Introduction

This ctf was apart of the **2025 - BuckeyeCTF Competition**. The challenge started with the following:

Description: "I don't know anyone with the same favorite number as me :("
File: "lonely_bot"

```
└──╼ $file lonely_bot
lonely_bot: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV),
dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2,
BuildID[sha1]=1d9362a9b9033f3a19668652211646b0204debe5, for GNU/Linux 3.2.0,
stripped
```

After running it you get this question and response.

```
└──╼ $./lonely_bot
What's your favorite number? :D
69
Ah, a fan of "69"...
Goodbye.
```

Start

So to start I open the ELF in **Ghidra** to decompile and analyze.

So first I notice 2 functions that have a decent amount of code

Function 1 entry:

```
void processEntry entry(undefined8 param_1,undefined8 param_2)

{
  undefined auStack_8 [8];

__libc_start_main(FUN_00102154,param_2,&stack0x00000008,FUN_001021c0,FUN_001
02230,param_1,
                  auStack_8);
  do {
                  /* WARNING: Do nothing block with infinite loop */
```

```
  } while( true );
}
```

After reading this we see that `__libc_start_main` calls function `FUN_00102154` which means that it should be main

Function 2 FUN_00102154:

```
undefined8 FUN_00102154(void)
{
  ulong i;

  for (i = 0; i < 159; i = i + 1) {
    (&i)[i + 2] = (ulong)(&PTR_LAB_00105020)[i];
  }
  return 0;
}
```

Reading this function we see that it takes the memory address of i, skips two slots, plus current i more slots over, then assigns that to that i-th element of an array called `PTR_LAB_00105020`

Analysis

So I checked out the array `PTR_LAB_00105020` in ghidra and saw it printing out the introduction prompt "Whats your favorite number?"

Now what was interesting there was a lot of 8 byte data pairs in between this and the "Goodbye!" message. I scrolled down until I saw data that wasent just 00.

```
        00105190 11             ??         11h
        00105191 cc             ??         CCh
        00105192 50             ??         50h    P
        00105193 fa             ??         FAh
        00105194 97             ??         97h
        00105195 a2             ??         A2h
        00105196 e8             ??         E8h
        00105197 5c             ??         5Ch    \
        00105198 31 21 10       addr       LAB_00102131
                 00 00 00
                 00 00
        001051a0 2f 21 10       addr       LAB_0010212f
                 00 00 00
                 00 00
        001051a8 40 55 10       addr       DAT_00105540
```

```
= ??
                00 00 00
                00 00
        001051b0 2b 21 10       addr        LAB_0010212b
                00 00 00
                00 00
        001051b8 54             ??          54h    T
        001051b9 fd             ??          FDh
        001051ba 35             ??          35h    5
        001051bb 8c             ??          8Ch
        001051bc a4             ??          A4h
        001051bd cc             ??          CCh
        001051be bc             ??          BCh
        001051bf 25             ??          25h    %
        001051c0 39 21 10       addr        LAB_00102139
                00 00 00
                00 00
        001051c8 2f 21 10       addr        LAB_0010212f
                00 00 00
                00 00
        001051d0 68 55 10       addr        DAT_00105568
= ??
                00 00 00
                00 00
        001051d8 2d 21 10       addr        LAB_0010212d
                00 00 00
                00 00
        001051e0 7d             ??          7Dh    }
        001051e1 72             ??          72h    r
        001051e2 35             ??          35h    5
        001051e3 ea             ??          EAh
        001051e4 8e             ??          8Eh
        001051e5 6e             ??          6Eh    n
        001051e6 00             ??          00h
        001051e7 00             ??          00h
        001051e8 31 21 10       addr        LAB_00102131
                00 00 00
                00 00
        001051f0 2f 21 10       addr        LAB_0010212f
                00 00 00
                00 00
        001051f8 48 55 10       addr        DAT_00105548
= ??
                00 00 00
                00 00
        00105200 2b 21 10       addr        LAB_0010212b
```

```
                00 00 00
                00 00
        00105208 5d              ??         5Dh    ]
        00105209 21              ??         21h    !
        0010520a 06              ??         06h
        0010520b 9c              ??         9Ch
        0010520c eb              ??         EBh
        0010520d 20              ??         20h
        0010520e 00              ??         00h
        0010520f 00              ??         00h
        00105210 39 21 10        addr       LAB_00102139
                 00 00 00
                 00 00
```

After looking at these 4 sets of bytes, I see that after each 2 sets of bytes, it made a call to a code location to `LAB_00102139`

```
void UndefinedFunction_00102139(undefined8 param_1,ulong param_2)

{
  ulong *in_RAX;

  *in_RAX = *in_RAX ^ param_2;
  return;
}
```

This takes in the value stored in `RAX` and XOR's it with the XOR 8 byte key. I couldent find anything that was put into RAX, but the function came perfectly after each two pairs so I thought it might be the first 8 bytes.
This is run for both pairs of two 8 byte text/key. So I think I ran the XOR of each of the two pairs

Pair 1

- cipher text (addr `0x00105190` → `0x00105197`):
  `11 cc 50 fa 97 a2 e8 5c`
- key (addr `0x001051b8` → `0x001051bf`):
  `54 fd 35 8c a4 cc bc 25`
- XOR result (cipher ⊕ key):
  Hex: `45 31 65 76 33 6e 54 79`
  ASCII: `E1ev3nTy`
  Pair 2

- cipher text (addr `0x001051e0` → `0x001051e7`):
  `7d 72 35 ea 8e 6e 00 00`
- key (addr `0x00105208` → `0x0010520f`):
  `5d 21 06 9c eb 20 00 00`
- XOR (cipher ⊕ key):
  hex: `20 53 33 76 65 4e 00 00`
  ascii: ␣`S3veN` (leading space, then `S3veN`, followed by two `\x00` bytes)
  After inserting this into the program, I received the flag.

```
└──╼ $./lonely_bot
What's your favorite number? :D
E1ev3nTy S3veN
bctf{Th4t5_a_n1C3_NuMB3r}
```