

Soluzione alternativa (trovata su Telegram e riscritta/riadattata)

All'interno del main, vi è un "while" in attesa dell'evento da tastiera che controlla lo stato di vittoria; se inverti il salto vinci in automatico.

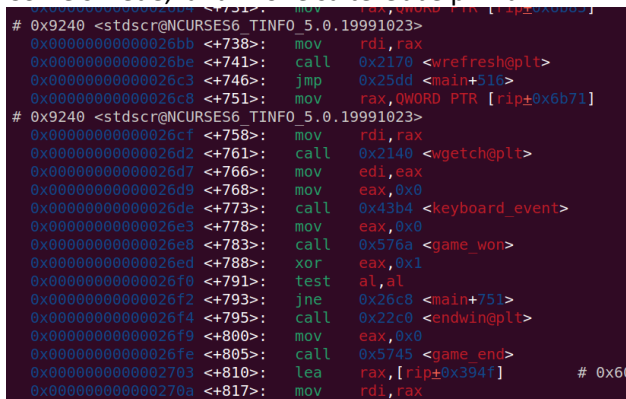
Come si vede sotto, si chiama la funzione per controllare se è stato vinto il gioco (game_won), sotto c'è il salto che controlla cosa ha tornato la funzione e decide se loopare. Se lo inverti vinci in automatico.

La call si trova dentro *game_won*, come si vede qui:



```
0x000026c3 jmp 0x25dd
0x000026c8 mov rax, qword [stdscr] ; obj.stdscr_NCURSES6_TINFO_5.0.19991023
; 0x9240
0x000026cf mov rdi, rax
0x000026d2 call wgetch ; sym.imp.wgetch
0x000026d7 mov edi, eax ; unsigned long long arg1
0x000026d9 mov eax, 0
0x000026de call dbg.keyboard_event
0x000026e3 mov eax, 0
0x000026e8 call dbg.game_won
0x000026ed xor eax, 1
0x000026f0 test al, al
0x000026f2 jne 0x26c8 <- Salto da invertire
0x000026f4 call endwin ; sym.imp.endwin
0x000026f9 mov eax, 0
```

Come si vede, la funzione salterebbe prima:



```
# 0x9240 <stdscr@NCURSES6_TINFO_5.0.19991023>
0x00000000000026bb <+738>: mov rdi, rax
0x00000000000026be <+741>: call 0x2170 <wrefresh@plt>
0x00000000000026c3 <+746>: jmp 0x25dd <main+516>
0x00000000000026c8 <+751>: mov rax, QWORD PTR [rip+0x6b71]
# 0x9240 <stdscr@NCURSES6_TINFO_5.0.19991023>
0x00000000000026cf <+758>: mov rdi, rax
0x00000000000026d2 <+761>: call 0x2140 <wgetch@plt>
0x00000000000026d7 <+766>: mov edi, eax
0x00000000000026d9 <+768>: mov eax, 0x0
0x00000000000026de <+773>: call 0x43b4 <keyboard_event>
0x00000000000026e3 <+778>: mov eax, 0x0
0x00000000000026e8 <+783>: call 0x576a <game_won>
0x00000000000026ed <+788>: xor eax, 0x1
0x00000000000026f0 <+791>: test al, al
0x00000000000026f2 <+793>: jne 0x26c8 <main+751>
0x00000000000026f4 <+795>: call 0x22c0 <endwin@plt>
0x00000000000026f9 <+800>: mov eax, 0x0
0x00000000000026fe <+805>: call 0x5745 <game_end>
0x0000000000002703 <+810>: lea rax, [rip+0x394f] # 0x60
0x000000000000270a <+817>: mov rdi, rax
```

Quindi, basta invertire il salto (da JNZ a JZ come sempre) e si vince.