Hackers: Aspectos divulgativos de la seguridad en redes.

Nieves Carralero Colmenar.
IES Pedro Mercedes. Junta de Comunidades de Castilla-La Mancha. España.

Resumen

El nombre hacker – neologismo utilizado para referirse a un experto (gurú) en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes, sistemas operativos. En general, estos conocimientos los usan para conseguir retos intelectuales, pero no suelen causar daños.

En este artículo se muestran detalles de los hackers más famosos de la historia y los motivos por los cuales fueron un peligro para la seguridad en la redes de comunicaciones.

Paul Baran

- En la década de los 60 y 70 trabajó en el proyecto que desarrollaría ARPANET.
- La mayor aportación fue la creación de un sistema de codificación de la información en paquetes para facilitar su envío y su adaptación a la red. (Estableció los fundamentos de las redes de conmutación de paquetes).
- También extendió su trabajo de conmutación de paquetes al espectro inalámbrico.
- Comenzó a edificar lo que hoy en día es el navegador.
- Por su trabajo en las bases de lo que luego se llamaría Internet ha sido considerado como el primer hacker de la historia.

John Draper

- En los años 70 fue conocido como "capitán Crunch", porque descubrió que con un silbato de los cereales Crunch se podía hacer phreaking (phreaker: pirata telefónico).
- Este silbato generaba un silbido de 2600 Hz, frecuencia que usaba AT&T para cortar los contadores de sus teléfonos. Voz y señal usaban mismo canal.
- Con esto creó la "Blue Box", una caja que permitía generar el resto de frecuencias de AT&T y que permitió a mucha gente de todo el mundo hacer llamadas a larga distancia gratuitas.
- AT&T al descubrir esta vulnerabilidad, la corrige usando circuitos separados para voz y señales. Posteriormente llego la tecnología digital.

Kevin David Mitnick

- Uno de los hackers más famosos de los EE.UU en la década de los 80 y 90. Conocido como Cóndor.
- Fue procesado en varias ocasiones diversos delitos electrónico. (Con 16 años se salto la seguridad del sistema administrativo de su colegio).
- El arresto más famoso fue en 1995, del que se hicieron películas y libros [Takedown] [The Fugitive Game]
- Fue debido a que en 1994, con el auge de la telefonía móvil y buscando software para el control de teléfonos móviles logró entrar en un servidor de Tsutomu Shimomura.
- Además de software le robó correo electrónico, y otras herramientas de seguridad en Internet. Posteriormente, el software lo usó para lanzar ataques a empresas tan conocidas como Apple, Motorola o Qualcomm.
- Permaneció casi cinco años en prisión, estuvo bajo libertad condicional hasta enero de 2003, donde se le prohibió acceder a cualquier tipo de ordenador, teléfono móvil, televisión, o cualquier aparato electrónico que pudiera conectarse a internet.
- En la actualidad, se dedica a la consultoría desde la óptica

particular de la ingeniería social; considera que más allá de las técnicas de hardware y software en las redes, el factor determinante de la seguridad de las mismas es la capacidad de los usuarios de interpretar correctamente las políticas de seguridad y hacerlas cumplir.

Tsutomu Shimomura

Científico americano y experto en seguridad
Era considerado un hacker blanco porque cuando descubría alguna vulnerabilidad la ponía en conocimiento de la policía o la entidad competente en vez de difundirlo a otros hackers por la Red.
Pero en la década de los 90, tras un ataque a su computador por parte de Mitnick, Shimomura se propone como reto personal atraparlo. Trazó su ataque y fue el causante de la detección de Mitnick.
Sin embargo, se cree que Shimomura se paso al lado oscuro, ya que tuvo que invadir el sistema de la AT&T para poder rastrear las llamadas de Midnitnick y escucharlas, para luego dárselas al FBI.
Actualmente, experto en seguridad informática de la National Security Agency.

Ataque Mitnick – Simomura

- Al servidor atacado solo se podía acceder desde una maquina cliente, con lo cual empieza con una relación de confianza entre las maquinas internas.
- El sistema operativo del cliente y del servidor era Solaris, de Sun Microsystems, específicamente la versión 4 de éste (SunOS4) y tenía una red conectada permanentemente a Internet, en la que tenia registrado el dominio "toad.com“.
- Primero usó sentencias finger para chequear los usuarios típicos de un sistema, las relaciones de confianza, etc.
- Después, realizó un ataque de denegación de servicio DoS mediante SYN flood (inundación de paquetes), así consiguió bloquear en un primer lugar al servidor, silenciándolo y al silenciarse no puede generar ninguna advertencia.

- Una vez silenciado el servidor, fue a por la maquina cliente comprobando debilidades en la pila TCP/IP, de forma que mediante SYN/ACK fué aprendiendo como se establecen las conexiones en la relación de confianza.
- Una vez chequeado el protocolo TCP/IP, encuentra una forma de conectarse y mediante IP spoofing, consigue simular al servidor atacado que no da signos de funcionamiento y consigue abrir un puerto en el cliente.
- Para finalizar, una vez abierta una sesión, usando comandos del tipo #rlogin -l root" alcanzó el control de la maquina cliente y a partir de ahí pudo llegar al servidor.

Mark Abene

- Conocido por Phiber Optik
- Lideró el grupo de hackers “Master of Deception”.
- En Noviembre de 1989, hizo colapsar las computadoras de WNET, uno de los principales canales de televisión de la ciudad de New York, dejando un mensaje "Happy Thanks giving you turkeys, from all of us at MOD" (Feliz Día de Acción de Gracias a Uds. pavos, de parte de todos nosotros en MOD).
- Después de varios años como consultor de seguridad creo la empresa de consultoría de seguridad Crossbar.
- Abene actualmente trabaja como consultor independiente para varias organizaciones. Participa en publicaciones como New York Times, washington Post o Wall Street Journal, y da conferencias por todo el mundo sobre seguridad Informática.

Johan Helsingius

- Finés, su apodo era “julf”. Fue quién creó el correo anónimo. En 1995 era responsable del más famoso servidor de mail anónimo, llamado penet.fi
- El servidor remailer, no almacena los mensajes sino que sirve como un canal de re-transmisión de los mismos. Remailer re-envía los mensajes, sin dar a conocer la identidad del remitente original.

- Tuvo que cerrarlo, debido a que la Iglesia de la Cienciología le acusó de divulgar secretos suyos en la red. Un tribunal finlandés sentenció que debía revelar la dirección real del remitente de los mensajes, y Helsingius prefirió cerrar antes que hacerlo.
- Justificaba el servicio de remailer diciendo que mucha gente prefiere tratar ciertos temas, violencia doméstica, acoso sexual, derechos humanos, con confidencialidad en Internet.
- Tras cerrar penet.fi, formó parte del equipo de Eunet que llevó el primer enlace de Internet a Rusia.
- Actualmente es asesor en tecnología de varias empresas europeas como BaseN.

Chen Ing-Hou

- Taiwanes, creador en 1998 del virus CIH (sus iniciales), al que el llamó Chernobyl, en conmemoración del 13 aniversario de la tragedia ocurrida en la planta nuclear rusa.
  - Este virus es uno de los más peligrosos de la historia.
  - El virus CIH destruye archivos en el disco duro. Borrando los primeros 2048 sectores y formateándolos.
- Reescribe la BIOS en los ordenadores con memoria de tipo Flash BIOS sobre-escribible y que se encuentre configurada como write-enabled.
- Su virus fue motivado por una venganza en contra de los que llamó "incompetentes desarrolladores de software antivirus".
- Actualmente trabaja como experto en Internet Data Security.

Sir Dystic

- Josh Buchbinde , es su nombre real.
- Autor de muchas herramientas hackers. Las más conocida es el administrador remoto “back orifice”.
- En concreto, “back orifice” lanzado en 1998, fue infectada con el virus CHI y ello dió motivo a que Sir Dystic anunciara que desarrollaría un antivirus denominado CDC Protector y otro que protegería a los sistema de los troyanos, denominado CDC Monitor.
- Back orifice es un programa informático diseñado para la administración de sistema remoto. Permite controlar un equipo que ejecuta el sistema operativo Microsoft Windows desde una

ubicación remota.
- Actualmente participan en conferencias hackers y en publicaciones y tertulias televisivas sobre aspectos relacionados con seguridad informática.

El Gran Oscarín

- Español, autor del troyano Cabronator, y muchos otros.
- Debido a este destructivo troyano, fue detenido en 2003 por la Guardia Civil en el marco de una operación llamada CLON.
- Pasó cerca de dos años en la cárcel.
- «Admito que se trata de buscar trabajo. Soy totalmente autodidacta porque nunca he estudiado informática. Los planes de estudio no me convencen porque enseñan muchas cosas inútiles. Yo he aprendido desde casa todo lo que sé, e intento que alguien me contrate, porque me parece injusto tener que pasar mi vida con contratos de seis meses».
- Creador de numerosos programas informáticos de hacking y cracking. Chivaror, bombita, anonimizame, psecreta, O-Mail
- ***Hacker o Lammer?.***

SOCIEDAD DE LA INFORMACION

www.sociedadelainformacion.com

Edita:

Director: José Ángel Ruiz Felipe

Jefe de publicaciones: Antero Soria Luján

D.L.: AB 293-2001

ISSN: 1578-326x