HACKERS, CRACKERS Y OTROS ...

NÉSTOR DARÍO DUQUE MÉNDEZ*, ALONSO TAMAYO ALZATE*

Todos los días se escucha, se lee, se comenta sobre los riesgos que representan esos seres "extraños" para nuestros sistemas de información, para nuestra privacidad y para nuestra tranquilidad. Asociamos los riesgos a factores externos, a personas que desde afuera vulneran nuestra seguridad. Algunos llegan a sostener que sí han violado la seguridad de grandes organizaciones, incluso dedicadas a la seguridad de países, ¿qué podremos decir entonces de las nuestras?; son muchas las personas que piensan que es preferible olvidarnos de Internet y ganar tranquilidad en nuestros sistemas. Pero qué son?, Qué hacen?, Qué métodos utilizan?, Qué los motiva?, Cómo protegernos?, ... Algunos de estos interrogantes trataremos de resolverlos en este artículo.

Múltiples son las situaciones que se pueden presentar: hurtos de identidad, ladrones de contraseñas, mercaderes de correo electrónico, etc. Recuerde que todo lo que usted hace en línea (conectado a una red, por ejemplo Internet) deja una pista. Cuando se visitan los sitios Web estos monitorean sus viajes, gustos y preferencias, grabando esa información (incluso las contraseñas) en archivos de texto llamados *cookies* o galleticas y guardándolas en su propia computadora. Además, los navegadores de Internet, guardan un historial de los últimos sitios y archivos visitados y los almacenan en carpetas para hacer más rápida las siguientes vistas al mismo lugar.

Ha recibido en alguna ocasión mensajes por correo electrónico invitándolo a visitar sitios u ofreciéndole un producto en particular?. De dónde salió esa información? Cuando se accede a un sitio Web a través de una computadora personal, ésta puede guardar un registro de cuando fue la visita, que examinó, el nombre y la dirección IP del visitante, la versión del explorador y el último sitio anteriormente visitado, por lo menos. Muchos sitios en Internet exigen que antes de ingresar por primera vez, el usuario se registre y suministre una serie de datos;

---

* Profesores Universidad Nacional de Colombia, Sede Manizales

cuando usted lo hace, ésta información se almacena en bases de datos y normalmente se comparte con otros sitios de similar preferencia. Si no es vital para su actividad, no proporcione información veraz y cuando lo sea, asegúrese del sitio a quien se la está proporcionando. Alguna información quedará en poder del propietario del sitio (dirección IP, por ejemplo). Incluso algunos sitios Web, podrían vender aquella información.

No confíe en sus contraseñas de Windows. No importa cuantas herramientas de seguridad aplique a Windows 95 o a Windows 98: contraseñas de BIOS (realmente es de la máquina), claves de usuario, protector de pantalla con clave; un *snoop* medianamente inteligente y conocedor del sistema puede apoderarse de su sistema en minutos. Quien tenga acceso a su máquina (y recuerde, no quiere decir físicamente, puede ser a través de la red), puede ingresar como usuario por defecto y con poco conocimiento del sistema, buscar y decodificar el archivo de contraseñas usando un software especial que se encuentra gratuitamente en Internet. Ahora, si usted usa la misma clave para entrar a Windows, para entrar a la red local, para entrar a los buzones públicos de correo, para sus cuentas Internet, ya ha entregado su privacidad. Ya obtuvo su conclusión?

Hackers

Quiénes son los hackers? La palabra se deriva de hack, término utilizado en inglés para describir las patadas de los jugadores de rugby. Esas mismas patadas eran utilizadas por los técnicos para 'arreglar' las cajas telefónicas y como esa era su función, empezaron a ser llamados hackers.

Hacker es un término usado que se puede interpretar de diversas formas, para algunos los hacker son astutos, intrépidos programadores y para otros, son personas que intentan romper la seguridad de los sistemas computacionales. Luego, cuando ocurrieron las primeras invasiones a la privacidad por vía telefónica, los intrusos heredaron ese nombre; algunos emplean el sobrenombre «pirata informático», pero eso no hace justicia a la idea original.

Para Eric Raymond, compilador del libro *The New Hacker's Dictionary*, un "good hack" es una inteligente solución a problemas de programación y "hacking" es la acción de realizar tal cosa.

Las siguientes características pueden calificar a un hacker, según Raymond:

- "Una persona que disfruta aprendiendo detalles de un lenguaje de programación o sistema y como aprovechar sus posibilidades, al contrario de la mayoría de los usuarios que prefieren aprender sólo lo imprescindible.

- Una persona que disfruta realmente programar; programa en forma entusiasta, casi obsesiva.

- Una persona capaz de apreciar el valor del "hackeo".

- Una persona que programa bien y rápidamente.

- Una persona que es experta en un lenguaje de programación, en un programa en particular o en un sistema operativo.

- Experto o entusiasta de cualquier tipo. Se puede ser un «hacker astrónomo», por ejemplo.

- El que disfruta del reto intelectual de superar o rodear las limitaciones de forma creativa.

- 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. Este último término es para aquellos que desean resquebrajar seguridades o realizar actos maldadosos."

Pero casi universalmente el término hacker se usa para quienes intentan irrumpir en los sistemas de computación. Típicamente este tipo de hacker pueden ser expertos programadores o ingenieros con suficiente conocimiento técnico como para hallar los puntos débiles en un sistema de seguridad.

Los hackers son personas que poseen vastos conocimientos y ansiosos de incrementarlos, invierten tiempo aprendiendo sobre sistemas y lenguajes de programación, poseen amplia experiencia en sistemas operativos como Unix, Linux, etc., e implementaciones TCP/IP, estudian sobre temas relacionados con seguridad en los computadores. El entrar a un sistema es para ellos un reto, una gran emoción. El hacker se deleita explorando tanto a nivel interno como externo, buscando malas configuraciones, errores y hoyos de seguridad en los sistemas operativos, en los que posteriormente van a incursionar, su reto es ingresar al sistema. Definir la frontera

entre el hacker y el científico es sumamente complejo, mientras tanto la comunidad se debe beneficiar de sus conocimientos y ponerlos en práctica.

Es contra la *ética hacker* alterar datos diferentes a los necesarios para no dejar pistas (logs, etc.). Ellos no necesitan o desean destruir datos como los maliciosos crackers, solo quieren explorar el sistema y conocerlo más, tienen un constante anhelo y sed de conocimiento que se incrementa e intensifica con sus progresos. Dice Gary Robson, de la revista Computers, Security & Internet, "Si llamas hacker a quien ama la tecnología, a quien tiene conocimiento de cómo ésta trabaja, entonces yo me siento orgulloso y agradecido de ser llamado Hacker". En el medio de los sistemas de información ser llamado hacker es un cumplido, entre la gente del común normalmente es un peyorativo.

Termina un hacker inspirado en la constitución o libro de la ley del hacker, realizado por "the mentor", expresando: "Si tener hambre de conocimiento, es ser criminal, sí lo soy. Si querer aprender cosas y educarme, o sea, tener acceso a toda la información que necesite, sin tener que pagar por ella, sí lo soy; si esto es un crimen, entonces soy un criminal y estoy orgulloso de ello. Nosotros no dañamos a nadie, no fabricamos armas, no traficamos con drogas, nuestro único crimen es la curiosidad, y lo que nadie nos perdona es ser más listos que los demás, porque siempre logramos nuestro propósito; pueden detener a uno de nosotros, pero nunca podrán detenernos a todos".

Refiriéndonos a la ética de los hackers, podemos recordar que fue mejor formulada por Steven Levy en 1984, en el libro *Hackers: Heroes of the Computer Revolution*, las principales tesis que esboza son las siguientes:

- "El acceso a las computadoras y a cualquier cosa que pudiera enseñarte algo sobre cómo funciona el mundo, debería ser ilimitado y total.
- Basarse siempre en el imperativo de la práctica.
- Toda la información debería ser libre.
- Desconfianza a la autoridad, promover la descentralización.
- Los hackers deberían ser juzgados por sus acciones y habilidades, no por falsos criterios como grados, edad, raza o posición social.
- Se puede crear arte y belleza con la computadora. Las computadoras pueden cambiar tu vida para mejorarla."

Algunos han tratado de encasillar a los hacker en algunos perfiles: "adolescentes de sexo masculino, introvertidos, de clase media - alta (no cualquiera puede pagar un acceso a Internet) y con una fuerte resistencia al control tecnológico", pero consideramos que estas características son excluyentes y no reflejan el universo.

Crakers

Quiénes son los Crakers? El término cracker es otorgado a quien rompe la seguridad de un sistema; fue acuñado hacia 1985 por hackers, en defensa contra la inapropiada utilización del término por parte de periodistas, como, "Es alguien que irrumpe en un sistema de computación, usualmente en una red, desviando o violando claves o licencias en programas de software, o en otros casos abre intencionalmente brechas en la seguridad del sistema. Puede hacer esto por beneficio económico, maliciosamente e incluso con propósitos altruistas o por un simple desafío. Algunos rompen, entran y hacen visible los puntos débiles del sistema de seguridad del sitio."

Para otros, un cracker es quien irrumpe en un sistema violando o adivinando las claves de los usuarios. La mayoría son jóvenes adolescentes, delincuentes, maliciosos que buscan obtener emoción destruyendo o alterando datos en un sistema. Los crackers tienden a reunirse en grupos pequeños, muy secretos y privados. Algunos crackers a menudo se definen a sí mismos como hackers, la mayor parte de los auténticos hackers los consideran una forma de vida inferior.

En la misma revista Computers, Security & Internet, el autor plantea que algunas personas que se autoproclaman como hacker, se inician haciendo un sencillo fisgoneo alrededor de los sistemas, pero luego realizan acciones vandálicas, borran datos, venden información y rompen los sistemas. Esos se deben llamar cracker.

Según Raymond, los hacker generalmente desaprueban a los cracker. Aunque se supone que cualquier hacker auténtico ha realizado algún tipo de crackeo y conoce muchas de las técnicas básicas, se da por descontado que cualquier que haya pasado la etapa de iniciación ha desterrado el deseo de hacerlo y solo lo hará por razones prácticas, por ejemplo, si es necesario pasar por alto algún sistema de seguridad para completar alguna tarea concreta.

Por lo tanto, hay mucho menos en común entre el mundo de los hackers y el de los crackers de lo que el lector normal cree, generalmente confundido por el periodismo

sensacionalista. Los hackers se consideran a sí mismos algo así como una elite, en la que los méritos se basan en la habilidad, aunque suelen recibir amablemente a nuevos miembros. Por lo tanto, hay una parte de satisfacción del ego en considerarse a sí mismo un hacker.

Entre las variantes de crackers maliciosos están los que realizan **Carding** (Tarjeteo, uso ilegal de tarjetas de crédito), **Trashing** (Basureo, obtención de información en cubos de basura, tal como números de tarjetas de crédito, contraseñas, directorios o recibos) y **Phreaking** o **Foning** (uso ilegal de las redes telefónicas).

Queda claro que existen grandes diferencias entre los hackers y los crackers. ¿Pero por qué para el común de la gente son prácticamente lo mismo? Fundamentalmente por el papel de los medios de comunicación que han desfavorecido a los hackers, al hablar sin conocimiento de causa sobre los asuntos en los que ellos se ven envueltos.

Mecanismos usados por los hackers para acceder a los sistemas informáticos sin autorización.

- Urgonear en los basureros. Hace poco una película basaba toda la estrategia de intromisión informática en encontrar en los basureros físicos de la empresa, las pistas que pudiesen acercarlos con los sujetos a penetrar. A través de la reunión y análisis de los gustos, lugares donde compran, llamadas efectuadas, cuentas de correo de internet, etc., se puede llegar a conocer la vida de una persona y sus preferencias.

- Entrar a los sistemas y ejecutar Finger. Si tengo el nombre de un usuario en un sitio, tengo la mitad de los que necesito para proceder a realizar mi trabajo, decía un hacker.

- Usar los servicios de Chat. Son muchos los hackers que van a estos sitios a buscar usuarios inocentes para "confesarlos" sobre donde trabajan, a que se dedican, averiguan sobre la importancia de la empresa donde laboran y mucho más, localizan sitios que representen para ellos gran interés y generalmente toman la palabra y retan constantemente a los demás, o en algunos casos se hacen pasar por inocentes novatos esperando consejos de alguien que conozca mucho, aplicando lo que se conoce en este medio como ingeniería social.

¿Qué tecnología se debe desarrollar par garantizar la seguridad del futuro inmediato?

⇒ Seguridad de acceso a nivel del Sistema Operativo.

⇒ La encriptación y la firma electrónica ante la posibilidad de interceptaciones de información en la red.

⇒ La biometría (lectores de retina, huellas digitales, etc.). Aunque ya existen manuales de cómo violar éstas seguridades.

⇒ Sistemas de comunicación sin cables.

¿Qué recomendaciones personales deben ser tenidas en cuenta?

- Establecer políticas de seguridad en las empresas, no sólo a través de cortafuegos (firewalls) en Internet, sino también dentro de sus redes privadas.
- Claves diferentes para los distintos sitios a que tenga acceso.
- Consejos para claves o contraseñas: use combinaciones alfanuméricas, mayúsculas y minúsculas, no use palabras, ni secuencias de letras o números (ejemplo 123), no use fechas de nacimiento, números de sus tarjetas, que su clave no sea el mismo nombre de usuario y use por lo menos 8 caracteres.
- Cambiar periódicamente su clave.
- No permitir accesos simultáneos con el mismo login.
- Bloqueo de cuenta luego de tres intentos fallidos al digitar la clave.
- Para sus programas de correo o el acceso a otros sitios, generalmente es posible permitir que Windows automáticamente recuerde la clave, sin que sea necesario que usted la digite, esto permite que cualquier usuario en su máquina entre con sólo tener su login. Evite esto.
- Los passwords son claves de seguridad, por lo tanto deben ser sólo de su conocimiento

- No conectarse a internet directamente a través de la red local.
- Emplear un sistema operativo de red lo más seguro posible, aprovechando las herramientas que provee.
- Dar a conocer a los usuarios de la empresa los riesgos y mecanismos que usan, para que por inocencia o desconocimiento no sirvan en bandeja de plata la seguridad de la organización a otros. Hay que evitar hacer atractiva la empresa para los intrépidos crackers u otros.
- No entregar información personal, a menos que sea necesario.
- Borrar los rastros y las galleticas (lo puede hacer utilizando un editor de texto), pero recuerde que esto hará más lento su trasegar por aquellos sitios.
- Es necesario revisar con frecuencia el registro de ingresos (logs).

Glosario de términos empleados en este artículo, según el diccionario de Jargon.

Backdoor. Puerta trasera de un sistema informático, un mecanismo del software que permite entrar evitando el método usual. Son fallas en el diseño del sistema.

Bombas Lógicas. Programa que se activará en un momento determinado llenando la memoria de la computadora. Programa orientado a colapsar el sistema de correo electrónico, este se suele llamar mailbombing.

Boxes: Aparatos electrónicos o eléctricos cuya finalidad es el phreaking, emula la introducción de monedas en teléfonos públicos. Las más conocidas son la bluebox, la redbox y la blackbox.

Bug, Hole, Agujero. Se trata de un defecto en el software, generalmente en el Sistema Operativo que permite la intrusión de los hackers.

Caballos de Troya. Programas que simulan ser otros para así atacar el sistema. 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 ejecutarsen despiertan un virus que se introduce en el sistema. El troyano más famoso es sin duda el Back Office, un troyano que utiliza las puertas traseras, apareció el 8 de agosto de 1998. Incluso aparece la versión para linux desarrollada por CDC (Cult of the Death Cow. Culto a la vaca muerta).

Carding. Uso fraudulento de tarjetas de crédito o sus números. Ello incluye la generación de nuevas tarjetas de crédito.

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

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. Son programas que se utilizan para desproteger o sacar los passwords encriptados de programas comerciales, pudiéndose utilizar éstos como si se hubiera comprado la licencia. Quienes los distribuyen son altamente perseguidos por las entidades que protegen los productores de software.

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 la IBM, Microsoft, Empresas Telefónicas, etc.

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

Fuerza Bruta. Forma poco sutil de entrar en un sistema y consiste en probar distintas contraseñas hasta encontrar la adecuada. Requiere mucho tiempo y para ello se emplea un crackeador que desencripta un archivo y obtiene las claves del archivo de passwords empleando las palabras del diccionario, etc.

Gusanos. También conocidos como Worms. Programa que se copia a si mismo llegando a crear miles de replicas del mismo y destruyendo la información del sistema.

Hacking. Entrar en forma ilegal y sin el consentimiento del propietario en su sistema informático. No conlleva a la destrucción de datos ni a la instalación de virus. También lo podríamos definir como cualquier acción encaminada a conseguir la intrusión en un sistema (ingeniería social, caballos de Troya, etc.)

Ingeniería social. Es una técnica por la cual se convence a alguien por diversos medios para que proporcione información útil para hackear o para beneficiarnos. Requiere grandes dosis de psicología y explota la tendencia de la gente a confiar en sus semejantes.

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.

Phreakers (crackers telefónicos). Distinguidos por que utilizan líneas telefónicas para sus actos. Este término mezcla las palabras inglesas phone (teléfono) y freak (monstruo o 'bicho raro'). Phreaking. Acciones tendientes a utilizar fraudulentamente las líneas telefónicas, es decir, 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 de 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.

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, su misión es fisgonear la red en busca de claves o puertos abiertos

Snoop. Fisgoneador, mirón. Persona que está pendiente de lo que pasa en la red y esperando encontrar información importante o huecos de seguridad.

Spams. No es un código dañino, pero sí bastante molesto; es un programa que ejecuta una orden repetidas veces. Ampliamente utilizado por empresas de marketing, usando el correo electrónico para enviar sus mensajes en forma exagerada.

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

Trashing. Recoger basura. Se trata de buscar en la basura (física o informática), información que pueda ser útil para hackear.

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

BIBLIOGRAFÍA

Jargon File 4.2.0. Enero 31 del 2000.

The New Hacker's Dictionary (Third Edition). Eric S. Raymond (compiler), MIT Press, 1996

Revista Jumping. Septiembre de 1997.

Revista Computers, Security & Internet. Abril de 1.997.

Revista PcWorld. Año V Número 55. Septiembre 1998.