

OBTENCIÓN DE LOS PASSWORD DE NIVEL DE UN JUEGO

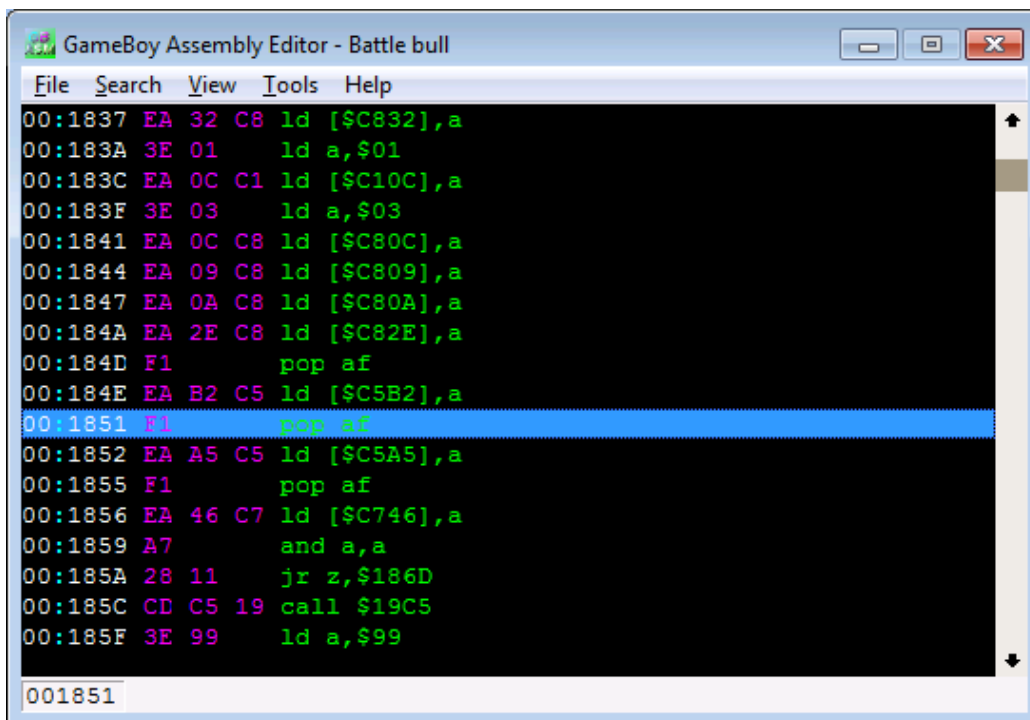
En este tutorial les voy a explicar como obtener los passwords de nivel de un juego en concreto pero que se puede aplicar a otros.

Para el ejemplo vamos a utilizar el juego "Battle Bull" de Gameboy en su versión europea.

Vamos a partir de que conocemos que la dirección de la RAM donde se guarda el número de nivel es la \$C10C.

¿Pero cómo se averigua esto?. Para averiguarlo debemos utilizar la búsqueda de cheats en algún emulador que lo permita (tal como GameLad), aunque no nos vamos a centrar en ello ya que no es el objetivo del tutorial.

Si abrimos el juego con el GbAsmEdit (Desensamblador de Gameboy), podemos ver el código fuente de "Battle Bull".



```
GameBoy Assembly Editor - Battle bull
File Search View Tools Help
00:1837 EA 32 C8 ld [$C832],a
00:183A 3E 01 ld a,$01
00:183C EA 0C C1 ld [$C10C],a
00:183F 3E 03 ld a,$03
00:1841 EA 0C C8 ld [$C80C],a
00:1844 EA 09 C8 ld [$C809],a
00:1847 EA 0A C8 ld [$C80A],a
00:184A EA 2E C8 ld [$C82E],a
00:184D F1 pop af
00:184E EA B2 C5 ld [$C5B2],a
00:1851 F1 pop af
00:1852 EA A5 C5 ld [$C5A5],a
00:1855 F1 pop af
00:1856 EA 46 C7 ld [$C746],a
00:1859 A7 and a,a
00:185A 28 11 jr z,$186D
00:185C CD C5 19 call $19C5
00:185F 3E 99 ld a,$99
001851
```

Podemos buscar en este programa el valor "EA 0C C1" que corresponde a la instrucción "ld [\$C10C],a".

Esta instrucción lo que hace es poner el valor que haya en "a" en la dirección \$C10C que es donde se almacena el número de nivel.

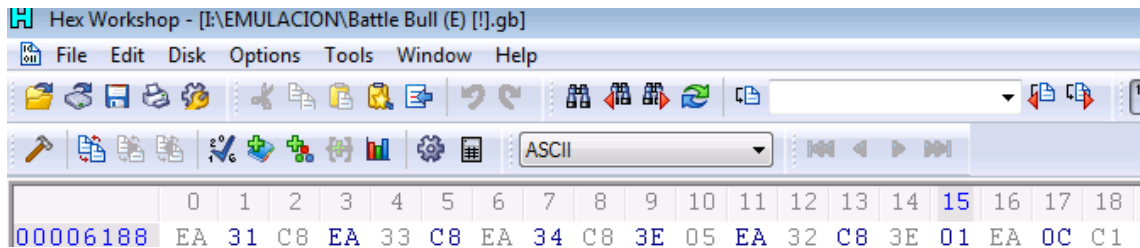
Buscando encontramos lo siguiente:

00:183A 3E 01 ld a,\$01 (Pone en a el valor \$01)

00:183C EA 0C C1 ld [\$C10C],a (Pone el valor \$01 en la dirección \$C10C)

En este código se pone el valor inicial del nivel (al inicio del juego empezamos en el nivel 1).

Una vez hecho esto nos basta con buscar estos valores hexadecimales en un editor (tal como HexWorkShop) y modificar el valor \$01 por cualquier otro para modificar el juego.



Vemos como los últimos valores que aparecen en la captura son los buscados (en concreto el byte 6204).

Podemos poner el valor \$02 y cargar el juego con el emulador y cuando perdamos todas las vidas nos aparecerá en pantalla el password correspondiente al nivel 2 (que es "BLBB").



Podemos repetir el proceso con los valores \$03-\$30 (que corresponde a los niveles 3-48).

Una vez hecho esto tendríamos todas las passwords del juego que son las siguientes:

Nivel 2: BLBB

Nivel 3: BQBB

Nivel 4: BVBB
Nivel 5: B0BB
Nivel 6: B4BB
Nivel 7: B8BB
Nivel 8: MBBB
Nivel 9: MGBB
Nivel 10: MLBB
Nivel 11: MQBB
Nivel 12: MVBB
Nivel 13: M0BB
Nivel 14: M4BB
Nivel 15: M8BB
Nivel 16: XBBB
Nivel 17: XGBB
Nivel 18: XLBB
Nivel 19: XQBB
Nivel 20: XVBB
Nivel 21: X0BB
Nivel 22: X4BB
Nivel 23: X8BB
Nivel 24: 7BBB
Nivel 25: 7GBB
Nivel 26: 7LBB
Nivel 27: 7QBB
Nivel 28: 7VBB
Nivel 29: 70BB
Nivel 30: 74BB
Nivel 31: 78BB
Nivel 32: GBBB

Nivel 33: GGBB
Nivel 34: GLBB
Nivel 35: GQBB
Nivel 36: GVBB
Nivel 37: G0BB
Nivel 38: G4BB
Nivel 39: G8BB
Nivel 40: RBBB
Nivel 41: RGBB
Nivel 42: RLBB
Nivel 43: RQBB
Nivel 44: RVBB
Nivel 45: R0BB
Nivel 46: R4BB
Nivel 47: R8BB
Nivel 48: \$F**

Si observamos las passwords a excepción de la del nivel 48 podemos ver como se forman.



Primeras contraseñas (Niveles 1-7):

La primera letra es B y las dos últimas también son B (para todos los niveles).

La segunda letra varía desde B, G, L, Q, V, 0, 4, 8.

Hay 4 espacios de distancia entre las letras que varían.

Siguientes contraseñas (Niveles 8-47):

El proceso es similar variando la segunda letra pudiendo ser una de las 8 letras vistas antes.

La primera letra varía en diagonal cuando se llega al final de las 8 letras (M, X, 7).

Después de esto, la primera letra comienza con la G y cuando se acaba con ésta se empieza con la que hay en diagonal y que corresponde a la letra R.

Contraseña del nivel 48:

\$F** : Esta password no sigue el proceso visto para el resto de contraseñas.