: *0000, 1111, 2222, 3333, 4444, 5555,* the one that generated a different response was: 2222, with this number we got a **"0"** then the program crashes (close socket).

Then I tried to send you information differently:

```
$ Perl-e 'print "Never \ $ olv3d! \ N"' | nc pwn522.ddtek.biz 6000
```

and seeing that I could do it, then send the specific case of 2.

```
$ Perl-e 'print "Never \ $ olv3d! \ N2222"' | nc pwn522.ddtek.biz 6000
000111222333444555000111222333444555000111222333444555
000111222333444555000111222333444555000111222333444555
Let's not be too rough on our own ignorance, it's What Makes America Great!
```

I searched for this phrase on the Internet and found that the author was: Frank Zappa
I tried various combinations on the scoreboard, but eventually use the key:
KEY = "Let's not be too rough on our own ignorance, it's

What Makes America Great!"

Proving to be the correct KEY => + 200.
Easy no? : P

Pd:
This challenge was resolved during a safety class with SENA, thanks to them!.

POSTED BY NONROOT (C) 2010/2011 21:09
TAGS: 2011 , CTF , DEFCON , QUALS