HACKE

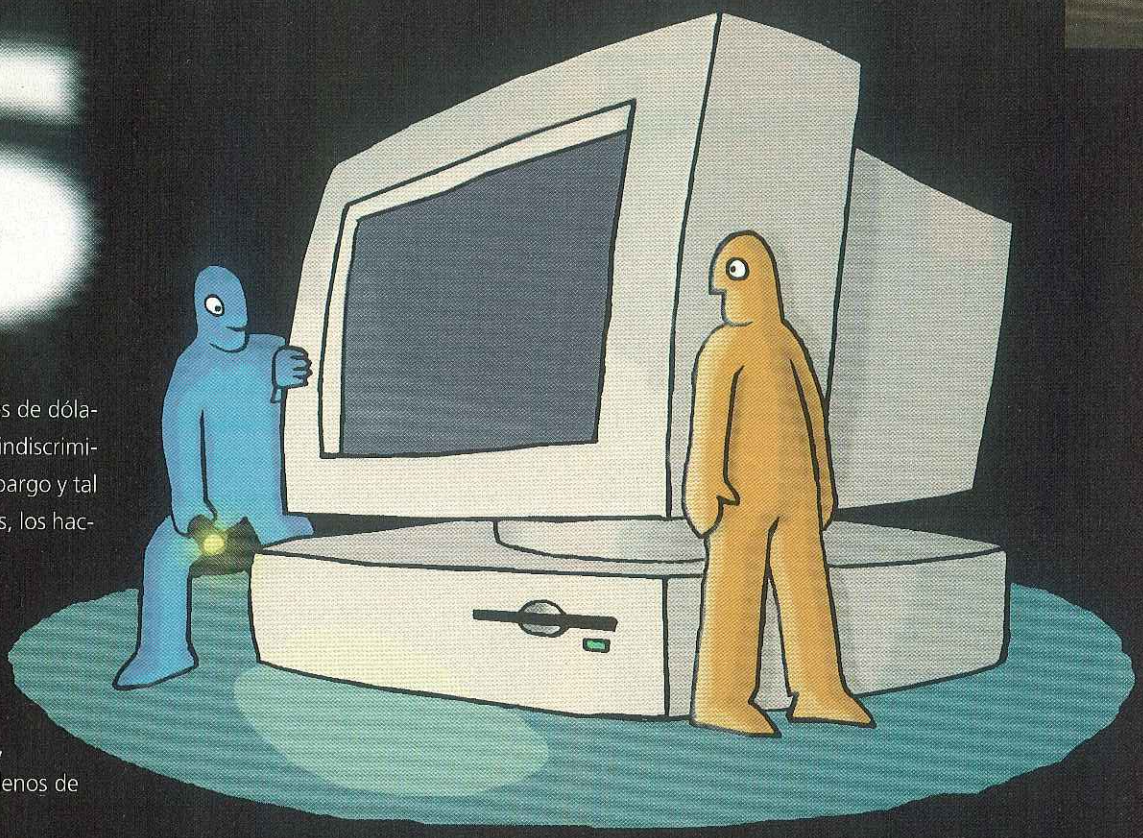
Internet es un territorio desconocido para la mayoría de los usuarios españoles, pero no para todos. Entre los internautas, existen unas personas cuyos conocimientos sobre la Red y la informática en general son superiores al del resto. Actualmente, tal vez por el caso de Islatortuga y las actuaciones de la BSA, están de moda y son perseguidos por los medios de comunicación y las fuerzas del orden público. En este reportaje vamos a intentar descubrir quiénes son y qué motivaciones tienen estos individuos, comúnmente conocidos como Hackers. Asimismo intentaremos averiguar si su persecución es justa o Injusta.

Introducción

Repasemos la situación actual: Por un lado nos encontramos con los hackers, cuya máxima pretensión (en su estado puro) es conseguir toda la información posible para divulgarla entre los demás usuarios (por lo menos en su reducido círculo de amigos). Hay que añadir que cuanto más grande sea el reto y más difícil sea conseguir esa información (independientemente del tipo o de la fuente), mayor será el aliciente para el hacker. Servidores como los del FBI, Microsoft o el gobierno (por poner unos ejemplos) son el punto de mira de muchos de estos individuos. Aunque los hackers ideales son bastante difíciles de encontrar, no hay que confundir a estas personas con piratas informáticos (que se dedican a vender información obtenida de forma ilegal, programas o CDs piratas), error que se produce comúnmente en la mayoría de medios de comunicación. Después veremos más extensamente qué son y qué es lo que hacen estas personas.

En la otra orilla se encuentra la BSA (Bussines Software Alliance), una asociación internacional promovida por los mayores fabricantes de software del mundo que pretende salvaguardar los intereses de las empresas asociadas.

R&S



Estas empresas pierden millones de dólares al año a causa del pirateo indiscriminado de sus productos. Sin embargo y tal como hemos mencionado antes, los hackers no se dedican al pirateo de software. Esto lo realizan los piratas informáticos de muy diversas formas: desde la venta ilegal de CD-ROMs, servidores warez, páginas Web o servidores FTP llenos de programas piratas.

La situación actual

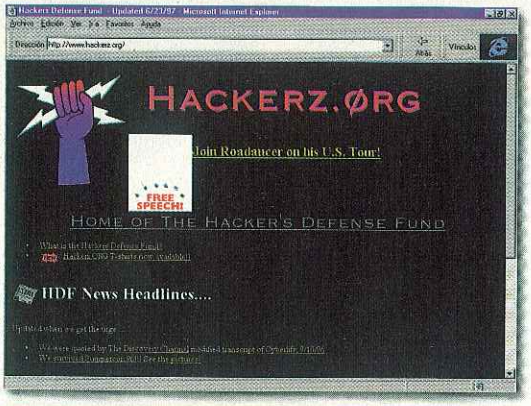
Este artículo está enfocado a descubrir un poco más acerca de estos personajes, que a menudo se mueven en las sombras de Internet. Normalmente son muy discretos, pero en ocasiones destacan y realizan acciones que repercuten sobre la inmensidad de la Red. Por ejemplo tenemos el "sonoro" caso de la caída de la página Web de Microsoft ocurrido el pasado 19 de Junio. A grandes rasgos, lo que ocurrió fue que el servidor Web de la compañía liderada por Bill Gates (uno de los Grandes Hermanos) fue atacado por un Hacker (o algo parecido) que, enviando una determinada dirección URL con su propio navegador al servidor de Microsoft, se aprovechó de un bug o fallo en el sistema operativo Windows NT 4.0 en el que se basa ese servidor. Esta instrucción, una simple dirección URL con varios parámetros, provocó serios problemas y la caída de la página Web de Microsoft, con la automática desconexión a Internet. Sin embargo Microsoft se recuperó pronto de este golpe, desarrollando rápidamente un parche que cubría este defecto. Esta acción hacker a nivel mundial contrasta con la actuación de la BSA en el caso Islatortuga (una intervención con muchas dudas por aclarar) y la continua eliminación de páginas Web con contenidos acerca del Hacking en varios de los servidores gratuitos más importantes del planeta, no sólo de España (caso de Geocities o Tripod, donde se han suprimido varias páginas españolas con estos contenidos). Así están las cosas, aunque es posible que los hackers no desaparezcan nunca (es imposible frenar la curiosidad y las ganas de aprender de algunos usuarios de Internet, que no se contentan sólo con navegar), sí es posible que el número de páginas hacker se vaya reduciendo y que cada vez sea más difícil la comunicación. Sin embargo eso sólo el tiempo lo dirá.

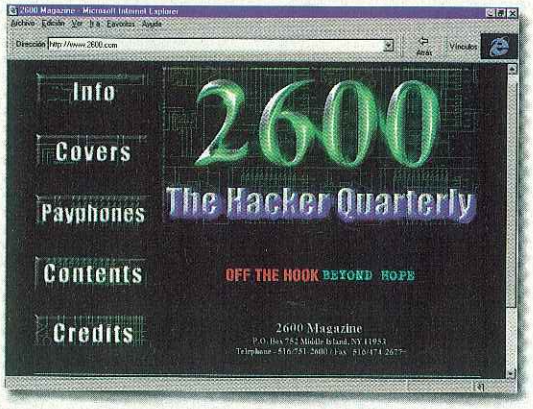
Ahora vamos a prender un poco más acerca de los hackers.

¿Qué es un Hacker?

Después de esta pequeña introducción y de ver por encima como están las cosas en este extraño mundo, vamos a averiguar un poco más sobre estos curiosos personajes. Salvando las distancias, podríamos comparar a los hackers con aquellos alquimistas que buscaban incansablemente la piedra filosofal, el conocimiento en su estado más puro. A los hackers les ocurre algo parecido, sólo que son más curiosos aún y como herramienta utilizan el ordenador y la informática.

Aunque la palabra hacker está irremisiblemente ligada al delito informático, no es así en todas sus facetas. Y es que a un hacker se le puede acusar de entrar sin permiso en un sistema informático, tal vez también se les pueda acusar de dejar





su huella o la marca de la casa (y es que hay algunos que pecan de orgullo, muchas veces les pillan por eso). Pero no se les puede achacar el destruir la información de forma intencionada, ni la venta de la misma tampoco, en ese caso ya no serían hackers.

Otra faceta muy ligada al hacking es el phreaking, por la cual se intenta conseguir no pagar las llamadas telefónicas que realizan (comprensible sí imaginamos todo el tiempo que estarán conectados a Internet). En España la cosa está bastante difícil, ya que Telefónica posee unos métodos de seguridad muy competentes y, en cambio en Estados Unidos se cuentan cosas bastante asombrosas, como el funcionamiento de las Box, circuitos electrónicos que se encargan de emular las señales de una central de teléfonos de forma que se estafa a la compañía de teléfonos.

Normalmente los hackers actúan solos, pero suelen formar grupos donde combren, para poder entrar.

Técnicas de hacking

Hay varias técnicas o métodos básicos que emplean los hackers para forzar los sistemas de seguridad e introducirse en los sistemas informáticos sin autorización. Estas técnicas requieren unos grandes conocimientos de informática y no están al alcance de todos los usuarios. Para aprender hay que hacer varias cosas, entre ellas estudiar informática, practicar mucho y bucear por Internet para encontrar información. Quien quiera aprender, ya puede olvidares de encontrar un sitio (página Web o revista) donde le cuenten los pasos a seguir para empezar a ser un hacker. Para entrar en un sistema, los hackers aprovechan las debilidades del mismo. Estas debilidades se agrupan en tres causas, que son: los usuarios inexpertos o novatos que dejan, sin darse cuenta, sus passwords (códigos de acceso al sistema) al alcance de los hackers; los passwords fáciles de adivinar (como por ejemplo poner como código "123" o el nombre de su novia); y los sistemas de seguridad débiles o mal configurados. A continuación os vamos a resumir las técnicas más comunes para reventar un sistema y forzar la entrada en el mismo:

Caballos de Troya: Se trata de introducir dentro de un programa en principio inocuo, un pequeño trozo de código que el usuario desconoce y que se ejecuta de forma automática., proporcionando el password, acceso al sistema o lo que queramos.

Sendmail: Se trata de poner código en un correo electrónico y enviarlo a una máquina. En este momento sendmail chequea el mensaje y la dirección electrónica, pero también el código añadido. Como Sendmail tiene todos los privilegios puede, por ejemplo, cambiar el fichero de passwords y proporcionar un acceso al sistema.

SuperZapping: Como utilizar las Norton dentro de uno de estos grandes ordenadores y modificar, copiar o insertar los datos almacenados.

Password Cracking: Esta técnica es la más antigua y una de las más utilizadas desde siempre. Se trata de conseguir el archivo de passwords de una máquina UNIX (normalmente está en el directorio /etc/passwd o en /etc/shadow) y extraer los login (el nombre de la cuenta) y passwords. Actualmente existen varios programas que automatizan la tarea con la ayuda de un diccionario: sólo hace falta pasarle el fichero y automáticamente intenta extraer los datos.

Puertas Falsas: Cuando se desarrolla el programa es normal que se coloquen interrupciones para chequear la ejecución de las aplicaciones o producir salidas de control para corregir defectos. También es normal que una vez terminado el programa las rutinas de detección de errores no sean eliminadas, proporcionando a los hackers unos asideros importantes, si los descu-

Ingeniería social: Se trata de convencer a la gente, mediante psicología o engaños, para que proporcione su identidad y contraseñas. Es típico llamar a un usuario haciéndose pasar por el administrador del sistema y, con alguna excusa, pedir el Password. Ante esto sólo hay una defensa: no dar nuestro Password ni a nuestra madre (si nos lo pregunta por teléfono, claro).

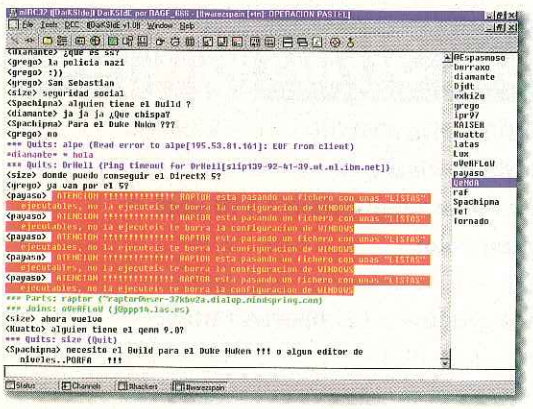
Simulación de Identidad: Es la evolución de la ingeniería social y consiste en engañar al usuario recreando su terminal de entrada (por lo que éste proporciona su login y su password sin creer que está siendo engañado). También es aplicable a entrar en un terminal utilizando la identidad de otra persona.

Para contrarrestar las acciones de los hackers, los administradores utilizan varios métodos para proteger sus sistemas. Los principales son:

FireWalls: Se trata de un software y hardware encargado de checkear y bloquear el tráfico de la Red (Internet) hacia un sistema determinado (una Intranet, una Red de área local o un servidor).

Smart cards: Son tarjetas de acceso con información codificada que sirven para tener acceso a algún sistema informático.

Monitorización: Se refiere al empleo de Logs, por lo que todas las conexiones recibidas en un servidor son grabadas para su posterior análisis. Los buenos hacker desactivan los Logs y borran cualquier huella que puedan haber dejado, de forma que el administrador no se entera de que alguien ha entrado sin permiso.



partir sus conocimientos y hazañas (este es el caso de Saqueadores, Iberhack o Underhak entre otros). La imagen que tenemos de los hackers es de un chico joven, bastante desaliñado y al que parece que la pantalla del ordenador le ha hecho "ventosa" (más que nada por las muchas horas que pasan frente a ella). Es posible que algunos respondan a este estereotipo (creado, seguramente, por la famosa película "Juegos de guerra", a la que le han seguido otras cintas de dudosa calidad, como es el caso de la última "Hackers"), pero no tiene por qué ser así. Casi todo el mundo que sepa lo suficiente de informática y tenga la suficiente curiosidad puede ser un hacker, solamente tiene que tener valor... y ganas.

BSA, la otra cara de la moneda

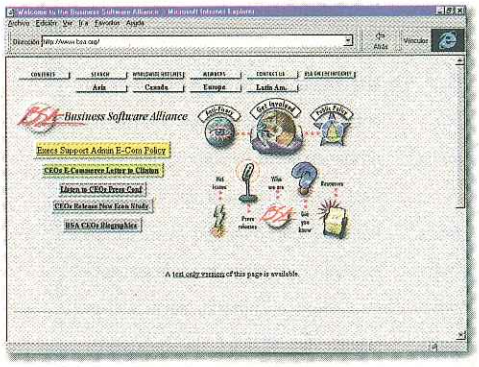
Actualmente la BSA, junto a las autoridades españolas, están acosando a todos los piratas, servidores warez y páginas Web donde se albergan los cracks (ver definición en el glosario). La BSA se dedica a salvaguardar los intereses de varias compañías de Software en más de 60 países (de prácticamente todo el mundo: Asia, Europa, Norteamérica e Hispanoamérica). Algunas de estas compañías son Microsoft, Adobe, Autodesk, Intergraph, Lotus, Novell, WordPerfect, Symantec, etc.

Aunque directamente la BSA no está enfrentada a los hackers ni tiene como finalidad hostigar a este colectivo, sí ve con muy malos ojos la inclusión de cracks o programas warez en las páginas Web de temática Hacker (tal y como hemos podido comprobar, en algunas páginas de temática hacker también podemos encontrar cracks y programas o enlaces a warez). Normalmente, las campañas que la BSA lleva a cabo para eliminar los deli-

Puntos de interés

Existen varios puntos de Internet donde podremos encontrar información acerca de este tema y muchos más. Empezaremos con las News, existen varios grupos en Inglés: Alt.2600, Alt.2600.loquesea, Alt.magazine.2600 y en general todos los que empiezan por alt.hacker. En castellano sólo existe un grupo: es.comp.hacker que, desgraciadamente, está inundado por múltiples peticiones de cracks y del que huyen los hackers más experimentados. Sin embargo, siempre es beneficioso para los principiantes, porque existen múltiples discusiones y en ocasiones se puede recoger información interesante. En el IRC existen varios canales de esta temática, entre ellos: #hackers o #warez. Para finalizar este apartado os vamos a dar varias direcciones HTML, entre las que destaca la de Islatortuga (www.islatortuga.com), donde podremos encontrar bastantes páginas con este tipo de contenidos. Sin embargo, es posible que al leer estas líneas algunas de estas páginas ya no existan ¡qué le vamos a hacer! (siempre nos quedarán las News y el IRC).

UNDERHACK http://www.geocities.com/SiliconValley/Park/7479/
Big Brother http://www.geocities.com/SiliconValley/Pines/7347/
Borno, el Hacker http://www.geocities.com/SiliconValley/Heights/9891/borno.html
Cosa Nostra http://members.tripod.com/~cosanostra23
CyberHack http://www.geocities.com/SiliconValley/Pines/2558/intro.html
Canal Pirata Digital http://www.geocities.com/ResearchTriangle/8531/indice.htm
La cueva de Van Hackez http://members.tripod.com/~kaligula/vanhackez.html
GATEKEEPER http://www.larc.net/Desertika/GateKeeper/index.htm
Saqueadores http://www.geocities.com/SiliconValley/8726/
The New Mafia Magazine http://www.ctv.es/mafia/
La vieja guardia http://www.geocities.com/SiliconValley/park/1734/index2.htm



tos informáticos en los distintos países tienen diferentes finalidades:

- Difusión de las leyes de protección jurídica de programas de ordenador y promoción y apoyo del cumplimiento de las leyes.
- Intentan concienciar a los usuarios de lo beneficioso para ellos que resulta utilizar programas originales. No se olvidan de recalcar las desventajas de emplear copias ilegales.

También emprenden acciones legales contra aquellas organizaciones que producen o comercializan copias ilegales de programas, así como contra quienes los compran o utilizan (como aquellos 30 usuarios que pasaron a disposición judicial por comprar a través de Internet CD-ROMs con programas piratas).

La BSA cuenta con un fuerte respaldo y grandes recursos para dedicarse a combatir la piratería informática, por lo que creemos que es un serio contrincante que dará muchos disgustos a todos aquellos hackers que sientan la tentación de cruzar la línea y emplear sus conocimientos para otros fines más oscuros.

Rafa Daroca

HACKERS al habla

Nos interesaba que conocieseis el punto de vista de uno de estos personajes. Por ello enviamos varios mensajes a todos los hackers que encontramos por la red. Aunque hubo más (desde aquí os damos las gracias a todos), uno de los que contestó fue Cy, del grupo Cyberhackers, que mantiene una página Web con información y enlaces referentes a esta temática. Cy publica periódicamente una revista con el mismo nombre en formato Adobe acrobat, donde nos explica las características escondidas de algunos teléfonos móviles, algo sobre virus, etc. El resultado de la entrevista que realizamos fue el siguiente:

¿Qué es un hacker para ti?

Un Hacker es una persona que no tiene por qué ser un maníaco del ordenador, ni ningún pirado que se tire enfrente de un monitor 30 horas al día... :-) sino que puede ser alguien normal y corriente (como yo) pero al que le atraiga saber más de los sistemas ocultos de las compañías (por ejemplo telefónica, CPIs, o incluso más de las máquinas de Coca-Cola). En conclusión, poder saber más que la persona que crea el sistema de seguridad.

¿Cómo nace un hacker? ...Y ¿cómo aprendiste tú a serlo?

Nadie nace sabiendo Hacking, pero sí se nace con ganas de serlo. No piensas cuando tienes 4 años que vas a hackear un VAX pero ves la vida de otro modo. Pues la mejor manera de aprender es practicar, y aquí la mejor manera es reventando tu propio sistema, y aprendiendo a ponerlo en marcha, subsanar fallos... etc.

¿Por qué te dedicas a esto?

Porque me fastidia al igual que otros muchos, que vivamos en el mundo de la información pero que nadie esté informado... entonces ¿sólo para unos pocos? :-?

¿Qué opinión te merece aquellos que hablan de Internet y de los hackers sin ningún conocimiento?

Pues como en decenas de revistas han hablado de que si los hackers destruyen, revientan, y tiran abajo todo lo que se mueve por Internet, entonces falla algo... o no están hablando de hackers, o los de la revista o los que comenten el tema son unos fantasmas.

¿Alguna vez has sido cracker? ¿Has hecho daño a alguien en la red alguna vez?

Cracker es una persona que se dedica a desproteger programas y a hacer cracks para ellos, producen Warez (software pirata), pero no me dedico a ello. Si he hecho daño a alguien ha sido porque se ha metido conmigo, en IRC... porque de otro modo nadie ha podido decir algo en contra mía. En IRC la manera de cargarte gente es flodeando, nukeando, Ultrapings... pero no es nada grave... lo máximo es que lo puedes desconectar de la línea con un Nuke.

¿Qué es lo que hace que cada cierto tiempo edites una revista con temas relacionados al Hacking, phreaking, virus o anarquía? ¿Te gusta comunicar a los demás tus conocimientos? ¿Compartir la información que consigues?

Exactamente, hasta ahora hay gente que se dedica a descubrir cosas o simplemente a rapiñear de los demás, y una vez que tienen mucha información y saben hacer algo, les gusta sentirse como dioses, estos no comparten entonces la libre información. Mi revista CyberHack está hecha basándose en conocimientos propios, pero sin las típicas fantasmadas que nos podemos encontrar en tantas otras revistas o Webs, sino que lo que hay ahí funciona.

Dime... ¿Existe una comunidad Hacker o algo parecido? ¿Tienes amigos dentro de este mundo o te dedicas a esto tu sólo? ¿Quiénes son?

Si, tengo amigos fuertes en el mundo del hack como Freezer, Daemon, Angelipas,... pero no es una comunidad grande, sino un grupo de amigos que nos movemos en el mismo ámbito y hemos llegado a entablar gran amistad... ;) un saludo a todos ellos.

Cuéntame alguna acción Hack que hayas protagonizado. Del tipo que más te guste.

La verdad que si te contara alguna y por casualidad algún día me pillaran, estaría firmando mi sentencia... ¿no crees?. De todos modos yo me he dedicado más al phreak y mi amigo Ipas al Hack... y no puedo contar nada en su nombre.

Tienes miedo de que te pase algo. Con Fer13 detenido, Isla tortuga pendiente de un hilo y con las páginas de hack más importantes en proceso de desaparición. ¿Qué opinas de la BSA y el caso de Islatortuga?

Creo que Fer13 cogía las cosas de un lado de la red y las ponía en otro, era como una hormiga que cogía las cosas perdidas por ahí, y las coleccionaba, por eso se hizo fuerte. Por otra parte, de la BSA no hace falta que comente nada, sus motivos son simplemente económicos... cuanto más gente pillen más dinero para ellos... :/

¿Hasta cuando seguirás siendo Hacker?

Toda mi vida, con o sin ordenador. Uno es hacker cuando siente algo dentro que le impulsa a saber sobre lo que nadie sabe, y a tener lo que nadie tiene. Se lleva dentro.

Pequeño glosario Hacker

A continuación os vamos a contar el significado de varias palabras relacionadas con el mundo hacker y underground en general:

Boxes: Aparatos electrónicos o eléctricos cuya finalidad es el phreaking (más abajo). Las más conocidas son:

Bluebox: Para llamar gratis.

Redbox: Emula la introducción de monedas en teléfonos públicos.

Blackbox: El que llame a un teléfono con este dispositivo no paga la llamada.

Carding: Uso fraudulento de tarjetas de crédito o sus números pertenecientes a otras personas. Ello incluye la generación de nuevas tarjetas de crédito.

Cracker: Un individuo que se dedica a eliminar las protecciones lógicas y físicas del software. Normalmente muy ligado al pirata informático puede ser un hacker criminal o un hacker que daña el sistema en el que intenta penetrar.

Crackeador o crack: Término muy de moda gracias al asunto de la "Página del Jamón y el vino". Son programas que se utilizan para desproteger o sacar los passwords de programas comerciales. Pudiendo utilizarse éstos como si se hubiera comprado la licencia. Quienes los distribuyen son altamente perseguidos por la BSA.

El gran Hermano: En el mundo del Hacking se conoce por este término a cualquier empresa poderosa que intenta controlar el mercado y el mundo de la informática. En este estado podríamos colocar a IBM, Microsoft, Telefónica, etc. El brazo ejecutor del gran hermano, como muchos habrán adivinado, es la BSA.

Hacking: Es cuando se entra de forma ilegal y si en consentimiento del propietario en un sistema informático para obtener información. No conlleva la destrucción de datos ni la instalación de virus. También lo podríamos definir como cualquier acción encaminada a conseguir la intrusión en un sistema (ingeniaría social, caballos de Troya, etc.)

Hacker: Cualquier persona que se dedica a hacer hacking. Debe ser bastante bueno con los ordenadores (como mínimo).

Lamer: Principiante en el mundo del hacking que se las da de listo o que copia, descaradamente, el trabajo de otros hackers. Cuando se les descubre se les desprecia y se les expulsa del círculo en el que se han introducido.

Phreaking: Todo lo relacionado con el uso del teléfono o servicios telefónicos de forma gratuita. También incluye la modificación o intervención de las líneas telefónicas y las modificaciones de aparatos telefónicos con el fin comunicarse gratuitamente.

Pirata informático: Es un delincuente informático que se dedica a la copia y distribución de software ilegal. Este software puede ser comercial crackeado o shareware registrado. También es otro nombre que reciben los crackers, no confundir con los hackers.

VIRUSES o VII: Textos sobre virus. Normalmente se incluye información acerca de como hacerlos y como protegerse de los mismos.

Warez: Programas comerciales ofrecidos gratuitamente a través de Internet. Periódicamente aparecen por Internet (en las News o IRC) unas listas con información de servidores FTP o WWW donde se encuentran programas de estas características. Piratería informática.

Ahora unos términos intrínsecamente relacionados con el Hacking:

Administrador, SysOp, Root: Individuo que se encarga del mantenimiento de un sistema informático y tiene un control total sobre el mismo. También se encarga de la seguridad.

Backdoor: Puerta trasera de un sistema informático, un mecanismo del software que permite entrar evitando el método usual.

Bug, Hole: Agujero. Se trata de un defecto en el software (normalmente el S.O.) que permita la intrusión de los hackers.

Caballos de troya: Programa que se queda residente en un sistema informático y facilita información sobre lo que ocurre en el mismo (passwords, logins, etc.). También es aplicable a programas que parecen normales y al ejecutarse despiertan un virus que se introduce en el sistema.

Cortafuego, firewall, bastión: Software y hardware de seguridad encargado de chequear y bloquear el tráfico de la red hacia un sistema determinado.

Crackeador: Programa que se emplea para extraer los passwords encriptados del archivo de passwords. Para ello se intenta desencriptarlo o se prueban múltiples combinaciones hasta encontrar la adecuada.

Exploit: Método de utilizar un bug para penetrar en un sistema.

Fichero de Password: Fichero donde se guardan las claves de acceso a un sistema.

Fuerza Bruta: Forma poco sutil de entrar en un sistema que consiste en probar distintos passwords (contraseñas) hasta encontrar la adecuada. Requiere mucho tiempo y para ello se emplea un crackeador, se desencripta un fichero encriptado, se sacan las claves del fichero de passwords empleando las palabras del diccionario, etc.

Ingeniería social: Es una técnica por la cual se convence a alguien, por diversos medios, de que proporcione información útil para hackear o para beneficiarnos. Requiere grandes dosis de psicología.

Sniffer y Sniffing: Un Sniffer es un programa que intercepta la información que transita por una red. Sniffing es espiar y obtener la información que circula por la red.

Tracear: Seguir la pista a través de la red de una información o una persona. Se utiliza por las grandes empresas (como Telefónica) para obtener la identidad de los sospechosos o hackers.

Trashing: En castellano recoger por la basura. Se trata de buscar en la basura (física o informática) que pueda ser útil para hackear.

War Dialer, Discador: Programa que escanea las líneas de teléfonos en la búsqueda de modems.