

Necesitamos:

iPhone en 1.1.4 o iPhone 3G en 2.0

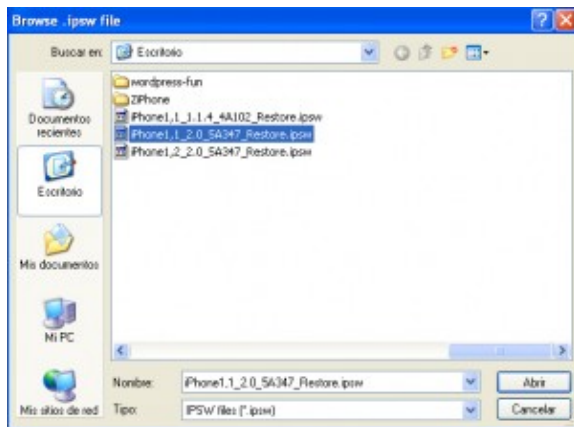
WinPwn 2.0.0.3– La podéis descargar desde

http://rapidshare.com/files/132425893/winpwn_2.0.0.3_Setup.zip.html

Firmware 2.0 para el iPhone desde http://appldnld.apple.com.edgesuite.net/content.info.apple.com/iPhone/061-4956.20080710.V50OI/iPhone1,1_2.0_5A347_Restore.ipsw o para el iPhone 3G desde http://appldnld.apple.com.edgesuite.net/content.info.apple.com/iPhone/061-4955.20080710.bgt53/iPhone1,2_2.0_5A347_Restore.ipsw o para el iPod desde http://uploaded.to/file/ih0z65/iPod1,1_2.0_5A347_Restore.ipsw.

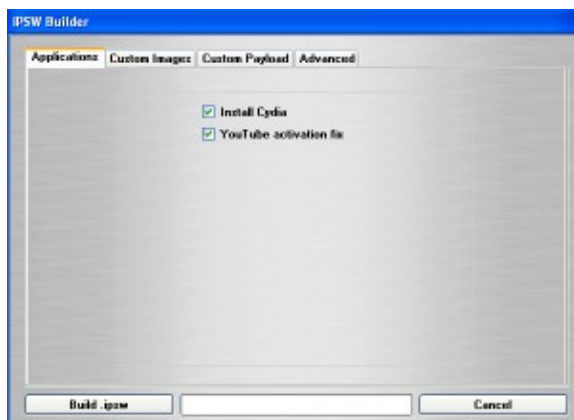
iTunes 7.7

- 1– Descargamos WinPwn.
- 2– Descargamos el firmware 2.0.
- 3– Instalamos WinPwn, lo abrimos y enchufamos el iPhone.
- 4– Cargamos el firmware 2.0 desde “Browse .ipsw”.



5– Pulsamos sobre “IPSW Builder” y creamos el firm personalizado.

5a– Marcamos “Install Cydia” y “YouTube activation Fix”.



5b– Personalizamos la imagen de arranque y de modo restauración, dejándo las originales, poniendo las que nos da el programa o seleccionando las que queremos nosotros.



5c- Nos descargamos el BootLoader y vamos a advanced. (necesario los 2: <http://ispazio.net/FFU/files/BL-39.bin.zip> <http://ispazio.net/FFU/files/BL-46.bin.zip>)

5d- Buscamos ambos Bootloader's y marcamos: "Activate iPhone", "Enable Baseband update", "Neuter Bootloader 3.9/4.6" y "Unlock baseband", siempre hablando de un iPhone 1.1.4. Para el 3G simplemente hay que marcar "Activate iPhone".



5e- Pulsamos sobre "Build .ipsw" y esperamos a que acabe la creación del firm personalizado.

6- Una vez creado el firm, pulsamos sobre Pwnage y seleccionamos el firm creado en el paso 5. Cuando acabe, iTunes estará listo para usar el firm personalizado.

7- Ponemos el iPhone en modo DFU (con el iPhone encendido pulsamos durante 10 segundo el botón home + sleep y pasados los 10 segundos soltamos el botón sleep y mantenemos el home otros 10 segundos, tiene que ser muy exacto, es recomendable usar algún reloj o cronómetro) y una vez iTunes lo detecte, pusamos shift + restaurar y seleccionamos el firm creado en el paso 5.

8- Cuando acabe la restauración se reiniciará el dispositivo y va a abrir una aplicación para terminar el proceso, debéis tocar la pantalla cada 15seg para que no se bloquee y ya tendremos un iPhone/iPod jailbrokeado en el firm 2.0.