Anatomía de una intrusión

Miguel Sánchez López
Depto. de Informática de Sistemas y Computadores, Universidad Politécnica de Valencia

<misan@upvnet.upv.es>

Resumen: *este artículo presenta el detalle de cómo la intrusión en el ordenador personal de mi despacho conduce a una cadena de acontecimientos, pasando por el estudio de cómo se llegó a producir (y que traerá inesperados resultados), hasta llegar a contactar con los intrusos responsables y, finalmente, con las autoridades.*

Palabras clave: *comunicaciones seguras, intrusión, política de seguridad, redes de computadores, seguridad de la información, vulnerabilidades.*

1. El entorno del incidente

El Depto. de Informática de Sistemas y Computadores (DISCA, <http://www.disca.upv.es>) es uno de los mayores departamentos de la Universidad Politécnica de Valencia (UPV, <http://www. upv.es>), agrupando a casi cien profesores, además de personal de administración y técnicos de laboratorio.

La red de la UPV es una de las mayores redes de las universidades españolas, reuniendo a más de 24.000 computadores y siendo Microsoft Windows en sus diferentes variedades el sistema operativo más utilizado, seguido de diferentes distribuciones de Linux (Debian, SuSE, Fedora, Mandrake) y diferentes sistemas Unix y también ordenadores Apple (OS9 y OSX).

La estructura de red ha ido evolucionando desde una única red Ethernet a 10 Mbps hacia el empleo masivo de *subnetting*, pero aún quedan segmentos de la red con miles de ordenadores en el mismo dominio de difusión. La interconexión entre las redes de los edificios y la red dorsal se produce a 100Mbps o 1Gbps.

Respecto a la administración de los ordenadores personales ésta depende de la ubicación y propósito de los ordenadores. El Área de Sistemas de Información y Comunicaciones (ASIC) mantiene muchos de los sistemas empleados por el personal administración, aunque en algunas secciones pueden disponer también de personal propio.

En el DISCA, siendo un departamento de Informática, los servicios centrales del departamento, como servidor de correo, colas de impresión y servidor de base de datos y de web son mantenidos por los técnicos de laboratorio con alguna colaboración ocasional de algún profesor, mientras que los ordenadores personales de cada profesor son atendidos o bien por el mismo profesor o bien por alguno de los técnicos del departamento sin seguir una regla fija. El software que cada profesor utiliza depende de sus preferencias personales existiendo total libertad en la elección.

2. El círculo de confianza

Mi entorno de trabajo ha ido cambiando con los años, haciendo un recorrido desde el MS-DOS 3.0, pasando por Windows 3.1, 3.11, 95 y 98, hasta llegar al Windows 2000. Tras una estancia en el extranjero y un cambio de ordenador se efectúa la transición a Linux, primero con RedHat y luego con SuSE Linux (ya que éste último estaba siendo instalado en algunos laboratorios docentes y también por parte de otros compañeros de trabajo).

A finales de los años noventa el departamento DISCA moderniza su servidor de correo y adquiere un paquete de la empresa SuSE, <http://www.linuxplanet.com/linuxplanet/reviews/4122/1/>, para disponer de un nuevo servidor que emplee conexiones seguras (*Secure Socket Layer*, SSL) para la recuperación del correo. Con anterioridad el tráfico y las contraseñas viajaban sin cifrar y parecía que era conveniente actualizar la infraestructura a las nuevas condiciones, teniendo en cuenta que en aquellos momentos la red del DISCA estaba en el mismo dominio de difusión que casi todos los ordenadores de la UPV, incluidos los de los laboratorios docentes, y apenas se empleaban conmutadores, lo que podría propiciar el acceso no autorizado al tráfico de los servidores.

El sistema funcionó bien durante varios años, dando algún problema sólo cuando alguien excedía su cuota de disco. Funcionó tan bien que la dinámica de actualizar el equipo para aplicar todos los parches de seguridad se fue relajando y al no producirse problemas tampoco nadie se preguntó nada a ese respecto. Como muchos usuarios, empleo la aplicación *ssh* para conectarme a los diferentes sistemas que utilizo, también para conectarme al ordenador de mi domicilio cuando necesito transferir o consultar algún archivo ubicado allí. Durante años utilicé las mismas contraseñas en aquellos equipos que consideraba 'fiables'. Así la cuenta en mi ordenador personal y en algunos otros ordenadores del departamento tenía la misma contraseña. Sólo en aquellos casos en los que el sistema era considerado sensible empleaba diferente contraseña.

3. Chequeos periódicos

Puesto que incluso la mejor seguridad puede fallar en algunos casos, suele resultar conveniente que los sistemas realicen algún tipo de registro de los accesos y operaciones importantes. Así luego el usuario puede comprobar que todo marcha bien o, en caso de algún problema quizá se pueda detectar y tomar la medidas oportunas para corregirlo.

El 30 de abril de 2004, al efectuar una comprobación rutinaria de los últimos accesos remotos (sesiones remotas con *ssh*) a mi ordenador personal, observé una dirección IP desconocida que me produce inmediatamente esa sensación en el estómago de que hay algo que no marcha bien. Se trata de un acceso efectuado el día 5 de Abril y la dirección IP resulta pertenecer a un servidor belga, (rootshell.be), <http://www. rootshell.be>, del que nunca había oído hablar antes. Tras unos minutos de consulta en su web queda claro que se trata de un servidor que ofrece accesos *ssh* gratuitos a sus usuarios. Quien haya accedido a mi ordenador lo ha hecho a través de este servidor para ocultar su identidad.

4. Pánico

Bien, ya ha sucedido, alguien ha accedido a mi ordenador sin autorización, dónde residen mi correo personal y los documentos de más diez años de trabajo (sólo yo tengo una cuenta en su equipo y soy el único que conoce -- o eso creía --la contraseña de mi usuario). Entonces me planteo las tres cuestiones que considero fundamentales:

- ¿Quién ha sido?
- ¿Cómo han conseguido entrar?
- ¿Por qué lo han hecho?

No obstante, antes de buscar respuestas y para evitar futuros accesos no autorizados se impone cambiar la contraseña. Sin embargo, dado que esa contraseña también la uso para acceder a otros equipos conviene comprobar si también allí se efectuaron accesos no autorizados.

Por otra parte, aún sin haber notado nada extraño previamente, tampoco conviene descartar la idea de que los intrusos podrían haber instalado algo en el ordenador para monitorizar cualquier operación del usuario (por ejemplo un programa de registro del teclado o *keylogger*). Además, siendo miembro de una comunidad conviene alertar a los técnicos del laboratorio y a los demás compañeros de trabajo para que comprueben si también ellos han sido afectados.

Una vez alertado el resto del departamento continúo con las indagaciones y descubro que, además de mi ordenador personal de la oficina, también un ordenador personal de mi domicilio, conectado a Internet con una línea ADSL, ha sido accedido desde la IP belga y desde otra dirección desconocida.

Con esta segunda dirección hay menos suerte y no tiene un nombre DNS asociado que me resulte significativo. Pertenece a un grupo de direcciones de la empresa Telefónica Transmisión de Datos, que asigna direcciones a sus clientes de ADSL.

Tras comprobar otras cuentas en los servidores del laboratorio de Redes de Computadores, observo que los intrusos también han estado allí. Y lo que es peor, muchos de los accesos entre todas estas cuentas convierten en sospechosos a otros muchos de los accesos que se hubieran originado en esos ordenadores hacia cualquiera de las otras cuentas en los demás ordenadores afectados. Una concienzuda comprobación de horas y fechas confirma que en algunos casos los intrusos entran en una cuenta y saltan de ésa a otras de mi mismo usuario, con lo que evitan que esos accesos me resulten sospechosos ya que provienen de máquinas en las que tengo cuenta y que utilizo ocasionalmente.

5. Otros afectados

Hasta ahora he verificado sólo mis cuentas en diversos servidores docentes y en tres de ellos han aparecido accesos de los intrusos, pero en uno de ellos descubro un acceso desde el servidor de correo del DISCA. Este acceso es claramente anómalo ya que no corresponde con el uso normal que hago de ese servidor.

Esto me indica que ese acceso tiene que ser de los intrusos. Como no dispongo de permisos de administración en ese ordenador solicito al administrador del servidor de correo la lista de accesos y entonces la auténtica dimensión del problema se manifiesta: aparecen accesos de usuarios previamente inexistentes (que han tenido que ser creados, necesariamente, por los intrusos), en ocasiones desde direcciones IP desconocidas pero pertenecientes al operador de cable ONO. Claramente alguien, además del administrador del servidor de correo, ha conseguido privilegios de administración para poder crear esos usuarios.

Los técnicos del departamento analizan el disco del servidor de correo y descubren que alguien, además, ha instalado un *sniffer* que ha ido recolectando nombres de usuario, contraseñas y algunos correos electrónicos y los ha registrado en un archivo. Está claro que el servidor no puede seguir operando en estas condiciones, y el servidor es desconectado mientras se decide qué hacer.

Queda de manifiesto que lo que parecía un problema individual de un profesor tiene unas raíces más profundas y extendidas. Ahora es un problema del departamento y por extensión de la Universidad.

6. Comienza la búsqueda

En este punto sabemos que unos intrusos han accedido a varios ordenadores del departamento. En el servidor de correo han instalado un programa para capturar credenciales de usuario. En este ordenador han conseguido escalar privilegios gracias a que el equipo no había recibido los últimos parches de seguridad. En los demás equipos han intentado algunos *exploits* sin éxito ni pericia, ya que los *exploits* utilizados no se corresponden con las versiones del núcleo que esos sistemas están ejecutando. Este detalle, junto al hecho de que los intrusos no hayan borrado el registro de acceso al menos en el servidor de correo dónde si consiguieron privilegios de administrador nos sugiere que no se debe tratar de personas con mucho talento.

Tan pronto como detecto el primer acceso, detección que no es rápida en parte porque las vacaciones de Pascua están por el medio, envío un correo a <abuse@rootshell.be> indicándoles que alguien está usando esa cuenta para fines que claramente están en contra de su propia "política de uso aceptable". La colaboración del administrador de esta compañía se mostrará esencial en el esclarecimiento de estos hechos.

Como primera medida, la cuenta utilizada para el acceso no autorizado es cancelada sumariamente por el personal de rootshell.be y, tras unas palabras amables me revelan los datos que suministraron al abrir la cuenta "user Eve[1]", una cuenta de Hotmail (mail_Eve@hotmail.com) y, lo que es más importante, las direcciones IP que emplearon en las últimas conexiones, que resultan pertenecer a "La casa del alumno", un aula informática de libre acceso situada en el campus de la UPV. Aunque esos ordenadores mantienen un registro de los usuarios que los emplean, los datos del registro sugieren que los intrusos habían empleado una cuenta 'robada' y no la suya propia.
No obstante, el hecho de que con estos datos se sitúe a los intrusos dentro del campus de la UPV parece sugerir que podrían ser estudiantes, posiblemente alumnos del DISCA, aunque esto no es muy significativo ya que el DISCA imparte asignaturas en muchos de los centros de la UPV.

7. La burocracia

Desde el principio se comunicó el incidente al ASIC, <http://www.asic.upv.es>, buscando también que ellos, empleando sus herramientas y el control que tienen de la red, pudieran ayudar en el esclarecimiento de este incidente.

Lamentablemente la experiencia parece indicarles que es muy difícil y consume mucha energía descubrir estos hechos y, aunque buena voluntad no les falta, parecen considerar que lo que se podía hacer ya está hecho, los agujeros están tapados y las contraseñas cambiadas.

El director del departamento también es informado y ha alertado a todo el departamento puesto que los intrusos han tenido acceso a nuestro correo privado y, en muchos casos, eso puede haber significado acceso a información sensible, como cuentas de bancos o contraseñas de otros equipos. Por todo ello el director se ha puesto en contacto con los servicios jurídicos de la universidad para que estén informados. Sin embargo, la UPV se encuentra en pleno proceso electoral en esos momentos y no parece que este incidente tenga demasiada importancia en el gran esquema de las cosas, en especial cuando las elecciones parece que serán especialmente reñidas.

8. El MUST

Continuando con el análisis de los registros de accesos de los intrusos a mi ordenador particular aparece la dirección de rootshell.be y otra dirección desconocida. Esta segunda dirección no produce resultados en Google, pero proporciona dos entradas en Altavista. Tras una cadena de coincidencias averiguo que esa dirección IP pertenece a la dirección de la red de alumnos del centro *Mediterranean University of Science and Technology* (MUST, <http://www.must-es.com>) que es un centro adscrito a la UPV, que está ubicado en el mismo campus de la UPV y ... a pocos metros de "La casa del alumno", ¡vaya casualidad!.

Sin perder más tiempo me dirijo a ese centro y me entrevisto con su director y con el administrador de su red pero, a pesar de que les proporciono diferentes fechas y horas de los accesos de los intrusos, no consiguen determinar los posibles responsables puesto que esa dirección está compartida por una treintena de computadores de uso docente y no se dispone de registros de tráfico (aunque esto es algo que podremos mejorar).

> Lo que parecía un problema individual de un profesor tiene unas raíces más profundas y extendidas

9. Buscando a Eve

Para abrir la cuenta de rootshell.be los intrusos tuvieron que proporcionar una cuenta de correo que ellos pudieran luego leer, ya que ese requisito es necesario para completar el proceso de registro (te das de alta y tienes que usar la contraseña que te envían por correo).

Por lo tanto, la cuenta de Hotmail que los intrusos emplearon para darse de alta debería funcionar y, si funciona tenemos un canal directo para hablar con los intrusos (intencionadamente estoy evitando el término *hacker* todo el tiempo).

Los indicios apuntan a que se trata de alumnos de la UPV, puesto que los accesos se han trazado mayoritariamente a dos localizaciones conocidas: la casa del alumno y el centro MUST. La búsqueda en Google de mail_Eve @hotmail.com no proporciona resultados, Altavista sin embargo nos lleva a un foro en Hackhispano, <http://www. hackhispano. com>, donde un usuario con alias mail_Eve tiene 34 mensajes enviados sobre sus actividades e intereses en los últimos dos años, principalmente dirigidos a sembrar el caos en aulas informáticas del instituto y luego en la biblioteca de su universidad desde el anonimato de la red. Pero casualmente hay un par de preguntas, las últimas, referidas a romper por fuerza bruta *ssh* y a dónde se almacena el registro de accesos en sistemas Linux. Todo parece indicar que éste puede ser uno de los intrusos que empieza a darse cuenta de que debería de procurar no dejar huellas de sus actividades.

En los datos asociados a ese usuario en Hackhispano aparece una cuenta de correo, que parece oportunamente modificada para evitar *spam*: mail_Eve@hotmail.co (en vez de .com) y un número de usuario ICQ, <http:// www.icq.com>. En la web de ICQ se puede ver que los datos que corresponden a ese número de usuario son los de una persona de nombre "Eve Simp", de 19 años y que vive en el código postal de una población de a pocos kilómetros de Valencia. La edad parece además coincidir con la 'actividad' e 'inquietudes' de ese usuario en Hackhispano, pero eso también significa que se trata de un estudiante de primer en año en la universidad. Esto me resulta extraño pues la asignatura que imparto es de segundo curso y esto no es compatible con la edad de esta persona. Por otra parte la idea de que los intrusos podrían ser alumnos míos es tan sólo una conjetura para dar una respuesta a la posible motivación de los atacantes. En especial porque aunque han podido acceder a mis cuentas en varios ordenadores, no han podido acceder al servidor en el que tengo una web de cuestionarios on-line donde están las notas de prácticas y las notas de los exámenes. Los registros de accesos de este ordenador muestran varios intentos infructuosos.

Unas cuantas llamadas de teléfono después, a personas con el apellido "Simp" en el código postal que figuraba en la ficha de Eve en ICQ, no produce resultados. Para poder avanzar y a la vista de se puede tratar de un alumno de la UPV, procedemos a un movimiento poco convencional pero con algunas posibilidades de éxito: durante el fin de semana del 8 de mayo, ya con el servidor de correo del departamento desconectado, le envío un correo electrónico a "Eve" a su dirección mail_Eve@hotmail.com indicándole que el juego ha terminado, advirtiéndole que el incidente ha sido comunicado a las autoridades y citándolo a una reunión urgente en el DISCA el lunes.

El mensaje recibe contestación a los pocos minutos, desde una dirección de Arsys (operador de ADSL de La Rioja), donde alguien que no niega llamarse Eve me pregunta si se trata de una broma o qué. Contesto diciéndole que en absoluto es una broma y que espero que no falte a la cita el próximo lunes a primera hora. Sin embargo, nadie se presenta el lunes. Una pena ya que en ese momento todavía no conozco su identidad, pero al menos confirmo que la cuenta de Hotmail sigue activa y que alguien la comprueba regularmente.

Dos días más tarde de este intercambio de mensajes, la página datos personales del usuario mail_Eve en ICQ ya no tiene el código postal. Parece que a resultas del correo que le he enviado esa persona empieza a pensar que quizá es mejor borrar las posibles huellas (aunque supongo desconoce que ya he accedido a esa información y que su acción no hace sino verificar que el código postal allí mostrado debe ser correcto).

10. Buscando a Trudy

Durante ese mismo fin de semana en que he enviado ese mensaje a Eve, el servidor de correo del DISCA se encuentra desconectado. El jueves anterior, 6 de mayo, cuando ya se ha detectado la intrusión en ese servidor, se procede cautelarmente a modificar la contraseña del administrador y se bloquean los usuarios con privilegios de administración que han venido usando los intrusos. Así el viernes 7 de mayo, un administrador del departamento me comunica que alguien ha intentado entrar al servidor de correo, de nuevo desde rootshell.be, pero sin éxito en esta ocasión porque desconoce la nueva contraseña.

Contacto de nuevo con el administrador de rootshell.be y le informo de la situación, pidiéndole en este caso que no desactive esta otra cuenta de los intrusos sino que monitorice su acceso y me informe sus movimientos. El usuario que está intentado acceder a nuestro servidor de correo tiene el alias "userTrudy[2]" y el correo de Terra Networks mail_Trudy@terra.es

Coincidiendo con el envío del mensaje de correo, el sábado 8 de Mayo, a la cuenta de Hotmail de Eve, ese usuario accede a su cuenta en rootshell.be e intenta infructuosamente acceder al servidor de correo del DISCA (ahora desconectado). Tras lo cual, y según me informa el administrador de rootshell.be, borra de su cuenta de rootshell. be varios archivos con nombres como .known_hosts de varios usuarios, k3ys.txt y users.txt. Parece que está haciendo limpieza para eliminar cualquier posible dato relacionado con el caso, pero no sabe que esta vez me estoy enterando de lo que hace y desde dónde se está conectando también: El domingo 9 de mayo se registra un acceso a la cuenta de ese usuario desde una dirección IP del operador de cable ONO. Esa misma IP ya aparece en otras ocasiones en nuestro registro de accesos, luego posiblemente corresponda con el domicilio uno de los intrusos. Los demás accesos a la cuenta "userTrudy" de rootshell.be se producen desde el centro MUST. Así que es hora de poner en marcha un monitor de red allí puesto que los atacantes siguen considerando aquel territorio como zona segura y anónima.

11. "Pescando" en el MUST

Aunque he encontrado el máximo apoyo e interés en el centro MUST para esclarecer este enojoso asunto, al no disponer de registros de tráfico de ningún tipo y salir a Internet con una dirección IP común a todos los

ordenadores (debido al uso de un *router* NAT), los responsables del centro MUST no me han podido proporcionar información sobre qué personas pueden estar llevando a cabo esta intrusión.

En su afán por colaborar en esta búsqueda les indico cómo poner en marcha un monitor de red que registre todo el tráfico de la red de sus alumnos, para que si alguno se conectara a rootshell.be se pudiera detectar esa actividad y, aunque el contenido de la sesión aparecería cifrado, al menos se podría establecer qué ordenador, qué hora y qué persona lo hizo.

Pasan unos días antes de que el sistema dé resultado, pero el viernes 13 de mayo recibo una llamada del MUST y me dicen que tienen a nuestro hombre. Un estudiante llamado Trudy, que se encuentra realizando un proyecto para una de sus asignaturas y que tiene asignado para su uso exclusivo un ordenador del centro. Se ha registrado un acceso desde su ordenador a rootshell.be. Como el ordenador es propiedad del centro MUST, el administrador de red ha retirado ese ordenador del aula una vez Trudy se ha marchado sin sospechar nada, y ha estudiado el contenido del disco duro. Ha podido comprobar que en el pasado se han efectuado múltiples conexiones *ssh* a la cuenta "userTrudy" en rootshell.be así como a dos direcciones de ONO, una de ellas la misma desde la que el pasado domingo se efectuó una conexión a la cuenta "userTrudy" en rootshell.be.

12. Sucesos inesperados

Sabedores de que las pruebas de estos casos se desvanecen muy rápidamente y a la vista de que la UPV no parece interesada en denunciar los hechos, el grupo de delitos telemáticos de la Guardia Civil, <http://www.guardiacivil.org/telematicos/>, viaja a Valencia para tomarme la denuncia que presento a título personal[3], por los accesos ilegítimos a mis cuentas en varios ordenadores. En esa mismo viaje también toman otra denuncia de una intrusión en un ordenador de un profesor en el centro MUST.

En la visita, uno de los técnicos de la Guardia Civil nos sugiere que volvamos a comprobar la cuenta mail_Eve@hotmail.com: en esta ocasión nos llevamos una gran sorpresa, ahora hay una entrada a una asignatura de un departamento de la UPV, pero no del DISCA. Se trata de un trabajo de la asignatura de Programación, del Depto de Sistemas Informáticos y Computación (DSIC). El trabajo lo presenta un alumno de nombre Eve, aunque su primer apellido no es Simp sino Simpson. También figura su domicilio, en la población cercana a Valencia y su dirección de correo electrónico, que es ... mail_Eve@hotmail.com.

Puesto en contactos con el profesor responsable de esa asignatura, me dice que, en realidad, Eve no es alumno suyo, sino que es hermano de un alumno, pero que envió su programa al saber que se publicaría en la web de la asignatura. Ese programa lo envió en diciembre de 2003 pero el profesor no lo colgó en la web hasta mayo de 2004.

En realidad Eve estudia primer curso en la ETSIT (Escuela Técnica Superior de Ingenieros de Telecomunicación). Al contactar con el administrador del centro para comunicarle estas averiguaciones, me indica que precisamente a esa persona le acaban de amonestar por otro incidente informático de un laboratorio docente del que se le considera responsable.

El responsable de seguridad del ASIC (centro de cálculo) también es informado de estas indagaciones. Ese mismo responsable me llama por teléfono al día siguiente con nuevas y sorprendentes noticias: ha pillado a Eve en la Biblioteca de la UPV utilizando una cuenta de administrador en un equipo de la biblioteca al que había conectado un disco duro USB (*Universal Serial Bus*). En esta ocasión se ha llamado a los guardias de seguridad, que le han pedido identificación para que sirva de base para posibles medidas disciplinarias que pueda tomar la universidad contra este estudiante. Desde luego parece que Eve no tiene tiempo de aburrirse.

13. Siguiendo el hilo

Paralelamente a la investigación sobre la identidad de los intrusos se procede en el DISCA, con la colaboración de los técnicos de laboratorio, al estudio detallado de los registros de acceso del servidor de correo afectado, con el fin de situar el origen de la intrusión.

Los primeros accesos de usuarios desconocidos se producen el 23 de marzo de 2004, y mirando ligeramente hacia atrás se observa que el día 22 de marzo hay una conexión de un usuario válido pero efectuada desde un lugar altamente improbable y sospechoso: la casa del alumno. Puestos al habla con este profesor, nos confirma que él nunca ha estado en la casa del alumno y que no se ha conectado jamás por *ssh* al servidor de correo, por lo que no puede haber sido él. Sin embargo, este profesor imparte docencia en la ETSIT, concretamente una asignatura de primer curso y, además, tiene como alumno a Eve.

Bien, con estos datos parece que Eve ha robado la contraseña a este profesor. Se ha conectado por *ssh* con el servidor de correo del DISCA usando esa cuenta robada y, una vez allí, ha probado, sólo o con la ayuda de Trudy, distintos *exploits* hasta que han conseguido escalar privilegios en ese sistema.

Unos días después han descargado diversas herramientas para poder compilar el *sniffer* Ettercap. Con esta herramienta en marcha han podido capturar tráfico, tanto local del servidor como de cualquier otro equipo en la misma subred, ya que este programa permite, mediante el uso de *ARP-poisoning* y retransmisión de tráfico, capturar tráfico de cualquier ordenador en una red conmutada. Para hacer las cosas algo peor para el departamento y mejor para los intrusos, resulta que las conexiones SSL al servidor de correo, tanto POP3 como IMAP, terminan en un programa que retransmite localmente sin cifrar los datos a servidores convencionales POP3 e IMAP que no soportan SSL. Claramente es una mala elección por parte del departamento, pues en este caso permite que los intrusos puedan espiar todo el tráfico local con cualquiera de esos dos protocolos (ambos envían los nombres de usuario y las contraseñas sin cifrado alguno).

A partir de aquí los intrusos pueden obtener una lista de nombres de usuarios y contraseñas de todo el personal del departamento. Además pueden leer todo el tráfico de correo que atraviesa o se almacena en ese servidor de correo.

Todo esto ha pasado completamente sin detección y sin levantar ninguna sospecha. Los intrusos realizan varios ajustes en el *sniffer* y lo dejan capturando y almacenando los datos en un archivo. Supongo que ocasionalmente aprovechan sus visitas al campus para descargar el contenido de ese archivo, con credenciales de usuarios y mensajes de correo, a algún dispositivo de almacenamiento masivo -- ¿quizá un disco USB? -- puesto que al detectar la intrusión el archivo tenía ya más de 200 MB y sólo llevaba unos días de captura.

De ese proceso de captura de tráfico es de dónde obtienen, entre otras, mi nombre de usuario y mi contraseña que utilizaba tanto para mi computador personal como para el correo del servidor departamental. Una mala idea que confío, el lector procurará evitar.

14. Recuperando la confianza

La mayoría de personal del DISCA no pudo verificar si sus equipos de los despachos fueron accedidos a no pues no tenían activadas las características de auditoría en sus ordenadores. Las personas que sí tenían estas características activas no apreciaron intentos de acceso.

Donde sí que pude constatar intentos fallidos de acceso fue a otro ordenador de mi despacho (con distinta contraseña) que albergaba una base datos de notas así como intentos de acceso a una empresa cuyo servidor figuraba en mi .known_hosts. Si se trataba de una intrusión totalmente dirigida

a un sólo objetivo o no es algo que por el momento desconozco, pero resulta curioso no encontrar al menos intentos de acceso a otros sistemas (si bien es cierto que este extremo no lo he investigado de forma exhaustiva).

A resultas de la detección de la intrusión alerté a todo el personal del DISCA para que procedieran a asegurar todos sus equipos informáticos y cuentas bancarias que se pudieran haber visto comprometidas. Hasta la fecha no conocemos que los intrusos u otros hayan realizado actividad alguna en esa dirección.

El departamento DISCA acordó dar de baja el servidor departamental de correo y pasar a utilizar los servicios centrales de la UPV, confiando en que el ASIC velará por la confidencialidad de las comunicaciones. Por otra parte el servidor central ahora ya soporta comunicaciones cifradas con SSL.

Aproximadamente un mes después de presentar la denuncia, personal del grupo de delitos telemáticos de la Guardia Civil regresó a la UPV con una orden del juez instructor para que se les facilitaran los discos duros de los servidores comprometidos, trámite que se completó sin problemas.

Los distintos proveedores de Internet cuyas direcciones aparecía como origen de accesos no autorizados también fueron requeridos para identificar a sus clientes. También a Microsoft se le requirió información sobre mail_Eve@hotmail.com y a Terra Networks sobre el usuario mail_Trudy

Como resultado de la instrucción el juez emitió sendas órdenes de registro de los domicilios de Eve y de Trudy, identidades que imagino quedaron confirmadas con las direcciones IP de sus domicilios particulares. Cierto material informático de sus domicilios fue confiscado para ser analizado y ambos fueron conducidos a declarar ante el juez instructor.

A resultas del incidente se optó por dar de baja el servidor de correo departamental y pasar a utilizar el servidor que para idéntico propósito tiene la universidad. Es una ironía del destino que el servidor que hoy se anula se pusiera en funcionamiento porque, en su momento, el servicio central de la universidad no empleaba SSL y se consideró poco seguro. Sorprende comprobar como, unos años después esa misma elección se volvió en nuestra contra y sirvió de vehículo a una intrusión.

En cualquier caso, el servicio central de la universidad ya ofrece acceso seguro mediante SSL (tanto IMAP como POP3) o mediante interfaz de correo web (*webmail*) con HTTPS (*Hyper Text Transfer Protocol Secure*).

Algunos miembros del departamento que son usuarios de sistemas Linux han desactivado completamente el acceso basado en contraseña. Todos los miembros han cambiado sus contraseñas.

Es sorprendente observar que después del incidente la postura "*no estoy preocupado pues no tengo nada importante en el ordenador*" sigue apareciendo como una forma de justificar pobres medidas de seguridad. Aparentemente algunos usuarios parecen no conceder demasiada importancia a que alguien curiosee entre sus cosas personales y/o utilice su ordenador como vehículo para nuevas intrusiones o como almacén de contenidos ilícitos.

El incidente ha puesto de manifiesto la debilidad de nuestros sistemas, nuestra carencia de una política de seguridad (defecto que todavía no hemos subsanado, varios meses después), la facilidad con la que los usuarios acudimos a 'atajos' inseguros y lo poco que nos suele preocupar por que rara vez consideramos que podamos estar en el punto de mira de alguien.

15. Conclusiones

Las universidades disponen de algunos elementos que parecen interesar a muchos intrusos:

- Conexiones a Internet de alta velocidad.
- Miles de ordenadores interconectados, muchos de ellos vulnerables a sencillos ataques.
- Información académica, tanto exámenes como calificaciones de alumnos.

Si a esto unimos el rápido crecimiento del parque de ordenadores, la multitud de fallos de seguridad en el software y la escasa preocupación del usuario medio acerca de la seguridad de su propio ordenador, nos encontramos con un terreno fácil para que los intrusos puedan entrar y quedarse en nuestros sistemas informáticos. Algunos documentos (por ejemplo, <http://www.cert.org/archive/pdf/ecrimesummary05.pdf>) sugieren que las intrusiones detectadas son una pequeña porción del total, sin embargo este dato es difícil de confirmar porque se trata de una premisa engañosa ya que no podemos conocer el número total de intrusiones y, seguidamente, conceder que muchas de ellas no son detectadas.

Los manuales de seguridad sugieren que una buena seguridad se tiene que basar en cuatro componentes: prevención para evitar los incidentes, protección para minimizar su impacto, políticas que estimulen el uso responsable de los recursos informáticos y la persecución legal de los infractores.

Si nuestra organización no dispone de un plan sobre cómo actuar en estas circunstancias, es bastante probable que los intrusos no sean adecuadamente perseguidos y que nuestros sistemas informáticos no estén adecuadamente protegidos.

Posdata procesal

A partir de la denuncia presentada ante el Grupo de Delitos Telemáticos de la Guardia Civil en mayo de 2005, el Juez Instructor emite diversos mandamientos que ocasionan la detención de dos sospechosos, que son interrogados y quedan en libertad. Los ordenadores personales de los sospechosos son confiscados. También se extienden mandamientos a diversos proveedores de servicios Internet para dilucidar la posible vinculación de los acusados con diversas direcciones IP de esos proveedores.

En septiembre de 2005 se lleva a cabo el juicio oral de la causa penal que se sigue contra los dos sospechosos. Se les acusa de un delito "*contra la Intimidad, descubrimiento y revelación de secretos del art. 197-1 del Código Penal*".

La sentencia del Juzgado de lo Penal considera probado que los acusados efectuaron diversos accesos no autorizados a diferentes servidores de la Universidad Politécnica de Valencia así como a ordenadores personales de un profesor. Sin embargo, esta primera sentencia absuelve a los acusados al considerar que no concurre el "animus desvelandi" o divulgación de la información obtenida.

El ministerio fiscal recurre esta primera sentencia y en diciembre de 2005 la Audiencia Provincial de Valencia revoca la sentencia del Juzgado de lo Penal y condena a los acusados a sendas multas de 3.600 Euros al considerar que han vulnerado la intimidad del profesor al acceder a sus ordenadores personales sin autorización.

Notas

[1] Los nombres y las cuentas de los intrusos han sido cambiados. Otros datos se han omitido para mantener el anonimato de los intrusos en previsión de posibles problemas legales.
[2] Este nombre de usuario también es ficticio, como lo serán el resto de los datos personales asociados a los presuntos intrusos.
[3] En el momento de redactar este documento aún desconozco si los intrusos emplearon alguna de mis cuentas para cualesquiera propósitos y una vez visto que los intrusos no tienen intención de colaborar en esclarecer los hechos, decido informar a las autoridades.