```
Prima del main viene chiamata questa funzione:

void _INIT_1(void)
{

long | Var1;

// La funzione ptrace viene utilizzata per tracciare o controllare processi.

// In questo caso, PTRACE_TRACEME viene utilizzato per consentire al processo corrente di essere tracciato.

| Var1 = ptrace(PTRACE_TRACEME, 0, 1, 0);

// Se ptrace restituisce -1, significa che il tracciamento non è permesso.

if (| Var1 == -1) {

// Stampa un messaggio di avviso.

puts("plz don\'t!");

// Esce dal programma con il codice di uscita -1.

exit(-1);

}

return;
}
```

In breve, questo snippet sta cercando di impedire al programma di essere tracciato. Utilizza la funzione **ptrace** con l'opzione **PTRACE_TRACEME** per permettere al processo corrente di essere tracciato. Se questa chiamata a **ptrace** restituisce -1, il programma stampa un messaggio di avviso e termina con un codice di uscita di -1. Il commento "plz don't!" sembra indicare che il programma non vuole essere tracciato e reagisce in modo appropriato se il tracciamento non è permesso.

Quindi un modo è quello di eliminare l'exit(-1) che fa terminare il programma. Però se provo a patcharlo da Ghidra poi il programma non va.

Allora provo a patchare l'argomento dell'if con: lvar == -2 in modo che non entri mai nell'if

```
2 void _INIT_1(void)
001012c2 55
                                                                           4 {
                           PUSH
                                        RBP, RSP
001012c6 b9 00 00
                           MOV
                                        ECX. 0x0
                                                                               lVar1 = ptrace(PTRACE_TRACEME, 0, 1, 0);
001012cb ba 01 00
                           MOV
                                        FDX.0x1
                                                                                 f (lVarl == -2) {
  puts("plz don\'t!");
001012d0 be 00 00
                                                                                                   /* WARNING: Subroutine does not return */
                           MOV
                                        ESI,0x0
                                                                          11
                                                                                 exit(-1);
001012d5 bf 00 00
                           MOV
                                        EDI, 0x0
                                                                               return;
001012da b8 00 00
                                                                          14 )
15
          00 00
001012df e8 8c fd
                           CALL
                                        <EXTERNAL>::ptrace
001012e8 75 16
001012ea 48 8d 3d
                                        RDI,[s_plz_don't!_001025
                           LEA
001012fl e8 4a fd
                                        <EXTERNAL>::puts
                           CALL
001012f6 bf ff ff
ff ff
                                       EDI, Oxffffffff
                           MOV
001012fb e8 80 fd
ff ff
                           CALL
                                        <EXTERNAL>::exit
                       -- Flow Override: CALL_REGRN (CALL_TER)
                      LAR 00101300
```

Ho fatto tasto destro sopra l'istruzione (CMP RAX...) e ho messo pacth instruction e al posto di -0x1 ho messo -0x2.

Poi ho esportato il file facendo file \rightarrow export program \rightarrow format:file originale e l'ho esportato sulla cartella condivisa su cui lavoro.

Poi se apro il file con gdb e metto il breakpoint a strncmp e faccio run con una stringa >2 e faccio un po' di volte *si* allora vedo il flag in chiaro!!

Per il patching del file : https://www.tripwire.com/state-of-security/ghidra-101-binary-patching