Hacker y cracker, dos filosofías diferentes

¿Qué es un hacker?

Un hacker se autodefine como una persona que sólo desea conocer el funcionamiento interno de los sistemas informáticos, ayudando a mejorarlos en el caso de que detecte fallos en su seguridad.

El hacker dice actuar por el ansia de conocimiento y el reto de descifrar el funcionamiento interno de los ordenadores y servidores de Internet. Para un hacker, el objetivo es asaltar los sistemas de seguridad de los servidores de Internet para llegar hasta su interior, pero, una vez dentro, no causar ningún daño. A veces, el hacker deja una señal o "bandera" en el servidor (al estilo de "yo estuve aquí"), que sirva como prueba de que ha conseguido acceder a él.

El hacker con su actividad permite que los administradores del sistema vulnerado detecten el acceso al servidor, ayudándoles así a mejorar la seguridad. Frecuentemente los "hackers", tras acceder a un sistema, informan a sus propietarios de los agujeros de seguridad que tiene su servidor, para que nadie malintencionado (como un cracker) pueda aprovecharse a posteriori de esa vulnerabilidad.

En los últimos años, los hackers han creado redes de comunicación entre ellos. Uno de los canales más usados es el IRC (Internet Relay Chat). Allí los interesados reciben las primeras lecciones, conocen otras personas para formar grupos e intercambiar información.

El IRC es anónimo. Un aspecto a destacar de la actividad del hacker es que nunca quiere revelar su verdadera identidad ni tampoco quiere ser rastreado. Actualmente existen cerca de 30.000 paginas web en la Internet dedicadas al hacking.

Los primeros hackers

En los años 60, los programadores del Massachussets Institute of Technology usaban hacks (pequeñas modificiaciones) y decidieron autodenominarse hackers. Su intención era hacer programas mejores y más eficaces.

Podría considerarse como uno de los primeros hackers a Linus Torvalds, creador de Linux. El sistema GNU/Linux ha sido creado y es mantenido por los hackers.

¿Qué es un cracker?

Al igual que el hacker, el cracker es también un apasionado del mundo informático. La principal diferencia consiste en que la finalidad del cracker es dañar sistemas y ordenadores. Tal como su propio nombre indica, el significado de cracker en inglés es "rompedor", su objetivo es el de romper y producir el mayor daño posible. Para el hacker, el cracker no merece ningún respeto ya que no ayudan ni a mejorar programas ni contribuyen a ningún avance en ese sentido. Desde distintos ámbitos se ha confundido el término hacker con el de cracker, y los

principales acusados de ataques a sistemas informáticos se han denominado hackers en lugar de crakers.
El término cracker fue acuñado por primera vez hacia 1985 por hackers que se defendían de la utilización inapropiada por periodistas del término hacker.

Se distinguen varios tipos de cracker:
PIRATA. Su actividad consiste en la copia ilegal de programas, rompiendo sus sistemas de protección y licencias. Luego distribuye los productos por Internet, a través de CD"s, etc.
LAMER. Se trata de personas con poco conocimiento de informática que consiguen e intercambian herramientas no creadas por ellos para atacar ordenadores. Ejecutan aplicaciones sin saber mucho de ellas causando grandes daños.
PHREAKERS. Son los crackers de las líneas telefónicas. Se dedican a atacar y "romper" los sistemas telefónicos ya sea para dañarlos o realizar llamadas de forma gratuita.
TRASHER. Su traducción al español es la de 'basurero'. Se trata de personas que buscan en la basura y en papeleras de los cajeros automáticos para conseguir claves de tarjetas, números de cuentas bancarias o información secreta para cometer estafas y actividades fraudulentas a traves de Internet.
INSIDERS. Son los crackers 'corporativos', empleados de las empresas que las atacan desde dentro, movidos usualmente por la venganza.
Kevin Mitnik, el mito.
Este californiano es un mito del "crackeo". En 1981 Kevin y dos amigos suyos irrumpieron en las oficinas de Cosmos (Computer System for Mainframe Operations) de la compañía Pacific Bell, una base de datos utilizada por la mayor parte de las compañías telefónicas. De allí obtuvieron la lista de claves de seguridad, la combinación de las puertas de acceso de varias sucursales, y manuales del sistema COSMOS, entre otras cosas. Lo sustraido por Mitnick y sus amigos podría tener un valor equivalente a 170.000 euros. Mitnick fue condenado por una corte juvenil a tres meses de cárcel y a un año bajo libertad condicional.

Su siguiente arresto tuvo lugar en 1983. Mitnick fue capturado por usar un ordenador de la universidad para obtener acceso (ilegal) a la red ARPAnet (la predecesora de Internet). Fue descubierto entrando en un ordenador del Pentágono a través de ARPAnet, y fue sentenciado a seis meses de cárcel.

En 1987 tuvo lugar el escándalo que lo lanzo a la fama. Kevin y su gran amigo, Lenny DiCicco, se enzarzaron en una lucha electrónica continua contra los científicos del laboratorio de investigación digital de Palo Alto. Mitnick estaba obcecado en obtener una copia del prototipo del nuevo sistema operativo de

seguridad llamado VMS y estuvo intentando conseguirlo obteniendo la entrada a la red corporativa de la empresa, conocida como Easynet. Aunque la empresa descubrió los ataques casi inmediatamente, no sabían de dónde venían. De hecho ni el propio FBI podía fiarse de los datos obtenidos de las compañías telefónicas ya que Mitnick se ocupaba de no dejar rastro alterando el programa encargado de rastrear la procedencia de las llamadas y desviando el rastro de su llamada a otros lugares. Al poco, un equipo de agentes del departamento de seguridad telefónica logró apresarle.

Tras salir de la cárcel y después de algún tiempo en la sombra, el mayor pirata informático de la historia publico dos libros, "The art of deception" (2002), donde donde describe técnicas de manipulación y persuasión gracias a las cuales se pueden obtener los códigos necesarios para entrar en la red de una empresa y hacerse pasar por otra persona y "The art of intrusion" (2004).

Otros casos de crackers

SHADOWHAWK. Bajo el pseudónimo de 'Shadowhawk', Herbert Zinn fue el primer sentenciado bajo el cargo de Fraude Computacional y Abuso en 1996. Violó el acceso a la AT&T y a diversos archivos y programas del Deparatmento de Defensa de EE.UU. Fue sentenciado a 9 años de cárcel y a pagar una multa de 10.000 dólares. En caso de haber sido mayor de edad podría haberse enfrenado a 13 años de prisión.

DARK DANTE. Bajo este alias se escondía Kevin Poulsen, que atacó el sistema informático de la fuerza aérea norteamericana. Aunque es más conocido por habilidad en controlar el sistema telefónico, lo que le llevó incluso a ganar un Porsche en un concurso radiofónico. Sus diversos delitos le llevaron a pasar 5 años en prisión.

CAPTAIN ZACK. Ian Murphy entró y dañó en 1981 los sistemas de la Casa Blanca, el Pentágono y BellSouth Corp. TRW. Después de los ataques, este cracker dejaba deliberadamente su currículum.