Caso Hispahack (3): Absolución de presuntos hackers. Dictamen del perito de la defensa

28-05-1999

Dictamen del périto de la defensa

PFG, Ingeniero de Telecomunicaciones, Doctor en Informática, Profesor Titular de Escuela Universitaria, y desarrollando mi trabajo de investigación sobre temas de seguridad, emito el siguiente dictamen a petición de la defensa.

I.- Consideraciones previas

1.- La seguridad del sistema operativo UNIX

1.1 Un sistema operativo puede estar pensado para el uso individual o para el uso de un colectivo de personas.

1.2 El sistema operativo UNIX, por su naturaleza, es un sistema operativo multi-usuario. Esto significa que múltiples usuarios pueden compartir recursos de un ordenador: ficheros, aplicaciones, etc.

1.3 De todas maneras, debe poder discriminarse qué usuarios tienen derecho a acceder al sistema y sobre qué recursos del mismo.

1.4 La manera de realizarlo es a través de la interrogación al usuario de un identificador personal (login) y una palabra de paso (password)

1.5 Cualquier acceso a la máquina, tanto si es de forma local (en frente del propio ordenador) como si es de forma remota (utilizando las redes de comunicaciones), implica que el usuario se ha de identificar previamente a través de su login y password.

1.6 El sistema contiene un fichero que le permite verificar, en base al login y password, si el usuario que intenta acceder al sistema está autorizado o no: es el conocido como fichero de passwords.

1.7 El nombre de fichero de passwords conduce a la confusión, dado que puede parecer que contiene los passwords de los usuarios del sistema; en realidad no es así.

1.8 El fichero de passwords sólo contiene una información cifrada en relación al login y el password.

1.9 Cuando el usuario introduce su login y password lo que hace el sistema operativo es repetir la operación de cifrado con estos datos y confrontar si el resultado de este cifrado coincide con el contenido en el fichero de passwords.

1.10 Por tanto, de los puntos 1.7-1.8-1.9, se deriva que de un fichero de passwords no pueden extraerse passwords de los usuarios, porque de hecho no están.

1.11 Es más, ni tan siquiera el administrador del sistema (que realiza operaciones de altas de usuarios, bajas de usuarios, concede derechos de accesos a recursos, etc.) puede, ni debe, llegar a conocer el password personal de ningún usuario particular.

1.12 Por su naturaleza, el fichero de passwords debe ser accesible a todos los usuarios del sistema, pues este acceso es paso previo necesario para acceder al mismo.

1.13 Esta característica, 1-12, probablemente no deseada, es plenamente conocida por todos los administradores de sistemas UNIX.

1.14 De los puntos anteriores, 1.12-1.13, se deriva que la seguridad del sistema no debe residir en la confidencialidad del fichero de passwords.

1.15 A pesar de lo dicho en los puntos 1.10-1.11, existe un posible ataque por fuerza bruta: probar para un login determinado los posibles passwords que pudiera haber escogido el usuario asociado a ese login.

1.16 Por lo dicho en 1.14-1.15, la seguridad del sistema reside en que los usuarios escojan passwords robustos, es decir, que no sean fáciles de "adivinar".

1.17 Es tarea del administrador del sistema informar y asesorar a sus usuarios sobre el tipo de password que ha de ser escogido, y también vigilar, realizando él mismo ataques por fuerza bruta, para controlar que sus usuarios, a pesar de sus recomendaciones, no hayan escogido passwords débiles.

1.18 Asimismo, es tarea del administrador hacer que de forma automatizada, el sistema obligue a los usuarios a cambiar de password periódicamente.

1.19 Una vez introducido el login y password correcto, el sistema de forma automatizada, y en base a la configuración introducida por el administrador del sistema, permite al usuario acceder a los recursos a los que tiene derechos (aplicaciones comunes, sus ficheros personales, etc.)

1.20 Inicialmente el sistema basado en login y password, permite al administrador imputar acciones particulares a usuarios particulares.

1.21 Cada usuario dispone de un login, que puede ser públicamente conocido, y de un password que sólo debe ser conocido por él (véase 1.10 y 1.11).

1.22 Un sistema bien configurado registra las operaciones relevantes que realizan los usuarios en un fichero que recibe el nombre de fichero de log.

1.23 Estos ficheros de log son de utilidad para el administrador para rastrear funcionamientos incorrectos del sistema, y acciones incorrectas realizadas por parte de los usuarios, permitiéndole corregir estas situaciones.

1.24 Los ficheros de log son ficheros de texto ordinarios, y que por tanto pueden ser manipulados por parte del administrador sin ningún problema.

1.25 De 1.24 se deriva que, a priori, no debiera considerarse la información contenida en un fichero de este tipo, como información de veracidad incuestionable.

1.26 A pesar de lo dicho en 1.20-1.21-1.22, si múltiples usuarios comparten un login y password, no hay manera de discriminar cuál de ellos ha realizado las operaciones que puedan quedar registradas en el fichero de log.

2.- Las conexiones en Internet

2.1 Para poder intercambiar información entre ordenadores a través de la red Internet, cada ordenador debe estar identificado con lo que se conoce como una dirección de red.

2.2 La dirección de red que utiliza cada ordenador debe ser única, dado que en caso contrario, el sistema no funcionaría correctamente.

2.3 Para no obligar a los usuarios a recordar la dirección de red del ordenador con el que desean dialogar remotamente, existe una segunda manera que permite referenciar los ordenadores que se denomina nombre de dominio (o nombre simbólico).

2.4 Existe una aplicación telemática que se encarga de realizar la traducción de un nombre de dominio a su correspondiente dirección de red.

2.5 A priori, puede parecer que la dirección de red identifica biunívocamente el ordenador, y por ende podría ser que también al usuario, que ha realizado una conexión remota.

2.6 Desafortunadamente, estas direcciones de red son manipulables por parte de los usuarios, de tal forma que un usuario puede configurar su ordenador con una dirección de red que realmente no le corresponde.

3.- La realización de peritajes telemáticos

3.1. Para realizar cualquier peritaje es fundamental disponer de información, e información fiable, sobre los hechos acaecidos.

3.2 Por desgracia, en el caso de sucesos telemáticos, la información de la que se puede disponer en la mayoría de los casos es escasa, o por su naturaleza es fácilmente manipulable (véanse 1.24 y 2.6).

3.3 Sorprende que se encargue el peritaje de la información contenida en el material incautado a una de las partes afectadas en el procedimiento (la parte denunciante): el E de la UPC.

3.4 No se duda de la competencia del personal que lo integra, ni tan siquiera que en este caso hayan actuado maliciosamente, pero repetimos que sorprende que sean denunciantes y peritos en el procedimiento seguido.

3.5 Destacamos de todas formas lo recogido en el folio 14 del procedimiento, manifestado por el propio E: "No es por tanto responsabilidad de E la de localizar a los atacantes, sino la de conocer sus métodos".

3.6 De todas formas, queremos reiterar y recalcar que no se pone en duda que toda la información que contiene el procedimiento no ha sido manipulada por los peritos y técnicos que han intervenido en la elaboración de los correspondientes informes.

3.7 No es así en el caso de la información concreta que contienen los ficheros analizados que podría haber sido manipulada por parte de los hackers que hubieran accedido a los sistemas.

4.- El hacking "blanco"

4.1 Definimos el hacking blanco como aquellas acciones realizadas por usuarios no autorizados, pero sin perseguir fines destructivos.

4.2 Encajan en la definición anterior, 4.1, los hackers que acceden sin autorización a sistemas remotos con el objetivo de conseguir tiempo de ejecución del ordenador, ficheros de passwords, etc, pero que no realizan, ni intencionada ni accidentalmente, la manipulación de información que no les pertenece. Es decir, no borran información de usuarios autorizados, no revelan información que debe permanecer confidencial, etc.

4.3 En ocasiones será difícil discriminar donde empiezan y donde acaban las acciones inocuas y las nocivas; la frontera no será siempre clara.

4.4 Parece exagerado "criminalizar" a un grupo de jóvenes que sólo persiguen aprender; el deseo de aprender, para alguien que procede del mundo universitario, siempre es loable.

4.5 De hecho no sólo aprenden los hackers, sino que indirectamente los administradores de sistemas también salen beneficiados.

4.6 Los "agujeros" de seguridad que detectan los hackers sirven para que los administradores mejoren la seguridad global de sus sistemas.

4.7 El punto 4.6 puede no parecer relevante, pero si pensamos que estos agujeros pueden ser utilizados para realizar acciones realmente maliciosas, que alguien las ponga de manifiesto es de gran utilidad.

4.8 También es cierto que sería preferible que los hackers informaran directamente a los administradores, y que estos no tuvieran que enterarse una vez producido el ataque y por otras vías.

4.9 No obstante, el E de la UPC, puede dar buena cuenta de que mucha de la información que manejan, y que les permite dar asistencia en relación a la seguridad de sistemas telemáticos, la han obtenido después de que un hacker realizara acciones no autorizadas en otros sistemas telemáticos.

II.- Sobre los hechos y daños descritos en los informes técnicos y periciales

---

5.- Hechos y daños en general

5.1 Las mayoría de los hechos descritos en los informes periciales y técnicos que se encuentran en el procedimiento no se refieren a la UPC y ni tan siquiera parecen relevantes para el procedimiento seguido en esta causa.

5.2 Siendo la acusación la de un delito de daños contra los intereses de la UPC, parece que deberíamos centrarnos en la información relacionada con ésta.

5.3 A pesar del punto 5.2, empezaremos recogiendo algunas de las informaciones extraídas del procedimiento.

5.4 Según consta en los folios 5 y 7 del procedimiento, la Guardia Civil manifiesta que un grupo de hackers han realizado las siguientes acciones:

5.4.1 Acceso no autorizado al ordenador del Congreso de los Diputados de Madrid.

5.4.2 Acceso no autorizado a los ordenadores de un proveedor de servicios de Internet de Girona, además de sustracción y difusión de datos personales y palabras de paso de 2500 usuarios del mismo (ver también folios 301 y 302).

5.4.3 Acceso no autorizado y daños en los sistemas informáticos de la UO (ver también folio 532, en el que además se añade que también acceden a ordenadores de la UB).

5.4.4 Intento de acceso no autorizado a ordenadores de la NASA.

5.5 En los ordenadores del Sr. JFS se han encontrado (ver folio 531) ficheros de passwords, utilidades de "pirateo informático", ficheros que contienen datos (ficheros de passwords) de la UO y de la UB, procedentes de sniffers. No se indica ninguna información relacionada con la UPC.

5.6 Según el peritaje realizado por el E (ver folio 531) el Sr. JFS ha descifrado claves de usuario (aproximadamente 414); vista la explicación realizada en 1.7 a 1.11, se entiende que la anterior afirmación es una licencia expresiva del autor del peritaje.

6.- Hechos y daños relativos a la UPC

6.1 El sistema informático de la UPC sufrió una entrada ilegal por usuarios no autorizados en 16 ordenadores servidores de la UPC, provocando una serie de daños en los mismos (ver folio 3)

6.2 La entrada ilegal (sic) se produce el 11 de septiembre de 1997 a las 4:16 horas a través de Internet, desde un ordenador ubicado en la UO denominado proy6.etsiig.uniovi.es.

6.3 Una vez realizada la entrada los atacantes:

6.3.1 Obtienen privilegios de los responsables técnicos de los 16 ordenadores servidores afectados de la UPC.

6.3.2 Suplantan su personalidad.

6.3.3 Capturan datos personales de usuarios como sus palabras de paso (passwords), a través de un programa informático denominado "sniffer" o "rastreador".

6.3.4 Se conectan a un ordenador, a través de Internet, denominado ftp.laredcafe.com ubicado en el Bar LRCC de PM.

6.3.5 Usan para ello el nombre de usuario (login) Hispahack y la palabra de paso (password) hhpax18.

6.3.6 La información obtenida en 6.3.3 se deposita en el directorio o apartado jfs del ordenador de 6.3.4

6.4 Según consta en la diligencia de exposición de hechos (folio 4):

6.4.1 El acceso ilegal ha afectado a todos los usuarios del sistema informático de la UPC.

6.4.2 Han debido realizarse numerosos ajustes de seguridad desde su conocimiento.

6.4.3 El impacto económico o daños ocasionados pueden estimarse cercano a los 2 millones de pesetas.

III.- Sobre la autoría de los hechos

7.1 Jafasa "miembro de un grupo de hackers" (sic) utiliza el alias jfs en un artículo publicado en Internet, e indica la dirección de correo jafasa@hotmail.com (ver folio 6).

7.2 El Sr. ECE declara (folio 190) :

7.2.1 Que accede al ordenador ftp.laredcafe.com de PM, con el nombre de usuario !HISPAHACK creyendo que su clave era lerele.

7.2.2 Que contaba con un directorio de uso personal de nombre Stk

7.2.3 Que la cuenta se la dio alguien de !hispahack.

7.2.4 Entre otros nombres de directorio recuerda el directorio Jfs

7.3 Se han realizado acciones no autorizadas (folios 242 y 243) en una máquina de O desde los ordenadores que tiene por direcciones de red 194.224.182.113 y 195.5.73.45, con su correspondientes nombres de dominio info63.jet.es y id-45.arrakis.es, respectivamente.

7.4 El Sr. JBC "cree" (ver folio 301) que en base a un diálogo por Internet, con alguien que utiliza como apodo Stk, miembros del grupo !HISPAHACK participaron en el ataque descrito en 5.4.2.

7.5 El Sr. ECE declara (folio 378) que Jfs accede al ordenador ftp.laredcafe.com de Palma de Mallorca, con el nombre de usuario (login) !HISPAHACK.

7.6 El Sr. JFS declara (ver folio 385) que utiliza el apodo JFS.

7.7 El Sr. BVV declara (ver folio 440) que a petición de un usuario que utiliza como apodo Cure da de alta un usuario en el ordenador ftp.laredcafe.com con nombre de usuario (login) HISPAHACK.

7.8 Según el peritaje elaborado por el E (ver folio 531) un usuario que utiliza como nombre de usuario (login) thelobo:

7.8.1 Accede a la máquina ftp.laredcafe.com desde la consola (es decir, de forma local, y no remotamente).

7.8.2 Conoce la existencia y el contenido de la cuenta hispahack.

7.8.3 Además (ver folio 536) accede a datos concretos: el fichero SUN01.TXT de la mencionada cuenta de usuario.

7.9 Del análisis de la cinta de datos incautada en el procedimiento (ver folio 532) se deriva que el hacker que ha intervenido en la acciones maliciosas utiliza el login rewt y distintos passwords.

IV.- Conclusiones

8.- Sobre los hechos y los daños

8.1 Los hechos relativos a la entrada en los servidores de la UPC encajan dentro de la definición de hacking blanco descrito en el apartado 4.

8.2 No se observa la destrucción de ningún tipo de información y por lo tanto no hay daños en este sentido.

8.3 La sustracción de ficheros de passwords no supone, o no debería suponer, ningún gran desastre (véanse 1.10 y 1.14). Pero además:

8.3.1 Los passwords deben ser cambiados periódicamente (ver punto 1.18).

8.3.2 Notificar de forma masiva a los usuarios que deben cambiar de password consiste, sencillamente, en enviar un correo electrónico a un grupo de usuarios.

8.4 La reinstalación del sistema operativo parece que queda demostrado que era una necesidad para eliminar fugas de seguridad que presentaba el sistema (ver 4.6).

8.5 De lo descrito en 5.5 lo único que se puede concluir es que el Sr. JFS es un entusiasta del mundo de la seguridad telemática (ver a propósito 4.4).

9.- Sobre la autoría de los hechos

9.1 Eran múltiples los usuarios que podían acceder a la información contenida en la cuenta HISPAHACK del ordenador ftp.laredcafe.com (véanse 7.2, 7.5 y 7.8)

9.2 De 9.1 se deriva que cualquier usuario distinto del Sr. JFS pudo haber depositado la información en ese ordenador (según se describe en el punto 6.3)

9.3 De la información de ficheros de passwords encontrada en el ordenador del Sr. JFS sólo se deriva que la obtuvo del algún ordenador, que podría ser el que tiene por nombre ftp.laredcafe.com o no, pero no que fuera él quien la obtuviera de las fuentes originarias.

9.4 Todos los demás datos no apuntan a que el Sr. JFS haya realizado ninguna de las entradas en ordenadores ajenos descritas en los apartados 5.4 y 6.3.

Lo que hago constar, según mi leal saber y entender, en Barcelona, a veintiséis de mayo de mil novecientos noventa y nueve.