Hungry_Friends

Description
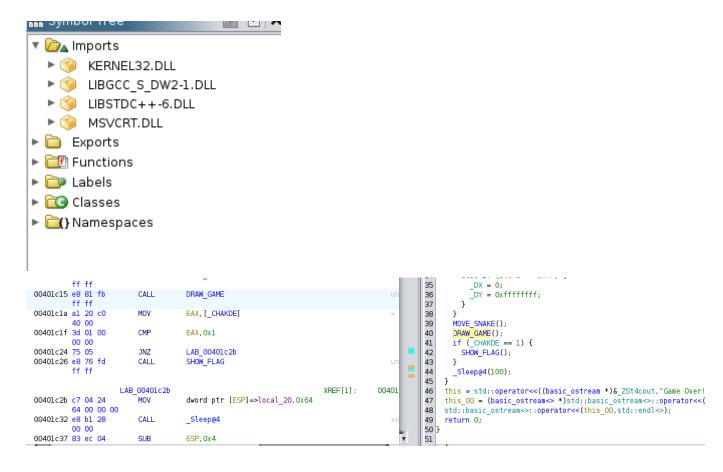
Feed my friend.

Category

#reverse

Solution

Note: This challenge is extremely annoying as the given file is a PE32 file written in C++ 2006. Meaning that we need to get on environment older than Windows 8.

Reading the code, we can see that this is a snake game, and to get the flag, you need 9999 score. Meaning we can simply change the required score to 1 or 0 (I didn't change to 0 with fear that it would break the game)

```
    }
    else if (iVar1 == 0x77) {
        _DX = 0;
        _DY = 0xffffffff;
    }
}
MOVE_SNAKE();
DRAW_GAME();
if (_CHAKDE == 9999) {
    SHOW_FLAG();
}
_Sleep@4(100);
}
this = std::operator<<((basic_ostream *)&_ZSt4cout,"Game Over! Score: ");
this_00 = (basic_ostream<> *)std::basic_ostream<>::operator<<((basic_ostream<> *)this,
std::basic_ostream<>::operator<<(this_00,std::endl<>));
return 0;
```

Another important thing to add is that the imported DLLs file in the original code weren't there, so I manually added them.

```
            ff ff                                                    35        _DX = 0;
00401c15 e8 81 fb       CALL    DRAW_GAME              un             36        _DY = 0xffffffff;
            ff ff                                                    37      }
00401c1a a1 20 c0       MOV     EAX,[_CHAKDE]         =             38    }
            40 00                                                    39    MOVE_SNAKE();
00401c1f 3d 01 00       CMP     EAX,0x1                             40    DRAW_GAME();
            00 00                                                    41    if (_CHAKDE == 1) {
00401c24 75 05          JNZ     LAB_00401c2b         ■             42      SHOW_FLAG();
00401c26 e8 76 fd       CALL    SHOW_FLAG            un             43    }
            ff ff                                                    44    _Sleep@4(100);
                                                         ■             45  }
            LAB_00401c2b                XREF[1]:    00401             46  this = std::operator<<((basic_ostream *)&_ZSt4cout,"Game Over!
00401c2b c7 04 24       MOV     dword ptr [ESP]=>local_20,0x64       47  this_00 = (basic_ostream<> *)std::basic_ostream<>::operator<<(
            64 00 00 00                                              48  std::basic_ostream<>::operator<<(this_00,std::endl<>);
00401c32 e8 b1 28       CALL    _Sleep@4            vo             49  return 0;
            00 00                                                    50 }
00401c37 83 ec 04       SUB     ESP,0x4                             51
```

So when I launch the application on Windows 7, for any DLL files that are missing. Download them on the internet with architecture = 32 bit.

Playing the game gives the flag