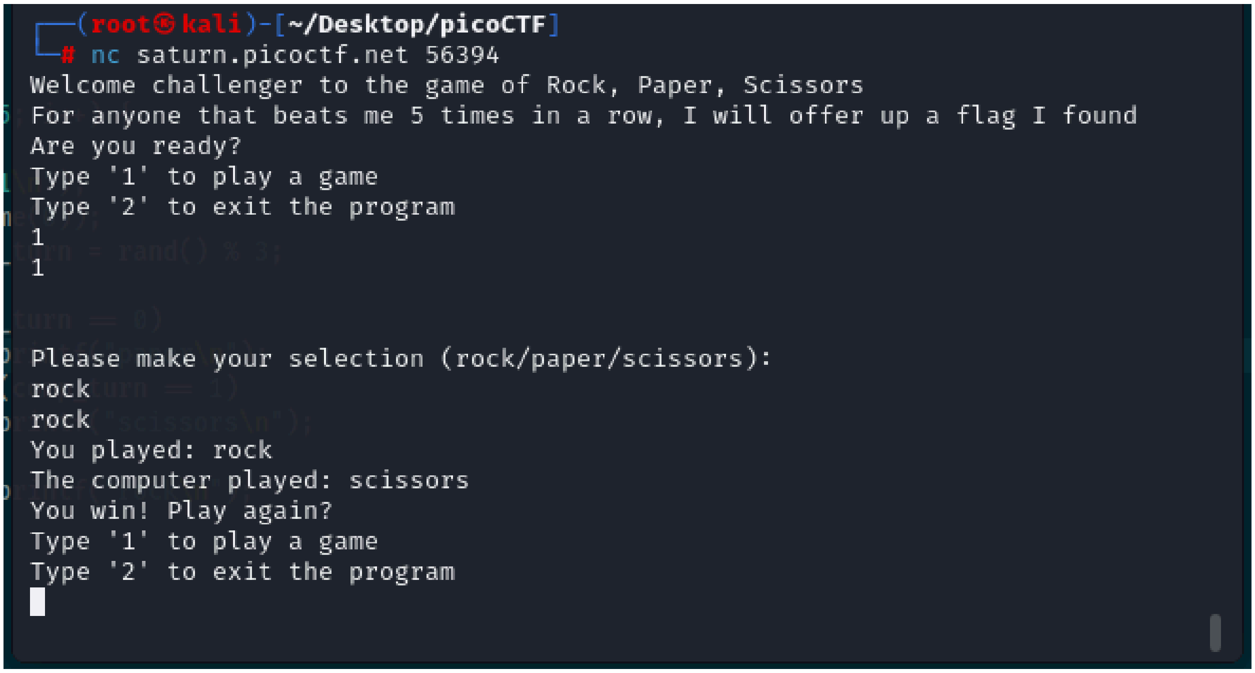
RPS

After running the `$ nc saturn.picoctf.net 64327` command in a Kali Linux terminal, I was presented with a program to play the game rock, paper, scissors. To get the flag, I must beat the machine at the game 5 times in a row.



```
┌──(root㉿kali)-[~/Desktop/picoCTF]
└─# nc saturn.picoctf.net 56394
Welcome challenger to the game of Rock, Paper, Scissors
For anyone that beats me 5 times in a row, I will offer up a flag I found
Are you ready?
Type '1' to play a game
Type '2' to exit the program
1
1


Please make your selection (rock/paper/scissors):
rock
rock
You played: rock
The computer played: scissors
You win! Play again?
Type '1' to play a game
Type '2' to exit the program
```

Opening up the source code of the game, there is a line of code srand(time(0)) which means it uses a timestamp as the seed number to generate responses for the game. This is easily exploitable because we can just copy this random function into our own exploit and it will generate the same seed and thus we can predict what the game will respond with. This rps.c file I wrote will provide the winning responses 5 times in a row based on the timestamp seed:

```
#include <stdio.h>
#include <stdlib.h>
#include <time.h>

int main() {

        int i;
        for (i = 0; i < 5; i++) {

                printf("1\n");
                srand(time(0));
                int comp_turn = rand() % 3;

                if (comp_turn == 0)
```

```
            printf("paper\n");
        else if (comp_turn == 1)
            printf("scissors\n");
        else
            printf("rock\n");

    }
    return 0;

}
```

After running the program as input to the game with the command ./rps | nc saturn.picoctf.net 57655 we get the flag:

Flag: picoCTF{50M3_3X7R3M3_1UCK_C85AF58A}