Quickcpy++

Hackstring: <48 số>rcos¹(10<??>!⊿▶t00xnor²⊿n00√(@20003:<strcpy>

Cách vào Quickcpy++

- 1. Vào 124an ở LineI/LineO -> Small font
- 2. Dùng strcpy để inject Quickcpy++ program. Mình sẽ làm mẫu địa chỉ đầu tiên là D8A0.
- 2.1 Overflow để lấy các kí tự in đậm ADAFDAC
 rồi nhập thành như sau:

123456
$$x$$
:
A = 10.000 A0 D1 A2 1F 01:
B = 1 2.0 01 02 80 D1 90 AC

[CALC][=][=][=]

2.2 Overflow để lấy các kí tự in đậm CCED rồi
nhập thành như sau:

123456
$$x$$
: C = 1 02 CC 3E 9D 23

[CALC][=][=]

2.3 Overflow để lấy các biến lỗi @ lần lượt là @<4D>, @<4E>, @<4F> rồi nhập thành như sau:

[CALC][=][=][=][↑]

2.4 Xoá các kí tự thừa hex <20> và 3 bytes <01> sinh ra ở đầu biến B và C sau đấy nhập như sau:

12345678901234567 89012345678°co 56789012345678°co s¹(10or! → t00xnor 2 → n00√(@20003: 00‱00‱0@.°@ ► tImP(∠0000@ln(10@!00E@ 000

[=][AC]

Tương tự với 2 địa chỉ còn lại là D8C0 và D8E0.

Riêng Launcher thì ta không cần nhập

rcos⁻¹(10<??>!」►t00xnor²」**n**00√(@20003: mà chỉ cần <48 số><Launcher>

Bonus: Với D8C0, [address] chính là địa chỉ mà khi vào được Quickcpy++ bạn sẽ bắt đầu inject từ địa chỉ đó.

VD bạn muốn inject từ EA30 trong quickcpy++ thì thay [address] ở

B = 1 2.0 9C 16 [address] 80 0E thành 30 EA

or © 0 0 0 0 ... thành 0 © (vì token của 30 là 0, token của EA là 0)

Cách dùng Quickcpy++

- Ta sẽ inject chương trình khác như sau:
- Nhập các hex của chương trình muốn inject vào Quickcpy++. Mỗi lần nhập

48 bytes = 96 chữ số = 3 dòng font nhỏ VD:

[Bin]

10E3420701000CE3F0F5020000000000 00000000000000002E62010010E3DA83 A89F00005CA00000949802000000000

[MENU][3]

Sau đó bạn sẽ thấy số 0 hiện ở góc dưới bên phải màn hình, đừng lo lắng mà hãy nhập 3 dòng tiếp theo, đừng bấm [AC] hay gì nhé

Quickcpy++ Program

D8A0:

123456*x*:

A = 10.000 A0 D1 A2 1F 01:

B = 1 2.0 01 02 80 D1 90 AC

123456*x*:

C = 1 02 CC 3E 9D 23

[CALC][=][=][=][+][->]

[->]x5 [->]x4 [DEL]x4 [->]x6 [->]x3 [DEL]x3

D8C0:

```
or @ 0 0 0 0 - 0 6 @ 2 0 [address] @ @ 1 0
RanInt#( ° 0 0 0 0 × @ 0 0 @ tanh( 1 0
```

123456*x*:

A = 10.000 C0 D1 A2 1F A0:

 $B = 1 \ 2.0 \ 9C \ 16 \ [address] \ 80 \ 0E$

123456*x*:

C = 1 9F BC 23

[CALC][=][=][=][+][->] [->]x5 [->]x4 [DEL]x4 [->]x6 [->]x3 [DEL]x3

D8E0:

0 0 . Q(1 0 efRanIn Mean(0 •a+bi @ 2 0 . Q(1 0 or @ or ! p @ or @

123456*x*:

A = 10.000 E0 D1 A2 1F 62:

B = 1 F.AEF 5A D2 03 62 A0

123456*x*:

C = 1 EF A0 BF A0 EF 23

[CALC][=][=][=][^][->]

[->]x5 [->]x3 [DEL]x3 [->]x6 [->]x3 [DEL]x3

Launcher:

<48 số>. Q(1 0 @ *t @ 0 *a+bi @ 2 0 . Q(
1 0 or @ or ! Q(@ 2 0 or @ p @ 0 0
Mean(

123456*x*:

A = 10.000 62 11 D1 02 D2:

 $B = 1 \ 0.3 \ 62 \ A0 \ EF \ A0 \ 62 \ 0D$

123456*x*:

C = 1 A0 EF BF 5A 23

[CALC][=][=][=][↑][->] [->]x5 [->]x3 [DEL]x3 [->]x7 [->]x3 [DEL]x3

Hex editor

```
E3 42 07 01 00 0C E3 F0 F5 02 00 00 00
                    00 2E 62 01 00 10
        00 00 00
                 00
                                       E3 DA 83
     00 00 5C A0 00 00 94 98 02 00 00 00 00
70 61 01 00 3E 9D 00 00 2F 00 90
                                C7 00 00 3E 9D
     04 00 D4 4B 01 00 3E 9D 00
                                00
                                    A7 00 F4
01 00 66 E3 D4 4B 01 00 08 40 02 00 00 00 00
     00 00 74 1F 02 00 70 61 01 00 F4 FC 01 00
                                C7 00
     86 8C 02 00 98 E3 00 00 90
                                       00
     A8 00 D4 4B 01 00 08 40 02 00 00 00 00
     00 00 74 1F 02 00 42 E6 3E 9D 00 00
  9C 00 00 44 E6 0F
                     00
                       AE 1B 02 00
                                    CC 61 01 00
16 39 01 00 D6 4B 01 00 52 0B 02 00 00 00
     02 00 3E 9D 00 00 44 E6 90 C7 00
                                       00 3E 9D
  00 38
        00 F4
              FC
                 01
                     00
                       EE E3 D4 4B 01 00 08 40
     00 00 00 00 00 00 00 00 74 1F 02 00 40 E6
  9D 00 00 00 00 A0 9C 00 00 1A E4 00 00 A5 9C
00 00 00 00 02 00 B0 3A 01 00 01 00 80 0E 01 00
44 E6 00 00 52 E5 36 16 02 00 00 00 BC 6E 01 00
00 00 74 1F 02 00 42 E6 3E 9D 00 00 01 00 A0 9C
  00 00 00 00 00 B0 3A 01 00 FA E5 74 1F 02 00
86 E4 D6 4B 01 00 A5 9C 00 00 00 00 00 00 F4 FC
```

```
00 1F FC 18 96 01 00 A8 9F 00 00 5C A0 00 00
3E 9D 00 00 C4 00 F4 FC 01 00 80 E4 D4 4B 01 00
08 40 02 00 00 00 00 00 00 00 00 74 1F 02 00
C8 E4 3E 9D 00 00 00 00 A5 9C 00 00 00 00 00
F4 FC 01 00 1E FC 18 96 01 00 A8 9F 00 00 5C A0
  00 3E 9D 00 00 68 00 F4 FC 01 00 C2 E4 D4 4B
01 00 08 40 02 00 00 00 00 00 00 00 00 00 74 1F
     00 00 3E 9D 00 00 00 00 F4 FC 01 00 26
18 96 01 00 A8 9F 00 00 5C A0 00 00 3E 9D 00 00
  00 F4 FC 01 00 FA E4 D4 4B 01 00 08 40 02 00
00 00 00 00 00 00 00 00 74 1F 02 00 B0 3A 01 00
02 E6 74 1F 02 00 40 E6 3E 9D 00 00 00 00 A0 9C
  00 00 00 00 00 30 BF 00 00 08 40 02 00 00 00
     00 00 00 00 74 1F 02 00 40 E6 3E 9D
01 00 A0 9C 00 00 00 00 00 B0 3A 01 00 52 E5
74 1F 02 00 40 E6 3E 9D 00 00 FF FF A0 9C 00
42 E6 42 E6 3E 9D 00 00 00 00 A5 9C 00 00 40 E6
00 00 3E 9D 00 00 00 00 A0 9C 00 00 BE E5 00 00
A5 9C 00 00 00 00 00 00 30 BF 00 00 70 61 01 00
FA 3F 02 00 00 00 00 00 00 00 00 A8 9F 00 00
5C A0 00 00 E6 C1 00 00 00 00 4E E6 A5 9C 00 00
```

```
EA ED 01 00 50 E6 00 00 00 00
   00
      00
         00
                                          D6 4B
01 00 A5 9C 00 00 5A E6 00 00 6A 21 01 00 00 00
74 82 01 00 10 40 02 00 D6 4B 01 00 A5 9C 00 00
00 00 00 00 2E 62 01 00 D4 DD 00 06 36 9D 00 00
2E 62 01 00 05 05 48 E6 80 8F 00 00 2E 62 01 00
05 25 53 E6 80 8F 00 00 7E 94 00 00 80 75 01 00
00 05 20 00 86 53 01 00 3C 9F 00 00 5C A0 00
48 A2 00 00 32 E6 3E 9D 00 00 01 00 A5 9C
                                          00
00 00 00 00 A5 30 01 00 40 03 60 E6 00 E3 00 00
32 89 0E 00 00 00 B0 3A 01 00 00 E3 74 1F 02 00
51 D5 00 00 00 00 00 00 41 64 64 72 3A 20 00 00
00 00 00 56 61 6C 75 65 3A 20 00 00 00 00 00 00
```

Launcher:

```
<48 số> x @ 0 0 G or 0 0 = 0 1 0 ( @ G

•Simp 0 m 0 0 @ tanh( 1 0 2 LCM( 1 0 0
0 = 0 1 0 M @ G •Simp ( p \ m 2 LCM( 1
0 0 0 √( @ 2 0
```

```
123456x:

0 = 10.000 20 9F A0 03 E9:

0 = 1 18 03 E9 01 1F 23
```

[CALC][=][=][=][↑][->] [->] [DEL] [->]x4 [->]x3 [DEL]x3

Lưu ý: Nhập xong Launcher của Hex Editor thì ấn [=][->] chứ KHÔNG phải [=][AC]!