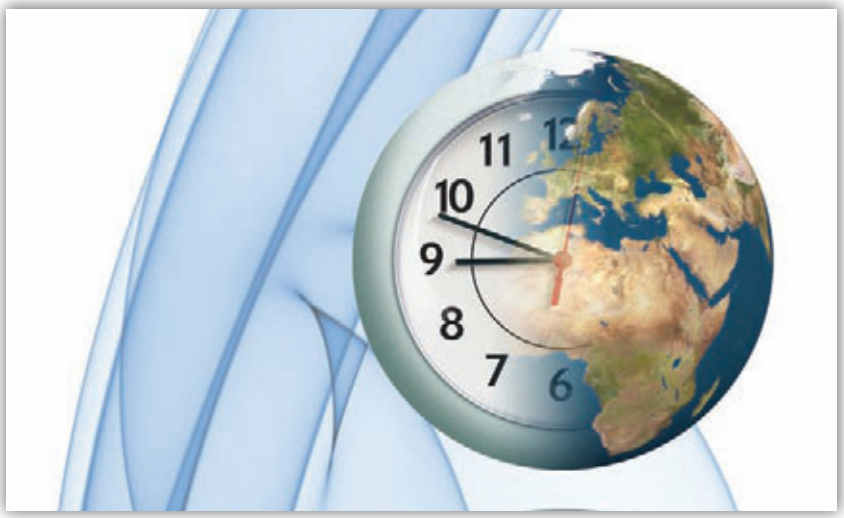
Un viaje en la historia del hacking

David Puente Castro

No existe mejor forma de afrontar el futuro que conociendo el pasado. ¿Quiere saber quiénes fueron los primeros hackers?, ¿quiénes los primeros grupos?, ¿cuál es la historia que da trasfondo a esta subcultura de gurús de la red? Continúe leyendo, y quizás pueda seguir sus pasos.



linux@software.com.pl

Un poco como dedicación a los tiempos pasados, hoy vamos a hacer un breve recordatorio desde las primeras épocas de los sistemas telefónicos e informáticos hasta la fecha de hoy sobre los actos más importantes que han sucedido acerca del mundo de la informática y el *underground*, y daremos unas escuetas descripciones a ciertos grupos de personas que han quedado enmarcados en nuestra memoria por sus diferentes actividades en el mundo del hacking.

Nacimiento del hacking

Lo más correcto sería utilizar definiciones provenientes del *Jargon File*, pero ya que la Wikipedia es un recurso universal utilizado por la mayoría de la gente, adoptaremos su breve definición acerca de lo que es un hacker: *Hacker es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc. Se suele llamar hackeo y hackear a las obras propias de un hacker.*

Y como muchos ya saben, esta palabra tan controvertida tiene sus orígenes en el MIT (*Instituto Tecnológico de Massachussets*), donde aparecieron por primera vez esas enormes computadoras que ocupaban habitaciones enteras y utilizaban tarjetas perforadas. Los más inteligentes y sedientos de curiosidad hicieron todo lo posible por acceder a esas máquinas el mayor tiempo posible, a la vez que aprendían de un modo incesante para mejorar sus programas y llevar esa nueva herramienta de la sociedad tecnológica a sus límites más extremos. Esos *chiflados de las computadoras* acabaron denominándose hackers.

A lo largo de la historia han existido hackers buenos y malos, aunque desgraciadamente los medios de información no han aprendido correctamente la lección de que a estos últimos debería llamárseles *crackers*. Es este el motivo del desprestigio que ha obtenido la palabra *hacker* entre la ignorante multitud que los pone a la altura de criminales o como algunos los denominan: ciberdelincuentes.

No debemos caer en la trampa de confundir el cracker cuando se utiliza como sinónimo de hacker *malo*, con el cracker de software que se dedica a encontrar las vulnerabilidades presentes en el mismo para evadir protecciones o saltarse ciertas restricciones. Para evitar esto, actualmente conocemos al cracker de software como *reverse engineer*. Una traducción que no es totalmente correcta sería *ingeniero reverso* o *ingeniero inverso*

Figura 1. Grupo L0pht

ya que la aplicación de sus técnicas abarcan un estudio conocido como *ingeniería inversa*.

Este tipo de cracker contribuye a la mejora de las protecciones de software y atrae nuevos conceptos sobre criptografía, aunque no dejemos de tener en cuenta las leyes que rigen el software privativo y las violaciones que al respecto se cometen cuando éstos facilitan al público sus famosos *cracks*, *serials* o *keygen's*.

Con el objetivo de poder distinguirnos unos de otros, existen hoy en día tres grupos principales en los que puede clasificarse la actitud de un hacker. Se resumen de la siguiente manera:

Hacker de Sombrero Blanco (White Hat)

El *white hat* es aquella persona que, de manera altruista o no, dedica su tiempo a la búsqueda de vulnerabilidades en un sistema para posteriormente reportarlas al administrador del mismo y colaborar con él en su consecuente reparación. Sus actos no comportan fines maléficos y normalmente realiza sus acciones bajo el consentimiento del propietario del sistema atacado.

Figura 2. Logo Cult of the Dead Cow

Hacker de Sombrero Negro (Black Hat)

El *black hat* es lo que comúnmente llamaríamos *cracker*, y sus fines son, además de lucrativos la mayoría de las veces, totalmente destructivos. Jamás avisa de los errores encontrados y los utiliza para echar abajo servidores importantes, borrar información privada o colapsar redes enteras bajo el efecto de un ataque de denegación de servicio (DoS o DdoS). Es, desde luego, la persona que menos puede aportar a la comunidad Underground preocupada de la seguridad de Internet, pero debemos ser realistas y afirmar que muchos de ellos acabaron convirtiéndose, después de una profunda madurez de su ética profesional, en hackers de sombrero gris o blanco.

Hacker de Sombrero Gris (Grey Hat)

Decir que el *grey hat* es una mezcla de los dos anteriores no es del todo correcto, dado que la mayoría de las veces se acerca bastante más al primero. Es el personaje que encuadramos dentro del llamado *hacker ético*. Podríamos decir que se encuentra en un limbo entre las dos fronteras pero que su actitud y ética le permite decidir con certeza qué comportamientos son los más adecuados a la situación a la que se enfrenta.

Sea como fuera, recordemos que todos ellos utilizan exactamente las mismas herramientas, y que solamente su cerebro y sus habilidades son los que diferencian claramente a unos de otros. Por lo demás, existen otros términos como *lamer*, *script kiddie*, *newbie*, *wannabie* y muchos otros. Los matices cambian dependiendo de la orientación que posean hacia el bien o hacia el mal, pero todos ellos tienen en común el bajo nivel de conocimientos de las técnicas de hacking. Es por ello que no los detallaremos aquí.

Si eres de los que todavía estás empezando en esto, y no encuentras un camino adecuado para adentrarte en la subcultura hacker, te recomiendo la lectura del documento *Hacker HowTo* (o Cómo Llegar a Ser un Hacker) escrito bajo la mano de Eric S. Raymond, fundador del movimiento Open Source, y que te ofrecerá las pautas necesarias para ir adquiriendo las habilidades propias del hacker de hoy.

Y si no, recuerda que hay algo que ha caracterizado a todo hacker que se precie, y es su capacidad para ser *autodidacta* y tener una curiosidad insaciable. Así es al menos el camino que muchos hemos seguido.

Historia

1878: Menos de dos años después de que el sistema telefónico de Alexander Graham Bell empezara a funcionar, un grupo de adolescentes echó abajo la red.

1958: EE.UU. crea ARPA (*Advanced Research Projects Agency*), ciencia y tecnología aplicada al campo militar.

1960: Los hackers originales utilizaron los primeros mainframes del MIT para desarrollar habilidades y explorar el potencial de la informática. En esa época, *hacker* era un término elogioso para los usuarios con un conocimiento exponencial de los ordenadores.

1969: La agencia de proyectos de investigación avanzados del *Departamento de Defensa* (DoD), construyó Arpanet.

1971: Antes del uso masivo de los ordenadores y de Internet, los *phreakers* utilizaron la extensa base de redes telefónicas. John Draper (*Cap'n Crunch*), descubrió que un simple silbato permitía a los usuarios entrar en los sistemas de facturación de las llamadas a larga distancia.

Figura 3. Richard Stallman

Figura 4. Kevin Mitnick

1973: Kahn desarrolla un nuevo protocolo, el TCP/IP (Transmisión Control Protocol/ Internet Protocol).

1976: Dos miembros del Homebrew Computer Club lanzaron las llamadas *blue box*, que se utilizaban para hackear sistemas telefónicos. La pareja (Steve Jobs y Steve Wozniak) conseguirían hacerse famosos después al fundar Apple Computer.

1983: Primer arresto de hackers por el FBI después de que invadieran el centro de investigación de Los Alamos. Se estrena la película *Juegos de guerra*, que cambió la percepción del público con relación a los hackers y estableció su prestigio.

1984: Se funda la publicación trimestral 2600 (nombrada como la frecuencia del silbato de John Draper), que ofrecía una plataforma a los hackers y phreakers para expresar sus conocimientos y habilidades. Se forma Legion of Doom (LoD).

1987: Herbert Zinn, de 17 años de edad, es arrestado después de entrar en el sistema de AT&T. Los expertos afirman que estuvo a punto de bloquear todo el sistema telefónico norteamericano. Se crea el primer virus conocido de MS-DoS, *Brain*. Los investigadores creen que se escribió en Pakistán. Infectaba el sector de arranque de los disquetes de 360 KB.

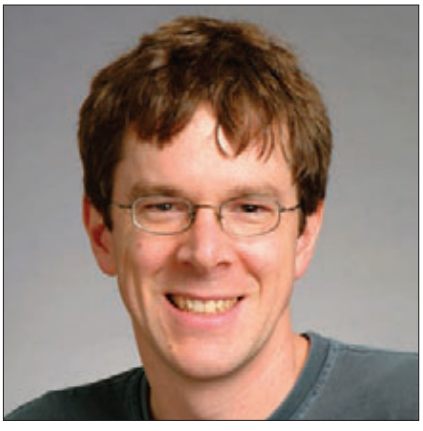


Figura 5. Robert Morris

1988: Robert Morris bloquea 6.000 ordenadores a través de ARPANET con su famoso virus, que lanzó, según sus propias palabras, de forma accidental. Se funda la CERT (*Computer Emergency Response Team*). Aparece el primer software antivirus, escrito por un desarrollador de Indonesia.

1989: Primer caso de ciberespionaje en Alemania Occidental. The Mentor lanza el manifiesto *Conscience of a Hacker*, que finaliza con una frase inquietante: *pueden detener a una persona, pero no pueden detenernos a todos*.

1990: Se lanza el grupo de apoyo *Freedom on the Internet*. Aparecen sofisticados tipos de virus como los polimórficos (que se modifican a sí mismos cuando se expanden) o los de multipartición (que infectan diversas zonas de una máquina). El First National Citibank de Chicago sufre el primer robo informático reconocido por una cantidad de 70 millones de dólares. El hacker *Dark Dante*, Kevin Lee Poulsen, es arrestado después de una búsqueda de 17 meses. Robaba secretos militares. Mitnick y Shimomura miden sus fuerzas.

1993: Se celebra la primera conferencia DefCon de hacking en Las Vegas. Se suponía que el evento era una celebración única para decir adiós a las BBS (obsoletas por la Web), pero resultó tener tal éxito que se convirtió en un evento anual. DefCon es la conferencia de hackers más importante del mundo, en la misma se reunen los hackers con conocimientos más avanzados con el fin de exponerlos al público, o de aplicarlos en las distintas competiciones que allí se realizan. En sus instalaciones hacen acto de presencia los agentes del FBI con el objetivo de llevarse nuevos *fichajes* para su plantilla (precisan a los mejores, y saben donde encontrarlos).

No obstante cabe aclarar, que como dijo Julio Cortázar: *la fama es una puta que se viste de verde*, y esta conferencia ha alcanzado tal reconocimiento que algunos hackers o *autodenominados* hackers, ven en ella una oportunidad para darse a conocer y conseguir aprobación entre el numeroso público. Esto es un arma de doble filo, porque tiende a una pérdida total del *espíritu hacker*.

1994: Hackers atacan a los sitios web federales de los EE.UU., incluyendo la CIA, el Departamento de Justicia, la NASA y la Fuerza Aérea. No fue la mejor forma de hacerse popular entre los estamentos militares. Vladimir Levin, el legendario líder de un grupo de hackers ruso, parece ser el cerebro del robo virtual de 10 millones de dólares del Citibank. Fue arrestado en Londres un año después y extraditado a EE.UU.

1995: El Departamento de Defensa de EE. UU. sufre 250.000 ataques en un año. Kevin Mitnick es arrestado bajo sospecha de robar 20.000

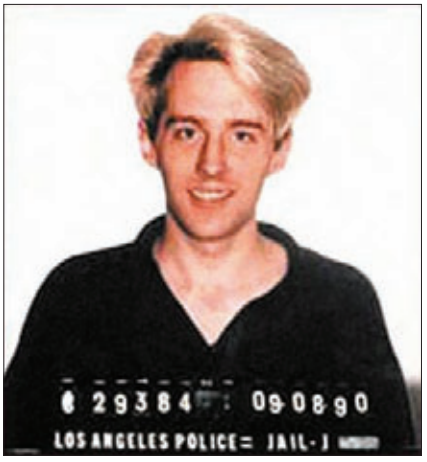


Figura 6. Kevin Poulsen

números de tarjetas de crédito. Es encontrado culpable un año después. La película *Hackers* llega a las pantallas de cine, difundiendo algunas ideas equivocadas sobre las actividades de los hackers.

1998: Network Associates emite un anuncio anti-hacker durante la Superbowl en los EE.UU. En él, dos técnicos de misiles soviéticos destruyen el mundo, inseguros de saber si las ordenes vienen de Moscú o de los hackers. Los hackers afirman haber entrado en el sistema de satélites militares y amenazan con vender secretos a los terroristas. Se crea la NIPC (*National Infrastructure Protection Centre*) con un presupuesto multimillonario.

1999: Nacimiento del software anti-hacking.

2000: Se producen ataques de denegación de servicio (DoS) sobre los grandes nombres de la Red.

2001: XP, *el Windows más seguro*, es crackeado antes de su lanzamiento.

2002: Bill Gates, el jefe de Microsoft crea Trustworthy Computing. El ISP CloudeNine es *hackeado hasta la muerte*.

2007: Se producen varios ataques phishing específicos contra entidades españolas especialmente agresivos a través de un kit que com-


Figura 7. Vladimir Levin

Figura 8. Mark Abene

prende a muchos bancos españoles. Se produce un ataque masivo a través de un mensaje que invita a visualizar un supuesto vídeo en Youtube. El reclamo en esta ocasión es reproducir el célebre incidente entre el Rey de España y el Presidente de Venezuela con la famosa frase: *¿Por qué no te callas?*.

2008: España ocupa el noveno puesto mundial en número de sistemas zombi, casi en empate técnico con Estados Unidos y Rusia. Se descubre una nueva forma de engañar a los servidores DNS para que den respuestas falsas, gracias a un fallo inherente del protocolo. No se han dado detalles técnicos sobre el problema. El descubridor Dan Kaminsky ha llevado en secreto su investigación durante meses, esperando a que todos los grandes fabricantes implicados se pusiesen de acuerdo para programar una solución y publicar los parches correspondientes.

Grupos de la élite del hacking

LEGION OF DOOM (LoD)

Este grupo de culto de los hackers se convirtió en un guardián con el lanzamiento de la empresa de seguridad ComSec. Algunos de los componentes que no entraron en el nuevo mundo de ComSec terminaron en prisión después de una prolongada guerra con su principal rival conocido como Masters of Deception.

COMPUTER UNDERGROUND

Un grupo casi esotérico dedicado a promocionar el libre intercambio de información, sobre todo con relación a la alta tecnología.

L0PHT

Fundado por un grupo de amigos en un loft de Boston -de ahí el nombre- L0pht alcanzó la prominencia cuando advirtieron a Washington que podrían paralizar Internet en media hora a menos que se mejoraran las medidas de seguridad del Gobierno. El grupo afirma que solamente hackea para detectar los *agujeros* que pueden presentar las empresas o los departamentos gubernamentales. Ha lanzado herramientas anti-hacking como AntiSniff, que controla las redes para evitar que se utilicen en ellas herramientas sniffer.

Entre sus obras más preciadas y conocidas se encuentra *lophtcrack*, un programa de fuerza bruta que es utilizado para crackear contraseñas.

MASTERS OF DECEPTION (MoD)

Famoso por haber violado la seguridad de Bank of America, AT&T y la NSA, los Masters of Deception vieron la luz después que Mark Abene (*Phiber Optik*) fuese expulsado de Legion of Doom. Los dos grupos se enzarzaron en una ciberguerra por un comentario racista sobre John Lee (MoD) y muchos creían que la batalla iba a remitir cuando la mayoría de los miembros de estos grupos fueron arrestados en 1993. MoD era un grupo dedicado al profundo conocimiento del sistema telefónico.

CULT OF THE DEAD COW

Este grupo de hacking lanzó el programa *Back Orifice* (troyano), una potente herramienta de hacking en Def Con. Una vez que se instalaba el programa en una máquina Windows 95/98, el hacker podía tener acceso remoto no autorizado al sistema.

YIHAT

Kim Schmitz lideró un grupo de hackers denominado YIHAT (*Young Intelligent Hackers Against Terrorism, Jóvenes Hackers Inteligentes Contra el Terror*), que afirmó haber tenido acceso a las cuentas bancarias de Osama Bin Laden en los días posteriores al 11 de septiembre de 2001. La afirmación se demostró falsa y el líder del grupo fue extraditado desde Tailandia a Alemania por una serie de delitos financieros.

CHAOS COMPUTER CLUB

El grupo alemán Chaos llegó a los titulares con una demostración televisiva en directo del robo de una cuenta bancaria, utilizando un simple control Microsoft ActiveX. El Club configuró un control ActiveX para que ejecutase una transferencia fraudulenta a un PC que ejecutaba una aplicación financiera. Microsoft señaló que muchos ejecutables podrían conseguir el mismo resultado. Actualmente está formado por más de 4000 miembros y es una de las organizaciones de hackers más importante de Europa.

Hackers memorables

Richard Stallman

Fue un estudiante de Harvard, consiguió un puesto en el laboratorio de inteligencia artificial del MIT. Odiaba la idea del software de propiedad privada, y por este motivo, más adelante creó la FSF (*Free Software Foundation*).

Después de retirarse de los laboratorios del MIT, allá por los 80, desarrolló un Sistema Operativo llamado GNU (*Gnu is not Unix*). También se encarga de la creación de muchas utilidades gratuitas para entornos UNIX.

Su filosofía acerca del software es una forma de vida que hoy en día es adoptada por una ingente cantidad de seguidores. Junto con todo su séquito es, sin duda alguna, uno de los mayores contribuidores de la comunidad Linux.

Esta filosofía se resume en cuatro principios o libertades, que él numeró del 0 al 3 (una pequeña broma de programadores):

- Libertad 0 : La libertad de usar el programa, con cualquier propósito.
- Libertad 1 : La libertad de estudiar cómo funciona el programa, y adaptarlo a tus necesidades. El acceso al código fuente es una condición previa para esto.
- Libertad 2 : La libertad de distribuir copias, con lo que puedes ayudar a tu vecino.
- Libertad 3 : La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie. El acceso al código fuente es un requisito previo para esto.

No obstante, yo me veo obligado a declarar mi punto de vista personal, y es que Stallman mantiene una ideología demasiado *axiomática*, lo que le hace creerse muchas veces poseedor de la *verdad absoluta*. Mientras admiro su fuerza y su poder de convicción, sus palabras inspiran a veces cierto egoísmo.

Figura 9. Dennis Ritchie

Figura 10. John Draper

En multitud de entrevistas se le puede ver declarando que *GNU es el sistema operativo, y Linux es su núcleo*, y así millones de veces. Un hacker real jamás se adentraría en un tema tan superficial mientras que su contribución ayude a la gente. Piénsese además que la definición formal de un sistema operativo es aquel programa que gestiona todos los recursos del sistema, manejando su hardware, gestionando la memoria y controlando los procesos que en él se ejecutan. Luego su último fin es brindar una interfaz al usuario. Por lo tanto, cabe aclarar que todas estas funciones están encargadas al núcleo y, en consecuencia, Linux es el Sistema Operativo, mientras que GNU es el conjunto de programas que lo complementan y proporcionan al usuario material con el que desarrollar sus actividades.

De un modo general es correcto decir que el sistema completo se denomina *GNU Linux*. Pero Stallman se ciega queriendo decir que Linux es una simple muleta en la que se apoya GNU mientras su núcleo propio, *Hurd*, no esté totalmente disponible.

Kevin Mitnick

Simplemente el más buscado por todos los cuerpos del FBI, sus acciones han sido ejemplo de mucha gente, algunos lo consideraban como *el chico perdido del ciberespacio*.

Con 10 años burló el sistema de seguridad de la Defensa de los Estados Unidos. Cazado a la vez por otro hacker llamado Tsutomu Shimomura después que un feliz Día de Navidad Mitnick penetrara sus ordenadores en busca de un software de OKI que hacía que su teléfono fuera invisible para los cuerpos del FBI.

Figura 11. Linus Torvalds

Los primeros ordenadores que fueron acariciados por las preciadas manos de Mitnick fueron los de las tiendas de *Radio Shack*. Conocido como *el Cóndor*, Kevin tuvo que realizar un tratamiento para intentar superar su adicción a los ordenadores.

Kevin Mitnick, ¿hacker o cracker?, por mucho tiempo éste ha sido un debate abierto...

Actualmente Kevin Mitnick es un reconocido consultor de seguridad, cuya empresa se llama *Mitnick Security Consulting, LLC* y cuya web se puede visitar en el siguiente enlace: *http://www.kevinmitnick.com*. Recomendamos ampliamente la lectura de sus dos mejores obras: *The Art of Deception* (El arte del engaño) y *El Arte de la Intrusión: La verdadera historia de las hazañas de hackers, intrusos e impostores*. Personalmente tengo la experiencia de haber leído dos veces este último y quedarme maravillado con las habilidades de los hackers de la vieja escuela.

Robert Morris

En el año 1988 puso en la red a un gusano que infectó más de 6000 ordenadores aprovechándose de una vulnerabilidad del servidor de correo *SendMail* a través de la red ARPANET. Tocó su primer ordenador cuando su padre, jefe del NCSC, le trajo una máquina directamente desde la NSA. Morris realizaba muchas de sus acciones desde una cuenta que poseía en los sistemas Bell y en los cuales consiguió acceso de *Super Usuario*.

Kevin Poulsen

Más conocido como Dark Dante se hizo famoso por el control que hizo de las llamadas que se realizaban a la emisora de radio KIIS-FM, así hizo que su llamada fuera exactamente la número *102* consiguiendo de esta forma un Porsche 944 S2.

Era poseedor de un TRS-80 y fue declarado culpable por la búsqueda de información secreta sobre los agentes del FBI.

Vladimir Levin

Saltó a la fama por su gran logro al robar 10 millones de dólares al prestigioso *Citibank*. Penetró en los sistemas bancarios utilizando el ordenador de su despacho personal en la universidad. Fue arrestado en Londres. Según declaraciones de Levin, uno de sus abogados era un agente del FBI. Algunos recuerdan a Vladimir como *una cabeza matemática*.

Mark Abene

Su apodo, Phiber Optik, fundador y miembro de *Masters of Deception*. Inspiró a miles de personas en los Estados Unidos a explotar los sistemas de la red telefónica. La revista New York calificó a Mark como uno de los 100 hombres más inteligentes de la ciudad.

Tuvo en sus manos bastantes máquinas, siendo solamente de su propiedad una TRS-80, las otras fueron:

- Apple II
- Timex Sinclair
- Commodore 64

Dennis Ritchie

Este excelente programador ha sido el creador del lenguaje C, uno de los más potentes que existen en el mundo de la programación. Trabajador de Bell Labs. En la actualidad trabaja en el desarrollo de un nuevo Sistema Operativo llamado *Plan 9* que es una evolución superior del sistema Unix, pero con una estructura totalmente diferente ya que se ha tenido que reescribir desde el principio.

John Draper

Su nick, *Capitan Crunch*. Su hazaña más destacable fue la de utilizar un silbato de los cereales Crunch (de ahí su nombre), para generar un sonido de 2.600 Hertzios el cual causaba el corte de los contadores de la red telefónica de Bell. John creó la primera *Blue Box*, ésta generaba el mismo tono y fue distribuida a muchísima gente que se aprovechó de su utilidad.

Linus Torvalds

Nacido en 1969, y estudiante de la Universidad de Helsinki, es uno de los hackers más respetados de la comunidad informática, a lo largo del año 1991 creó la primera versión del núcleo del innovador sistema operativo Linux. Obviamente, sin su hazaña hoy en día no estarías leyendo esta revista.

Conclusión

La historia del hacking es larga, desde luego demasiado como para poder describirla aquí, precisaríamos varios tomos para un completo acercamiento; pero nuestra intención era ofrecer un breve resumen de los acontecimientos más importantes que se han sucedido con el transcurso de los años. Invito a todos los lectores a que obtengan el libro *The Hacker Crackdown* de Bruce Sterling, el cual puede ser encontrado en formato PDF, gratuito y libre. Esto será para muchos un gran acercamiento a una etapa realmente crítica del hacking mundial.

Espero y esperamos que, algún alma con suficiente talento y curiosidad, pueda algún día pasar a formar parte de esta historia, y continuar así con una evolución que, aunque muchos no sean conscientes, es el pilar básico del funcionamiento global de la red de redes y el desarrollo tecnológico.