Instrucciones (1ª revisión)

Primero restaura el ipod, descarga el iphuc http://rapidshare.com/files/61742428/iphuc.zip

1.- Carga http://jailbreak.toc2rta.com en el iPod

2.- Sal de iTunes, y mata el proceso ituneshelper.exe

3.- Extrae iPhuc a un directorio de tu ordenador

4.- Copia iTunesMobileDevice.dll de C:\Program Files\Common Files\Apple\Mobile Device Support\bin a la misma carpeta de iPhuc.exe

5.- Copia readline5.dll desde http://gnuwin32.sourceforge.net/down…ne-bin-zip.php a la misma carpeta donde esta iPhuc.exe

6.- Ejecuta iPhuc.exe

7.- Conecta tu iPod

8.- En iPhuc escribe “getfile /dev/rdisk0s1 rdisk0s1 314572800“, esto puede tardar un rato, es un archivo de 300Mb

9.- haz una copia de seguridad de rdisk0s1 de lo que acabas de descargar.

10.- Ahora necesitas algún editor hexadecimal. La aplicación que yo uso es HxD (http://www.mh-nexus.de/hxd/). Abre rdisk0s1 con tu editor hexadecimal.

11.- Busca el string ASCII “noexec” en el archivo. El segundo hit should look like the /etc/fstab file: /dev/disk0s1 / hfs ro 0 1 /dev/disk0s2 /private/var hfs rw,noexec 0 2

Cuidado porque los editores hexadecimales mostrarán “.” o semejante en lugar del carácter. Esta serie de caracteres se encuentran habitualmente entre 0xF8F9000-0xF8F9045. Deben tener los siguientes códigos de caracteres:

2F 64 65 76 2F 64 69 73 6B 30 73 31 20 2F 20 68 66 73 20 72 6F 20 30 20
31 0A 2F 64 65 76 2F 64 69 73 6B 30 73 32 20 2F 70 72 69 76 61 74 65 2F
76 61 72 20 68 66 73 20 72 77 2C 6E 6F 65 78 65 63 20 30 20 32 0A

(¡asegúrate de que buscas en modo hexadecimal!)

12.- Cambia esto a /dev/disk0s1 / hfs rw 0 1 /dev/disk0s2 /private/var hfs rw 0 2

con saltos de línea al final de la cadena de texto para que tengan exactamente el mismo tamaño que el antiguo /etc/fstab. La nueva serie de caracteres debe ser la siguiente:

2F 64 65 76 2F 64 69 73 6B 30 73 31 20 2F 20 68 66 73 20 72 77 20 30 20
31 0A 2F 64 65 76 2F 64 69 73 6B 30 73 32 20 2F 70 72 69 76 61 74 65 2F
76 61 72 20 68 66 73 20 72 77 20 30 20 32 0A 0A 0A 0A 0A 0A 0A 0A

13.- Graba los cambios. Estoy asumiendo que has reemplazado el archivo rdisk0s1 de tu disco duro con la versión modificada. Como prueba de seguridad asegúrate de que el tamaño del archivo modificado y el de la copia de seguridad es exactamente el mismo.

14.- Carga la imagen rdisk0s1 en el iPod. en iPhuc, escribe lo siguiente “putfile rdisk0s1 /dev/rdisk0s1″.

15.- Sal de iPhuc y reinicia tu iPod.

16.- Abre iPhuc de nuevo y conecta tu recien reiniciado iPod. Escribe “getfile /etc/fstab”. Esto descargará fstab al directorio de iPhuc. Abrelo con tu editor de texto favorito y confirma los cambios que hemos hecho are still there. If they are, congratulations.

Has desbloqueado tu iPod, más o menos.

17.- Ahora necesitamos instalar ssh y sus herramientas asociadas. Esto es terreno conocido pero, por desgracia, todo está diseñado para Mac. Tenemos que hacer un esfuerzo aquí. Descarga http://iphone.natetrue.com/dropbearkey.exe. También necesitarás cygwin1.dll de http://www.dll-files.com/dllindex/dl….shtml?cygwin1.

18.- Abre una ventana de comandos CMD y haz lo siguiente:

dropbearkey -t rsa -f dropbearrsahostkey
dropbearkey -t dss -f dropbeardsshostkey

Deberías obtener dos archivos en ese directorio, dropbearrsahostkey y dropbeardsshostkey. Cópialos o muévelos al directorio de tu iPhuc.

19.- Descarga y extrae http://iphone.natetrue.com/BSD_Base-2.0.tar.gz en el directorio de tu iPhuc.

20.- Descarga y extrae http://www.abigato.com/iphone-ssh-kit-vr1.tar.bz2 el el directorio de tu iPhuc. Asegúrate de que dropbear, fd6, au.asn.ucc.matt.dropbear.plist, glob6, goto, osh y sh6 están en el mismo directorio que iPhuc.exe, si no, muévelos al mismo.

21.- Abre la aplicación iPhuc y escribe “mkdir /etc/dropbear”,

22.- “cd /etc/dropbear”.

LOS DIRECTORIOS SON: /etc/dropbear/dropbearrsahostkey, /etc/dropbear/dropbeardsshostkey, /bin/chmod, /bin/sh y /usr/bin/dropbear

23.- “putfile dropbearrsahost_key”

24.- “putfile dropbeardsshost_key”

25.- “cd /bin”

26.- “putfile chmod”

27.- Rename sh6 in your iPhuc directory to sh, then “putfile sh” in iPhuc.

28.- “cd /usr/bin”

29.- “putfile dropbear”

30.- Asegurate de que /etc/dropbear/dropbearrsahostkey, /etc/dropbear/dropbeardsshostkey, /bin/chmod, /bin/sh y /usr/bin/dropbear existan en tu iPod con iPhuc.

31.- “cd /usr/sbin”

32.- “getfile update”

33.- In Windows Explorer, rename “update”, which you just downloaded, to “update.orig”.

34.- Renombra “chmod” in the iPhuc folder to “update”.

35.- En iPhuc, “putfile update”, estas reemplazando “/usr/sbin/update” con chmod.

36.- “cd /System/Library/LaunchDaemons/”

37.- “getfile com.apple.update.plist”

38.- Abre com.apple.update.plist en un editor de texto.

Justo después de donde dice: “/usr/sbin/update” añade:

<string>555</string>
<string>/bin/chmod</string>
<string>/bin/sh</string>
<string>/usr/bin/dropbear</string>

39.- Guarda el archivo. Sube el modificado con “putfile com.apple.update.plist”

40.- también, “putfile au.asn.ucc.matt.dropbear.plist”

41.- Reinicia el iPod dos veces. El primer reinicio lo requiere los permisos. El seundo inicia el servidor SSH (since proper permissions are now set). Cierra iPhuc.

42.- Teóricamente, SSH debería funcionar ahora. Enceuntra la IP de tu iPod en las preferencias wireless del iPod.

43.- Intenta conectarte por ssh cn Putty (http://www.chiark.greenend.org.uk/~s…/download.html). Nombre de usuario “root”, contraseña “alpine”.

Vale, ahora necesitamos ejecutar sftp, hacer algo de limpieza y entonces podremos instalar Installer.app, descarga WinSCP (http://winscp.net/download/winscp404setup.exe)

44.- Descarga http://apps.iphonexe.com/24940.zip. Necesitarás de estos archivos: “/libexec/sftp-server”, “/usr/bin/scp” y “/usr/lib/libarmfp.dylib”. Extraelos al directorio de tu iPhuc.

45.- Mediante la funcionalidad putfile de iPhuc, envía sftp-server a /usr/libexec/, envía scp a /usr/bin/ y envía libarmfp.dylib a /usr/lib/.

46.- ¿Recuerdas el directorio BSD_Base que extrajiste? Necesitamos sacarle algunos comandos. Necesitarás /bin/ls, /bin/mv, /bin/pwd, y /bin/csh. Cópialos al directorio de iPhuc.

47.- Escribe en iPhuc:

cd /bin
putfile ls
putfile mv
putfile pwd
putfile csh

48.- Entra mediante SSH en el iPod. Necesitamos cambiar los permisos de usuario a todos los ficheros para que sean ejecutables.

49.- Escibe en SSH lo siguiente: “/bin/chmod 555 /bin/ls”

50.- “/bin/chmod 555 /bin/mv”

51.- “/bin/chmod 555 /bin/pwd”

52.- “/bin/chmod 555 /bin/csh”

53.- “/bin/chmod 555 /usr/bin/scp”

54.- “/bin/chmod 555 /usr/libexec/sftp-server”

En teoría sftp debería funcionar ahora.

55.- Sube “glob6″ a “/bin” con iPhuc y en SSH escribe “/bin/chmod 555 /bin/glob6″

56.- Escribe “/bin/csh” en SSH. Esto hará que no tengas que escribir la ruta completa en futuras ocasiones.

57.- En SSH escribe “cd /var/root”

58.- Escribe “ls”. Debes de tener los directorios “Library”, “Mediaold”, y “Media”.

59.- Escribre en ssh “mv Media Media_sym”

60.- En SSH “mv Mediaold Media”

61.- Reinicia tu ipod y revisa tu iPod en iTunes

Instalando AppTap

62.- Descarga e instala 7-zip. Necesitamos para abrir el archivo Installer.app

63.- Descarga el Windows installe para Installer.app en http://www.nullriver.com/~adam/AppTappInstaller.exe

64.- Usa 7-zip para abrir AppTappInstaller.ex y extraer la carpeta de Installer.app de él.

65.- Usa SFTP para subir Installer.app en “/Applications” en tu iPod.

66.- En SSH, escribe “/bin/chmod -Rf +x /Applications/“

67.- Desliza para desbloquear tu iPod, en el escribe en SSH /Applications/Installer.app/Installer y pulsa enter para lanzar el Instalador.

68.- Despues de que AppTapp se abra, presiona Control + C en SSH para cerrarlo.

69.- Abre Safari en el iPod y navega a http://conceitedsoftware.com/iphone/beta. por favor asegurate de que cuando hagas esto la imagen TIFF hackeada no esta cargada. Si empeiza a cargar, hit the X.

70.- Presiona “Yes” para añadir el Instalador.

71.- Vuelve al SSH, escribe /Applications/Installer.app/Installer y pulsa enter para lanzar de nuevo el Installer.

72.- Instala el paquete “Community Sources”.

73.- Instala “Trip1PogoStick” localizado debajo de “System” para activar el deslizado y las aplicaciones.

74.- Reinicia el iPod. Debería estar terminado.
Fin