SEGURIDAD EN INTERNET

José A. Pérez Cruz

Historia

En 1959 un grupo de alumnos del Massachussets Institute Technology (MTI) fueron los primeros en usar aquellas computadoras inmensas por medio de un curso de programación llegando a ingeniárselas para pasar todo el tiempo posible con "la bestia".

Para esos tiempos apareció la TX-0 teniendo acceso ilimitado a este juguete, pues ya no funcionaba con tarjetas perforadas y tenía un teclado incorporado que permitía ver directamente los frutos del trabajo hecho. Pronto fueron capaces de hacer cosas que ni los mismos diseñadores de la máquina habían imaginado. De aquí nace el término hacker.

Este término se empezó a usar a finales de los 80 con la llegada de las PC a las casas, dándoles el sinónimo de "piratas informáticos", naciendo destripadores de la red como la Legion of Doom (Legión del fin del mundo) y Masters of Deception (Maestros de la decepción), los cuales se enfrentaron en una guerra, la cual término con varios detenidos, donde la prensa que desconocía los términos los tomó como vándalos electrónicos.

Entre todo esto aparece Kevin Mitnick, quien fue el hacker más buscado y todo un mártir de los hackers. Sus seguidores hackearon Yahoo, New York Times, Motorola, Penthouse, y la web de la NASA. Podemos terminar diciendo que hay usuarios, usuarios un pocos más informados, técnicos, programadores y hackers.

Hackers

Hacker [originalmente, alguien que fabrica muebles con un hacha]. 1. Persona que disfruta con la exploración de los detalles de los sistemas programables y cómo aprovechar sus posibilidades; al contrario que la mayoría de los usuarios, que prefieren aprender sólo lo imprescindible. 2. El que programa de forma entusiasta (incluso obsesiva). 3. Persona capaz de apreciar «el valor del hackeo». 4. Persona que es buena programando de forma rápida. 5. Experto en un programa en particular, o que realiza trabajo frecuentemente usando cierto programa: como en "es un hacker de UNIX." (Las definiciones 1 a 5 están correlacionadas, y la gente que encaja en ellas suele congregarse.) 6. Experto o entusiasta de cualquier tipo. Se puede ser un "hacker astrónomo", por ejemplo. 7. El que disfruta del reto intelectual de superar o rodear las limitaciones de forma creativa. 8 [en desuso] Liante malicioso que intenta descubrir información sensible cotilleando por ahí. De ahí vienen "hacker de contraseñas" y "hacker de las redes". El término correcto en estos casos es cracker

Tipos de hackers

Samurai: un hacker que crackea amparado por la ley o la razón, normalmente es alguien contratado para investigar fallos de seguridad, que investiga casos de derechos de privacidad, éste amparado por la primera enmienda estadounidense o cualquier otra razón de peso que legitime acciones semejantes. Los samuráis desdeñan a los crackers y a todo tipo de vándalos electrónicos.

Sneaker: es aquel individuo contratado para romper los sistemas de seguridad por las empresas e instituciones con la intención de subsanar dichos errores.

Crackers: En los márgenes de la comunidad hacker se sitúan los crackers. Los crackers, temidos y criticados por la mayoría de hackers, por el desprestigio que les supone ante la opinión pública y las empresas, son aquellos que utilizan sus conocimientos técnicos para perturbar procesos informáticos.

El que rompe la seguridad de un sistema. Acuñado hacia 1985 por hackers en defensa contra la utilización inapropiada por periodistas del término hacker (en su acepción número 8.) Falló un intento anterior de establecer "gusano" en este sentido en 1981-1982 en Usenet.

Hay distintos tipos de crackers. Muchos crackers pertenecen a la categoría de script kiddies, es decir, bromistas de mal gusto, muchos de ellos adolescentes, que penetran sin autorización en sistemas o crean y difunden virus informáticos para sentir su poder, para medirse con los otros, para desafiar al mundo de los adultos

¨ Docente de tiempo completo en la Universidad Autónoma del Carmen.

* Texto tomado de el archivo Jargon (jerga) de Internet, que también puede encontrarse en forma de libro como el «Diccionario del Hacker» [«The New Hacker´s Dictionary», segunda edición, de Eric S. Raymond.]

y para chulear con sus amigos o con sus referentes en la red. La mayoría de ellos tiene conocimientos técnicos limitados y no crea ninguna innovación, por lo que son, en realidad, marginales al mundo hacker. Otros crackers, más sofisticados, penetran en sistemas informáticos para desafiar personalmente a los poderes establecidos, por ejemplo, a Microsoft o las grandes empresas. Y algunos utilizan su capacidad tecnológica como forma de protesta social o política, como expresión de su crítica al orden establecido. Ellos son quienes se introducen en sistemas militares, administraciones públicas, bancos o empresas para reprocharles alguna fechoría. Entre los ataques de crackers con motivación política hay que situar los practicados por movimientos políticos o por servicios de inteligencia de los gobiernos, como la guerra informática desarrollada entre los crackers islámicos e israelíes o entre los pro-chechenos y los servicios rusos.

Los demás

Delincuente informático

Es la persona o grupo de personas que en forma asociada realizan actividades ilegales haciendo uso de computadoras en agravio a terceros. Una de las prácticas más conocidas es la de interceptar compras en línea a través de Internet.

Wannabes

Alguien que podrá a llegar a ser un hacker, pero que aún no lo es. Todos los hackers pasan por esta etapa. Un wannabe adquiere el status de hacker cuando los veteranos deciden empezar a considerarle uno de los suyos.

Newbie

Algo muy similar a wannabe, son novatos. Ellos pueden ser unos tiernos pipiolos en determinados círculos, pero debido a sus habilidades pueden no ser tan novatos en el área y darnos buenos sustos.

Estado Larval

Para entrar a este comando de élite dentro de los guerreros de los bits hay que pasar por diferentes estados de desarrollo. Uno de los periodos más frecuentes es el larval que oscila entre los 6 meses y los 2 años y en el que el sujeto se encierra en su habitación a escribir código e ignora en mayor o menor medida la realidad que le rodea.

Mundane (Mundano)

Cualquier persona no iniciada en este mundo underground. Es decir, el común de los mortales.

Bogus (Farsante)

Ser hacker es un honor que hay que ganar y que la comunidad hacker concede. Uno no puede proclamar que lo es sin la aprobación de dicha comunidad, a menos que quiera ser mirado con desprecio y pasar a formar parte de la tribu de los hackers de pacotilla, los farsantes conocidos como bogus.

Lamer, sinónimo de Leecher y de Luser

(Mezcla entre user, usuario; y looser, perdedor), empleado más frecuentemente entre los crackers que entre los hackers. Es aquella persona que se aprovecha de los recursos de la comunidad underground sin aportar nada a cambio. Alguien que, por poner un ejemplo, descarga cracks sin cesar pero nunca desarrolla uno.

Muggle

Denominación inspirada en los personajes carentes de poderes mágicos de la serie de libros de Harry Potter, que convivían en el mismo mundo de los magos, pero eran ignorantes de la existencia y los poderes de estos últimos. Es decir, de nuevo el común de los mortales.

Weenie

El típico weenie es ese adolescente aficionado al rol y a la música metal, con escasas aptitudes sociales, que pulula y puebla parte del universo underground.

Bigot (Fanático)

Una persona que es férrea partidaria de un lenguaje de programación, de un particular sistema operativo o una computadora en concreto. Aplicable a los hackers y a la familia circundante.

Los tentados por el lado oscuro de la fuerza

Todos los hackers tienen habilidades de sobra para convertirse en crackers, pero han resistido la tentación y se mantienen dentro de la legalidad, incluso rechazan frontalmente a los caídos. Cuando un hacker responde al llamado del lado oscuro de la fuerza se convierte en un cracker o en un dark side hacker.

Warez d00dz

Una parte de estos ángeles caídos se refiere a sí mismos

de esta manera porque se dedican a obtener, desproteger o distribuir copias ilegales de software propietario.

Prehackers

Son aquellos que “rompen“ y hacen un uso ilegal de las redes telefónicas. Los phone phreaker son los más famosos en los medios de comunicación por los desastres que han hecho a través de los años. En los años 60 ya existían los phone phreaks y la gran víctima era ATT. Uno de los más famosos phone phreaks de esa época era John Draper, alias Captain runch (http://www.fc.net/phrack.html). Él descubrió que modificando una caja de cereal podía producir el silbido que simulaba un tono de 2600 Hz para desbloquear el acceso a una troncal y poder hacer llamadas internacionales gratis.

Cual es la diferencia

La utilización de ambos neologismos refleja una fuerte repulsión contra el robo y vandalismo perpetrado por los círculos de crackers. Aunque se supone que cualquier hacker auténtico ha jugado con algún tipo de crackeo y conoce muchas de las técnicas básicas, se supone que cualquier que haya pasado la etapa larval ha desterrado el deseo de hacerlo, con la excepción de razones prácticas inmediatas (por ejemplo, si es necesario pasar por alto algún sistema de seguridad para completar algún tipo de trabajo.)

El término hacker tiende a connotar participación como miembro en la comunidad global definida como **“**la red**“**. También implica que la persona descrita suele suscribir alguna versión de la ética del hacker.

Los crackers tienden a organizarse en grupos pequeños, muy secretos y privados, que tienen poco qué ver con la policultura abierta y enorme que se describe en este diccionario; aunque ellos a menudo se definen a sí mismos como hackers, la mayor parte de los auténticos hackers los consideran una forma de vida inferior.

Por lo tanto, hay mucho menos en común entre el mundo de los hackers y de los crackers de lo que el lector mundano, confundido por el periodismo sensacionalista, pueda suponer.

Consideraciones éticas aparte, los hackers consideran que cualquiera que no sea capaz de imaginar una forma más interesante de jugar con su ordenador que romper los sistemas de alguien ha de ser bastante perdedor. Algunas de las otras razones por las que se mira con desprecio a los crackers se describen en las entradas sobre cracking y phreaking (crackers telefónicos).

La diferencia

“Tenemos una casa**“**, ¿no? Bien, pues ¿qué haría un hacker? Sencillo, llegaría a la casa, daría la vuelta alrededor de la misma, y entraría por la puerta de atrás; después daría una vuelta por la casa, miraría, y se marcharía; por el contrario, el cracker tiraría una piedra contra la ventana, entraría y te ‘limpiaría’ la casa de arriba a abajo. ¿La diferencia? Tú nunca sabrías que el hacker entró en tu casa, pero sí sabrías que el cracker estuvo. Pues bien, tu ordenador, terminal o servidor, es tu casa.

Los hackers en la política

El movimiento hacker más político (en términos de política de libertad tecnológica) es el creado por Richard Stallman, un programador de MIT que constituyó en los años ochenta la Free Software Foundation para defender la libertad de acceso a los códigos de UNIX cuando ATT trató de imponer sus derechos de propiedad sobre UNIX, el sistema operativo más avanzado y más compatible de su tiempo, y sobre el que se ha fundado en buena parte la comunicación de los ordenadores en la red. Stallman, que aprendió el valor de la libertad en el movimiento de libre expresión en sus tiempos de estudiante en Berkeley, sustituyó el copy right por el copy left. Es decir, que cualquier programa publicado en la red por su fundación podía ser utilizado y modificado bajo licencia de la fundación bajo una condición: difundir en código abierto las modificaciones que se fueran efectuando. Sobre esa base, desarrolló un nuevo sistema operativo, GNU, que sin ser Unix, podía utilizarse como UNIX.

Que han hecho los hackers

En realidad, los hackers han sido fundamentales en el desarrollo de Internet. Fueron hackers académicos quienes diseñaron los protocolos de Internet. Un hacker, Ralph Tomlinson, trabajador de la empresa BBN, inventó el correo electrónico en 1970, para uso de los primeros internautas, sin comercialización alguna. Hackers de los Bell Laboratories y de la Universidad de Berkeley desarrollaron UNIX. Hackers estudiantes inventaron el módem. Las redes de comunicación electrónica inventaron los tablones de anuncio, los chats, las listas electrónicas y todas las aplicaciones que hoy estructuran Internet. Y Tim Berners-Lee y Roger Cailliau diseñaron el browser/editor World Wide Web, por la pasión de programar, a escondidas de sus jefes en el CERN de Ginebra, en 1990, y lo difundieron en la red sin derechos de propiedad a partir de 1991. También el browser que popularizó el uso del World Wide Web, el Mosaic, fue diseñado en la Universidad de Illinois por otros dos hackers (Marc Andreesen y Eric Bina) en 1992.

La tradición continúa. En estos momentos, dos tercios de los servidores de web utilizan Apache, un programa servidor diseñado y mantenido en software abierto y sin derechos de propiedad por una red cooperativa. En una palabra, los hackers informáticos han creado la base tecnológica de Internet, el medio de comunicación que constituye la infraestructura de la sociedad de la información. Y lo han hecho para su propio placer, o, si se quiere, por el puro goce de crear y compartir la creación y la competición de la creación. Ciertamente, unos pocos de entre ellos también se hicieron ricos como empresarios, pero mediante aplicaciones de sus innovaciones, no mediante la apropiación de la innovación cooperativa en su propio beneficio (aunque el caso de Andreesen es menos claro, en este sentido).

Otros obtuvieron buenos puestos de trabajo, pero sin l de hackers, fuente esencial de innovación en la era de la información.

Ética del hackerËW

1. El acceso a los ordenadores, y a cualquier cosa que pudiera enseñarte algo sobre cómo funciona el mundo, debería ser ilimitado y total.

2. Básate siempre en el imperativo de la práctica.

3. Toda información debería ser libre.

4.El acceso a los ordenadores, y a cualquier cosa que pudiera enseñarte algo sobre cómo funciona el mundo debería ser ilimitado y total.

5. Desconfía de la autoridad, promueve la descentralización.

6. Los hackers deberían ser juzgados únicamente por su habilidad en el hackeo, no por criterios sin sentido como los títulos, edad, raza o posición social.

7. Se puede crear arte en un ordenador.

8. Los ordenadores pueden cambiar tu vida a mejor.

Hackers famosos

De acuerdo a la historia de la era de la computación, la primera persona sindicada como hacker fue una respetable y sabia mujer: almirante de la Armada de los Estados Unidos, Grace Hooper, con la cual empezamos nuestra galería. Obtenga sus propias conclusiones.

La almirante, creadora del lenguaje COBOL

Grace Hooper creó el lenguaje Flowmatic, con el cual desarrolló muchas aplicaciones y en 1951 produjo el primer compilador, denominado A-0 (Math Matic). En 1960 presentó su primera versión del lenguaje COBOL (Common Business-Oriented Language).

Paradójicamente, recibió entre muchos reconocimientos y condecoraciones, el título de Hombre del Año en Ciencias de la Computación, otorgado por la Data Processing Management Association. También fue la primera mujer nombrada miembro distinguido de British Computer Society y hasta el día de hoy es la primera y única mujer con el grado de Almirante de la Marina de Guerra de su país. Grace Hooper falleció en 1992.

Por estas connotaciones, para muchos estudiosos la almirante Grace Hooper es considerada la primera hacker de la era de la computación.

Precursores de los creadores de virus informáticos

En 1939, el famoso científico matemático John Louis Von Neumann, de origen húngaro, escribió un artículo -publicado en una revista científica de New York, exponiendo su Teoría y organización de autómatas complejos, donde presentaba la posibilidad de desarrollar pequeños programas que pudiesen tomar el control de otros, de similar estructura.

En 1949, en los laboratorios de la Bell Computer, subsidiaria de la AT&T, tres jóvenes programadores: Robert Thomas Morris, Douglas McIlroy y Victor Vysottsky, a manera de entretenimiento, crearon un juego al que denominaron CoreWar, inspirados en la teoría de John Von Neumann.

Puesto en la práctica, los contendores del CoreWar ejecutaban programas que iban paulatinamente disminuyendo la memoria del computador y el ganador era el que finalmente conseguía eliminarla totalmente. Este juego fue motivo de concursos en importantes centros de investigación como el de la Xerox en California y el Massachussets Technology Institute (MIT), entre otros. Muchos lo tildan de hacker. Saque sus propias conclusiones.

En 1975 William Henry Gates y Paul Allen forman Microsoft Corporation, en la ciudad de Albuquerque, Nuevo México. Microsoft fue el proveedor de la versión del lenguaje BASIC para la computadora personal MITS Altair. Sin embargo, el lenguaje BASIC (Beginners All-purpose Symbolic Instruction Language) fue creado en 1964 por John G. Kemeny y Thomas E. Kurtz, del Dartmouth College.

Asimismo, la versión GW-BASIC, desarrollada por Microsoft para las primeras IBM PC, guardaba una gran similitud con la creada por los profesores Kurtz y Kemeny, en todas sus instrucciones.

El GW-BASIC motivó a Kemeny y Kurtz a reescribrir y lanzar al mercado su versión denominada TRUE BASIC, en 1984. ¿Bill Gates fue un hacker?

Autor del Tour Of The Worm en Internet

El 2 de Noviembre de 1988 Robert Tappan Morris, hijo de uno de los precursores de los virus y recién graduado en Computer Science en la Universidad de Cornell, difundió un virus a través de ArpaNet, (precursora de Internet) logrando infectar 6,000 servidores conectados a la red. La propagación la realizó desde uno de los terminales del Instituto Tecnológico de Massachussets (MIT).

Cabe mencionar que el ArpaNet empleaba el UNIX, como sistema operativo. Robert Tappan Morris, al ser descubierto, fue enjuiciado y condenado en la corte de Syracuse, estado de Nueva York, a 4 años de prisión y el pago de 10,000 dólares de multa, pena que fue conmutada a libertad bajo palabra y condenado a cumplir 400 horas de trabajo comunitario.

Kevin Mitnick un hacker famoso en la historia

Es quizá el más famoso hackers de los últimos tiempos. Nacido el 6 de agosto de 1963 en Van Nuts, California, desde muy niño sintió curiosidad por los sistemas de comunicación electrónica y fue auto cultivando una obsesiva curiosidad por investigar cosas y lograr objetivos aparentemente imposibles, hasta llegar a poseer una genial habilidad para ingresar

a servidores sin autorización, robar información, interceptar teléfonos, crear virus, etcétera.

Cuando el gobierno acusó a Kevin de haber substraído información del FBI, relacionada a la investigación de Ferdinand Marcos y de haber penetrado en computadoras militares, en 1992, él decidió defenderse en la clandestinidad, convirtiéndose en un fugitivo de la justicia durante casi tres años. Mitnick fue arrestado por el FBI en Raleigh, North Carolina, el 15 de Febrero de 1995.

Kevin descubrió y reveló información de alta seguridad perteneciente al FBI, incluyendo cintas del consulado de Israel, en Los Ángeles. Sus incursiones costaron millones de dólares al FBI y al gobierno norteamericano y obligó a este departamento policial a mudar sus centros secretos de comunicación a sitios inaccesibles.

Vladimir Levin, autor del más grande fraude electrónico

Un graduado en matemáticas de la Universidad Tecnológica de San Petesburgo, Rusia, fue acusado de ser la mente maestra de una serie de fraudes tecnológicos que le permitieron a él y la banda que conformaba, substraer más de 10 millones de dólares de cuentas corporativas del Citibank. En 1995 fue arrestado por la Interpol, en el aeropuerto de Heathrow, Inglaterra, y luego extraditado a los Estados Unidos.

Las investigaciones establecieron que desde su computadora instalada en la empresa AO Saturn, de San Petersburgo, donde trabajaba, Levin irrumpió en las cuentas del Citibank de New York y transfirió los fondos a cuentas aperturadas en Finlandia, Israel y en el Bank of America de San Francisco, Estados Unidos.

«Sir Dystic», el hacker autor del programa original Back Orifice, lanzado en 1998, da a conocer el lanzamiento de su nueva versión para Windows 2000 y NT.

En agosto de 1998 se difundió un sistema de control de redes, denominado Back Orifice, desarrollado por el grupo de hackers conocido como El culto de la vaca muerta. Concebido como una irónica demostración de la falta de seguridad en Windows® 95 y 98, (su nombre está inspirado en el MS Back Office), en esa oportunidad fue desarrollado para Windows NT y Windows 2000, con el nombre de Back Orifice 2000.

Su lanzamiento fue oficialmente anunciado el 10 de julio de 1999, en la VII Convención de Hackers, denominada DEFCON 7. Para evitar ser sorprendidos por el FBI, esta página web con frecuencia desaparece y vuelve a aparecer en otras locaciones. PER ANTIVIRUS® detecta este Caballo de Troya, impide su ejecución y lo elimina eficientemente.

El software el FBI

El software Carnivore fue concebido y desarrollado por el FBI de los Estados Unidos para investigar y descubrir actos de terrorismo, autores de virus, intrusos en la red (crackers), otros. Su secreto lanzamiento y accionar fue finalmente descubierto por EPIC.

A pesar de que hasta la fecha es materia de controversia, el Federal Bureau of Investigation de los Estados Unidos continúa usándolo. A propósito de la propagación del virus CodeRed en agosto del 2001, parte de los archivos de Carnivore fueron capturados por un grupo de hackers que los distribuyeron en un website temporal.

Como es sabido, contando con una orden judicial, el FBI puede instalar el sistema Carnivore en los servidores de un Proveedor de Servicios de Internet (ISP), con el objeto de monitorear todo el tráfico y las comunicaciones a través de ese ISP.

El FBI ha afirmado constantemente que su sistema filtra el tráfico de los datos y conserva solamente los paquetes que la corte ha autorizado a los investigadores. Sin embargo, el FBI ha mantenido el sistema completamente en secreto y fue hasta el 11 de julio de 2000 que se descubriese su existencia y la corporación EPIC hizo un seguimiento de los documentos del FBI relacionados con el sistema, al amparo del Acta de Libertad de la Información (FOIA). EPIC inquirió al FBI a que hiciera de público conocimiento todos los expedientes referentes a Carnivore, incluyendo su código de fuente, detalles técnicos y análisis que apuntaban a implicancias potenciales en contra de la privacía. The FBI's Cyber Crime Division is responsible for criminal investigations of intellectual property, high tech and computer crimes.

Richard Stallman, creador del concepto software gratuito

Richard Stallman fue otro de los jóvenes precoces que conoció e hizo uso de computadoras en 1969, a la edad de 16 años en el IBM New York Scientific Center. Fue dándose a conocer cuando empezó a trabajar en el Laboratorio de Inteligencia Artificial del Massachussets Institute of Technology(MIT), en 1971. A pesar de haber estudiado en la Universidad de Harvard, no concluyó sus estudios de Ciencias de la Computación. Mortificado por el hecho de que el *software* era considerado propiedad privada, Stallman fundó la *Free Software Foundation* (Fundación de Software Gratuito).

En la década de los 80, Stallman dejó de trabajar en forma estable en el MIT, pero continuó haciéndolo en sus horas libres desde una oficina de esa entidad. Allí creó el nuevo sistema operativo llamado GNU, compatible con Unix, pero con código fuente abierto y gratuito.

Bibliografía

HAFFNER, K.; MARKOFF, J. (1995). *Cyberpunks: outlaws and hackers in the computer frontier.* New York: Touchstone Books.

HIMANEN, P. (2001). *The hacker ethic and the spirit of the Information Age.* Prólogo de Linus Torvalds. New York: Random House (en castellano, Destino, 2002).

LEVY, S. (1984). *Hackers. Heroes of the computer revolution.* New York: Penguin.

RAYMOND, E. (1999). *The cathedral and the bazaar. Musings on Linux and Open Source by an accidental revolutionary*. Sebastopol, California: O' Reilly (en castellano, Alianza Editorial, 2002).