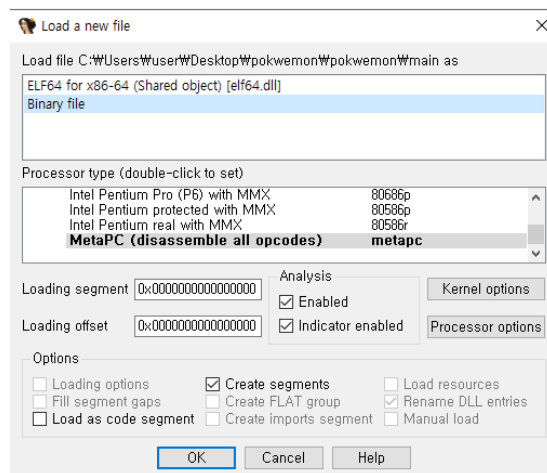


3S CTF

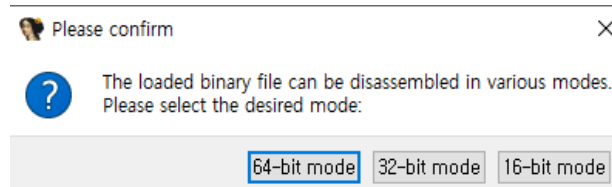
PWN-PokWemoN

SWING 32 기 한재희

일단 pwngdb 설치가 오류나서 다른 방법으로 살펴봐야 하는데 IDA 이용해서 파일을 열어봤다.



이런 창이 떠서 바이너리 파일로 열어봤다.



64 비트로 하고 살펴봤다.

IDA 에서도 hex 값을 볼 수 있었는데 내려보다가

```
} .....  
; .....Normal.F  
} ire.Water.Grass.  
7 Electric.Ice.Fig  
: hting.Poison.Gro  
} und.Flying.Psych  
} ic.Bug.Rock.Ghos  
t.Dragon.Dark.St  
: eel.Fairy.r./pro  
; c/self/maps.fope  
} n.%lx....'.'.'..
```

불, 물 이렇게 써져 있길래 이 문제가 포켓몬 문제였어서 그런지 타입 별로 적혀있는 걸 확인할 수 있었다.

```

champion!..DAMAG
E·IS·CRITICAL!!!
!..DAMAGE·IS·WEA
K.....NO·DAMAG
E.....==·Health·
Bars·==·Opponent
·Pkwemon(%s):..
My·Pkwemon(%s):
.....====·Roun
d·%d·====.....
Opponent·Pkwemo
n(%s)'s·current·
health:·%d·|·dam
age:·%d.....
My·Pkwemon(%s)'
s·current·health
:·%d·|·damage:·%
d.....Choose·t
o·Attack(a),·Bas
ic·Attack(b),·or
·Defend(d):..·%c
.....Opponent
·Pkwemon·is·in·
defense·mode!...

```

또 내려보다가 읽어보니까 포켓몬들이 싸우는 걸 글씨로 표현해 놓은 것 같았다.

```

s..CONGRATUATION
!!!!.YOU·ARE·TH
E·PkwemoN·CHAMP
ION._____RANK
_____.|1.·KIM
.....9..|.|
2.·MIN.....
9..|.|3.·ROKAF..
.....9..|.|4.·G
ivMeInJ.....8..|
. |5.·JUN.....
..7..|.|.
.....|.|_

_|.ENTER·YOUR·NA
ME:.|1.%s10|..|2
.·KIM.....9
..|.|3.·MIN.....
.....9..|.|4.·RO
KAF.....9..|.
|5.·GivMeInJ....
·8..|.|6.·JUN...
.....7..|.
Choose·your·Pkw
emon's·type·(0.N

```


이 부분을 보니까 내가 직접 포켓몬 타입을 선택하고 그러는 것 같은데 우분투가 말을 안들어서... 너무 아쉽다. 포켓몬 챔피언이 되면 뭔가 플래그를 줄 것 같기도 하고 ctrl F 로 flag 관련 검색 해봤는데 나오는 건 없었다.

```

; Segment type: Regular
seg000      segment byte pi
            assume cs:seg0
            assume es:noth:
            db  7Fh ; 0
            db  45h ; E
            db  4Ch ; L
            db  46h ; F
            db   2
            db   1
            db   1
            dh   0

```

뭔가 다 db 로 덮혀있길래 데이터베이스로 열어보려 했는데 안열려서 확장자까지 .db 로
바꿔서 열어봤지만

pokwemon		▼ ↺	pokwemo	
이름	^	수정한 날짜	유형	
 main		2024-07-18 오후 8:34	Data Base File	

열리지 않았다.

우분투 gdb 를 꼭 고쳐서 설치한 후 실행을 해봐야겠다..