LOS *HACKERS* Y OTROS HABITANTES INDESEABLES DEL CIBERESPACIO

*José Ebert Bonilla**
Corporación Universitaria Unitec

El presente artículo busca reivindicar el concepto de hacker como aquella persona que tiene como propósito primario la adquisición de conocimiento técnico y que, con él, intenta colocar la tecnología al servicio de la sociedad sin costo. Por otra parte, se centra en los crackers, *quienes son los que se dedican a romper los sistemas de seguridad de los sistemas informáticos.*

[**Palabras** claves: hacker, cracker, ética hacker.]

1. El hacker

Con diez mil gigas por banda ancha,
ratón en popa a toda mecha,
no corta la red, sino vuela,
un hacker bergantín;
bajel pirata que llaman,
por su cerebro el Temido
en toda la red conocido
hasta por el mismísimo jovilin.[1]
—José de Espronceda

*Ingeniero de Sistemas de la Universidad Católica de Colombia. Especialista en Gerencia de Tecnología de la Escuela de Administración de Negocios. Magíster en Ciencia de la Información y Telecomunicaciones de la Universidad Distrital de Bogotá. Jefe de los Programas de Tecnología en Sistemas y Tecnología en Electrónica y Telecomunicaciones de la Corporación Universitaria Unitec. Correo electrónico: jbonilla@unitec.edu.co

En la actualidad no es extraño haber sufrido, haber oído o saber de alguien a quien, mientras se encontraba conectado a Internet, le saquearon la información, le alojaron un virus, le dañaron la información a tal punto que la volvieran irrecuperable o, en el peor de los casos, hicieron que el computador iniciara el formateo sin alguna explicación aparente.

La evolución de la tecnología de interconectividad de redes de computadores ha hecho posible que se transmita y comparta información en tiempo real, lo cual está llevando a la humanidad a un estado de paranoia; además, se sabe que no todos los que se encuentran conectados a la red lo hacen con fines pulcros y éticos. Existen algunos usuarios que tienen otros propósitos que no son para nada plausibles.

En el libro *Hacker Beware*,[2] su autor, Eric Cole, plantea: "…mientras no se entienda cómo los atacantes rompen y entran en los sistemas y por qué lo hacen, se tendrá que invertir mucho tiempo en lograr la seguridad de un sistema, dado que actualmente se usa una gran variedad de ataques para comprometer dichos sistemas."[3]

Asimismo, Cole señala en la parte introductoria de su libro que: "Cualquier nueva tecnología, siempre presenta dos aspectos, uno positivo y otro negativo. El aspecto positivo

está representado en las tremendas oportunidades de negocios; la parte negativa es el enorme riesgo de seguridad, el cual ha poseído a la mayoría de compañías, pero sólo unas pocas están totalmente concientes del daño potencial."[4]

Por otro lado, se sabe que el elemento más preciado actualmente es la información y los computadores y sus conexiones hacen que ésta fluya de manera eficiente a fin de soportar los procesos, productos, servicios y decisiones de las empresas. Por lo tanto, se hace necesario que se cuenten con elementos que permitan preservar esa información inalterada, disponible y en ciertos casos lejos del conocimiento de algunas personas.

Mientras que las empresas hacen ingentes esfuerzos por desarrollar mecanismos de seguridad informática, por otro lado existen grupos de personas dedicadas a encontrar la forma de vulnerar esos sistemas de seguridad. A estos últimos se les ha dado el mal nombre de *hackers*.

Históricamente este problema se inició el 15 de enero de 1990; ese día sucedió la caída del sistema de la compañía norteamericana de comunicaciones AT&T, quedando inoperativa la red de larga distancia de los Estados Unidos. Sobre este hecho, comenta Bruce Sterling: "Fue un extraño y grave suceso de proporciones gigantescas; sesenta mil personas se quedaron sin teléfono. Durante las nueve largas horas de desesperados trabajos que llevó restablecer el servicio, unas setenta millones de llamadas no pudieron realizarse."[5]

Después de horas, los ingenieros de software empezaron a comprender qué había causado el fallo; si técnicamente era difícil de entender, más lo era para la gente del común. Teniendo en cuenta esto, la AT&T dio una explicación a sus clientes, más o menos satisfactoria; pero no lo fue así para las autoridades e ingenieros que tenían información confiable proveniente del *underground,*[6] la cual aseguraba que la falla había sido provocada desde el exterior por personas técnicamente bien preparadas; por lo tanto, debió haber sido un *hacker*. Hasta ese momento las empresas de servicios telefónicos nunca habían presentado fallas de tal magnitud y uno de los grandes estandartes de mercadeo de AT&T era la calidad de su servicio. A partir de este instante se dio inicio a una de las más sonadas operaciones policiales de los Estados Unidos en el ciberespacio; ésta tuvo como nombre "la caza de *hackers*."

Respecto a cuál es el concepto de *hacker,* Claudio Hernández, en su libro *Hackers,* plantea lo siguiente:

> (…) parece que este acrónimo se vincula muy especialmente a los llamados *hacks* o, dicho de otra manera, así se llaman los golpes secos que efectuaban los técnicos de telefonía cuando intentaban reparar alguno de sus aparatos; estos golpes secos recibían el nombre de "hachazos" o en el argot ingles *hacks* y es más que probable que quienes lo hacían se denominaban *hackers*.
>
> (…) Un *hacker* es una persona, sin importancia de edad, con amplios conocimientos informáticos o electrónicos, que a su vez descubre la intolerancia de algunos organismos por proteger ciertas cosas o intereses. Un *hacker* no sólo habita en los suburbios de una gran red como lo es Internet, ni navega continuamente entre los discos duros de los ordenadores, aunque se les conocen en estos entornos mayoritariamente, los *hackers* también fisgonean sistemas fuera de una CPU.[7]

Por su parte, Terry Bernstein y otros[8] comentan: "… el término *hacker* fue originalmente referido a usuarios quienes fueron pioneros de la revolución del computador, especialmente durante los 70 y principios de los 80. Ellos desarrollaron software que era distribuido libremente a la comunidad de usuarios de computador, que por ese entonces era reducida; a menudo prestaban acceso a computadores (de forma gratuita) cuando nadie los estaba usando; por aquellos días la obtención de tiempo de computador era difícil y costosa";[9] mas el concepto ha tomado una connotación extremadamente negativa y es regularmente usado para referirse a vándalos electrónicos y criminales a través del computador.[10]

Originalmente la palabra *hacker* estaba destinada a aquellas personas que habían adquirido grandes conocimientos y que daban solución a problemas de cómputo a través de segmentos de código muy ingeniosos (a los cuales se les denominaba *hack*); así, la fuerza que los impulsaba era siempre la búsqueda del conocimiento. Por lo tanto, es claro que el *hacker* real tiene unos objetivos muy distintos a todos aquellos que merodean por la red tratando de romper sistemas.

Uno de los más famosos *hackers* de los Estados Unidos es Kevin D. Mitnick, alias El Cóndor, quien fue arrestado por última vez el 15 de febrero de 1995, acusado de haber entrado a uno de los computadores más seguros de la unión americana. Como los demás *hackers,* tenía obsesión por obtener conocimientos de informática y electrónica; pero su mejor herramienta era la ingeniería social,[11] la cual usó con todo su potencial. Para él, el eslabón más débil de la seguridad es el ser humano y éste fue siempre al que atacó. En su libro *Controlling the Human Element of Security:*

The Art of Deception[12] presenta las diferentes metodologías que a lo largo de su trayectoria usó para obtener la información necesaria para poder ingresar a los sistemas sin necesidad de emplear sofisticadas herramientas de software o hardware.

Pero ¿cómo es el aspecto físico de un *hacker*?, ¿se puede hacer un bosquejo de sus rasgos más significativos? Muy seguramente cuando se escucha la palabra *hacker*, viene a la mente de muchos la imagen de un adolescente ojeroso, con los ojos enrojecidos por no haber dormido durante algunos días y que se la ha pasado frente a una pantalla de computador desarrollando sus labores. Este es el estereotipo que se ha vendido, pero la realidad es otra. Un *hacker* puede ser cualquier estudiante o persona con conocimientos de informática o electrónica, el cual tiene una vida normal con amigos y novia y sale a divertirse.[13]

Como se dijo en párrafos anteriores, el término fue degradado y ahora se usa para denominar a todos aquellos que de una u otra forma violentan los sistemas informáticos y las redes de comunicación. Estos individuos se han especializado a tal punto que se tiene un amplio repertorio de ellos. En la actualidad son personas dedicadas a timar a otras personas, robar secretos industriales, números de tarjetas de crédito y bancos, o cometer actos ilegales que atentan contra los bienes y servicios de personas y empresas. Dependiendo de su actividad han tomado diversos nombres dentro de los que se pueden presentar los siguientes:

- *Cracker*
- *Phreaks*
- *Virus writers*
- *Pirates*
- *Cypherpunk*
- *Anarchists*
- *Cyberpunk*
- *Script-lidies*
- *Lamers*

2. Perfil psicológico de un hacker

Estudios realizados han intentado dar un perfil psicológico de las personas que se dedican a cometer delitos en el ciberespacio. Algunas de las características son las siguientes: en la mayoría de los casos son personas solitarias, falsas, embaucadoras, que tienen un gran delirio de grandeza y, por lo general, son desadaptados sociales. No obstante, debe tenerse en cuenta que, actualmente, son personas que tienen una gran capacidad para interrelacionarse, más que conocimientos técnicos. De tal forma, aunque saben un poco más que el común de las personas, no alcanzan al nivel de conocimientos amalgamados por un *hacker*. Por otro lado, hay que ver que el intruso utilizará cualquier artilugio que le haga más fácil su acceso y posterior ataque. Dicho en otras palabras, el atacante no sólo usa herramientas tecnológicas sino que se valdrá de todo lo que tenga a su disposición.

Respecto al tema del perfil psicológico, se hizo contacto a través de correo electrónico con Bruce Sterling y se le preguntó si actualmente era posible establecer un perfil psicológico de los hacker; su respuesta fue contundente: "I am sure this has been tried many times, but hackers are not all the same."[14] Y es claro, cada *hacker* tiene una forma de actuar y de pensar, por lo tanto, es muy complicado tratar de establecer un patrón psicológico que los cobije a todos.

Las razones por las cuales un *hacker* infringe la ley son múltiples; éstas van desde la venganza hasta las razones económicas, pasando por necesidades de aceptación, búsqueda de respeto, publicidad, idealismos, héroes protectores, venganza, curiosidad, aprendizaje, anarquía, espionaje industrial, espionaje nacional o razones políticas. En algunas ocasiones una persona puede llegar a infringir la ley a través de un computador sin saberlo, pero la ignorancia no es un argumento válido de defensa.

3. Los crackers

Los *cracker* son los encargados de romper los sistemas se seguridad y efectuar la comisión de los ilícitos. Claudio Hernández dice acerca de los *crackers:*

> (…) en realidad son *hacker*, pero con unas intenciones que van más allá de experimentar en casa. Por cualquier motivo su *crack* puede extenderse como la pólvora.
>
> Un *cracker* se dedica única y exclusivamente a "reventar" sistemas, ya sean estos electrónicos o informáticos. Alcanza el éxtasis de satisfacción cuando logra [su objetivo] y esto se convierte en una obsesiva compulsión. Nunca tiene bastante y aprovecha la oportunidad para demostrar al mundo que sabe más que nadie.[15]

Por su parte, N. Sukhai[16] define a un *cracker* como una persona que irrumpe dentro de los sistemas computacionales de otras personas a fin de suplantarlo o intentando causarle daño o perjuicios.

Una de las cosas que sí caracterizan a este tipo de atacantes es que, una vez logran el acceso no autorizado a un sistema, inmediatamente lo publican. Lo interesante de estos individuos es que en la realización del ilícito tratan de dejar la menor cantidad de evidencias digitales posibles; de tal manera que, si tienen el conocimiento y la experticia suficiente, intentarán por todos los medios técnicos borrar las posibles huellas.

Los ataques que pueden efectuar estos individuos se clasifican en dos tipos: activos y pasivos. Los ataques pasivos se caracterizan porque el *cracker* se dedica a mirar la información, pero no realiza nada sobre ella, sólo la visualiza. Por otra parte los ataques activos son los que causan daño sobre la información o sobre los dispositivos que la contienen.

Dentro de los ataques que se le pueden efectuar a un sistema informático, los siguientes son algunos ampliamente conocidos en el ámbito de la seguridad informática: exploit, virus, caballos de Troya, gusanos, *bugs, trapsdoor, snack overflow,* bombas lógicas, falsificación, usurpación, *snnifers, spoofing, spam* y negación del servicio.

En la actualidad es muy usual que los *crackers* usen herramientas que no dejan rastros al realizar los ilícitos; a éstas se les denomina herramientas antiforenses, las cuales ayudan a que se cometa el delito y a borrar todas las posibles huellas de éste, logrando que el *cracker* se vuelva casi imperceptible. Dentro de las labores ejecutadas por las herramientas antiforenses están las de inhabilitar los *logs* (archivos de registro de actividad en el sistema), borrar los registros que se generan en el momento de realizar el acceso fraudulento al sistema, cambiar los tiempos de acceso o lograr el borrado real de archivos.[17] Cuando se usa este tipo de herramientas por parte del atacante, se complica la labor del investigador forense digital; es casi como llegar a cometer el crimen perfecto.

4. Motivaciones para realizar un ataque

En primera instancia lo que hace un *cracker,* después de lograr el acceso, es crear puertas traseras *(back door)* poder ingresar aparentemente de forma oculta y sin ser detectados. Aparte de las razones para que un *cracker* efectúe un ataque y que ya se enunciaron en forma general, aquí se presentan algunas más particulares:

- Probar sus capacidades o conocimientos recientemente adquiridos.
- Iniciar un profundo y contundente ataque sobre la red desde un equipo al que ha ganado acceso.
- Obtener información, lo cual es una de las principales razones; esto lo hace a través del monitoreo y almacenamiento de las teclas digitadas, observando el comportamiento del usuario durante largos períodos de tiempo, usando *sniffers* sobre la red y exfiltrate de datos desde la fuente. Esto normalmente se realiza a través de herramientas tales como *keylogger*[18] y *rootkit*.[19]
- Destruir los datos que están almacenados en un equipo. Para tal caso, generalmente se emplean bombas lógicas que han sido dejadas con anterioridad, luego de ingresar por una puerta trasera.

Aquí es determinante la forma en la cual el *hacker* accede al sistema; la idea que el atacante lleva es la de no ser detectado; para tal fin debe establecer una metodología que lo haga casi imperceptible, con lo cual se asegura la consistencia de los resultados.

Algunas formas para lograr lo anterior podrían ser las siguientes: enviar pequeños fragmentos de tráfico que se ha capturado, evitando almacenar archivos en el disco duro del equipo comprometido; otra forma puede ser almacenar archivos en el disco, pero usando técnicas de ofuscamiento, lo cual hace que la labor del investigador forense digital sea más complicada. Si el sigilo y la cautela son usados apropiadamente, las técnicas de investigación forense digital nunca serían usadas en el sistema comprometido, porque la intrusión nunca sería detectada.

5. Ética hacker

Dentro de la múltiple literatura que hay sobre el tema, se habla de una ética *hacker*. La mayoría de las actividades ejecutadas por el hombre tienen su ética, con el fin de que sus miembros tengan una autorregulación y la actividad *hacker* no es la diferencia. Steve Levy[20] dedica el segundo capítulo de su libro a este tema. Otra fuente de referencia a este tema es el artículo "Is there a Hacker Ethic for 90's Hacker?", escrito por Steven Mizrach, quien refiere lo comentado por Levy pero contextualizándolo a los años 90. Respecto a la ética original de los *hacker* dice:

> The code demonstrates the shared core values necessary for people to practice within the professional community. And it enables the public and the government to have some degree of trust for the profession. Some of these codes may be very ancient and formalized, such as the Hippocratic Oath sworn by physicians. Others may be very modern and legalistic, like the code of ethics for applied or academic anthropologists. Some ethical systems may be "underground," (such as the Pirates' Code of 18th century buccaneers or Mafia oaths of loyalty) enabling members of subcultures or groups to survive, cooperate, and escape outsiders. Yet others like the original Hacker Ethic are very informal and simple–rules of thumb to live by.[21]

La última frase es muy diciente, toda vez que nos indica que es informal y simple, lo cual va en total concordancia con las pretensiones de los *hacker,* como lo es el hacer que las cosas sean simples y sin ninguna restricción. Además, la última parte indica que son reglas rápidas de consulta y para la vida; básicamente, cómo sobrevivir en el mundo *underground* sin ser capturados.

Algunos de los principios que establece la ética *hacker,* son:

1. *Hands on Imperative:* el acceso a los ordenadores y a cualquier cosa que pueda enseñarte algo sobre el funcionamiento del mundo, debe ser ilimitado y total.
2. *Information Wants to Be Free:* toda información debe ser libre.
3. *Mistrust Authority:* desconfía de la autoridad, promociona la descentralización.
4. *No Bogus Criteria:* los hackers deben ser juzgados por sus trabajos, no por criterios irrelevantes como títulos, edad, raza o posición.
5. *You can create truth and beauty on a computer:* puedes crear arte y belleza en un ordenador.
6. *Computers can change your life for the better:* los ordenadores pueden mejorar tu vida.

Como se puede apreciar, la ética *hacker* presenta seis conceptos sobre los cuales debe discurrir la vida de un *hacker* real. Estas concepciones éticas son las que guiarán todo su accionar y la forma como interpreta su mundo, que gira en torno a los sistemas informáticos.

6. Conclusiones

- La acepción que normalmente se le da a la palabra *'hacker'*, no es la más adecuada y corresponde más a la palabra *'cracker'*.
- Los *hacker*, por medio de su conocimiento, buscan poner a disposición de la sociedad la tecnología informática sin costo.
- Es necesario que se tenga en cuenta que los *cracker* no están fuera de las organizaciones, sino que en la mayoría de los casos están al interior de las mismas.

- Es necesario preparar a los empleados para evitar que les apliquen ingeniería social y así el posible atacante obtenga la información necesaria para ingresar al sistema computacional sin ser autorizado pero con *password* válido.
- Al igual que otras actividades, el *hacking*[22] tiene su propia ética.
- Las personas que quieran dedicarse a la seguridad informática, necesariamente deben conocer a profundidad a sus contrincantes: los *crackers*.
- El uso de herramientas antiforenses por parte de los *crackers* los hace casi imperceptibles y letales.

Referencias bibliográficas

1. Bernstein, Terry. *Internet Security for Business*. Nueva York: John Willey & Sons, 1996.
2. Bonilla O., José Ebert. "La ingeniería social: el uso de la mayéutica en la era digital." *Computerworld*. No. 303 (mayo 15-mayo 28 de 2003).
3. Cole, Eric. *Hackers Beware*. Indianapolis (EE.UU): New Riders Publishing, 2001.
4. Hernández, Claudio. Hackers. *Los clanes de la red 2000*. [PDF] Disponible en internet en la dirección: idefix.eup.uva.es/Manuales/Seguridad/Hackers-1.0.pdf.
5. Hollinger, Richard. "Hackers: Computer Heroes or Electronic Highwaymen?" *Computer & Society*. Vol. 21, No. 1 (junio 1991).
6. Levy, Steven. *Hackers: Heroes of de Computer Revolution*. Nueva York: Delta, 1996.
7. Mitnick, Kevin y William Simon. *Controlling the human element of security: The Art of Deception*. Indianapolis (EE.UU): Wiley Publishing, Inc., 2002.
8. Mizrach, Steven. *Is there a Hacker Ethic for 90s Hackers?* [en línea]. The CyberAnthropology Page. Disponible en internet en la dirección: http://www.fiu.edu/~mizrachs/hackethic.html
9. Sterling, Bruce. *La caza de hackers: ley y desorden en la frontera electrónica*. S.l: s.d., 1999.
10. Sukhai, Nataliya. "Hacking and Cybercrime." Ponencia en la 1st Annual Conference on Information Security Curriculum Development. Kennesaw, (EE.UU.), 8 de octubre de 2004.

Otra bibliografía relacionada con el tema

1. Gibson, William. *Neuromante*. Buenos Aires: Minotauro, 1984.
2. Stoll, Clifford. *El huevo del cuco: una asombrosa historia real sobre el tenebroso mundo del espionaje informático*. Barcelona: Planeta, 1990.

Notas

[1] Fragmento de la Canción del Pirata. Fue modificada por un anónimo. Disponible en Internet en la dirección: www.fortunecity.es/ilustrado/infinito/40/textos/pirata.htm

[2] Eric Cole, *Hackers Beware*. Indianapolis: New Riders Publishing, 2001, p. 21.

[3] Traducción libre.

[4] Traducción libre.

[5] Bruce Sterling, *La caza de hackers: ley y desorden en la frontera electrónica*. S.l: s.d., 1999.

[6] La palabra *'underground'* significa literalmente subterráneo o submundo. En este texto se usa para identificar un bajo mundo que se desarrolla al margen de la actividad pública oficial.

[7] Claudio Hernández, *Hackers: los clanes de la red 2000*. Este libro apareció en el sitio web idefix.eup.uva.es/Manuales/Seguridad/Hackers-1.0.pdf. Es un documento de distribución libre y gratuita.

[8] Terry Bernstein, *ét al., Internet Security for Business*. Nueva York: John Willey & Sons, 1996.

[9] Traducción libre.

[10] Richard Hollinger, "Hackers: Computer Heroes or Electronic Highwaymen?" *Computer & Society*. Vol. 21, No. 1 (junio de 1991).

[11] José Ebert Bonilla, "La ingeniería social: el uso de la mayéutica en la era digital." *Computerworld*. No. 303 (mayo 15-mayo 28 de 2003).

[12] Kevin Mitnick y William Simon, *Controlling the Human Element of Security: The Art of Deception*. Indianapolis: Wiley, 2002.

[13] Steven Levy, *Hackers: Heroes of de Computer Revolution*. Nueva York: Delta, 1996.

[14] Bruce Sterling, Correo electrónico al autor, 7 de enero de 2007.

[15] Claudio Hernández, *óp. cit.*

[16] Nataliya Sukhai, "Hacking and Cybercrime." Ponencia en la 1st Annual Conference on Information Security Curriculum Development. Kennesaw, (EE.UU.), 8 de octubre de 2004.

[17] Con la frase borrado real de archivos, se quiere significar que cuando se hace un borrado normal de archivo, este no se erradica del disco, lo único que se hace es borrar el apuntador que permite su ubicación física en el disco; por lo tanto es necesario que se borre tanto lógica como físicamente para lograr un borrado real del mismo.

[18] Software que se encarga de registrar las pulsaciones que se realizan sobre el teclado para almacenarlas en un archivo y enviarlas a través de Internet a un correo electrónico específico.

[19] Un *rootkit* es una herramienta, o grupo de ellas, que tiene como finalidad esconderse a sí misma y a otros programas, procesos, archivos, directorios, llaves de registro y puertos que permiten a un intruso, atacante o cracker mantener el acceso a un sistema para remotamente comandar acciones o extraer información sensible, a menudo con fines maliciosos o destructivos.

[20] Steven Levy, *óp. cit.*

[21] Steven Mizrach, *Is there a Hacker Ethic for 90's Hackers?* [en línea]. The CyberAnthropology Page. Disponible en internet en la dirección: http://www.fiu.edu/~mizrachs/hackethic.html

[22] El *hacking* se entiende en este texto como la técnica o arte de encontrar los límites y las vulnerabilidades de los productos, aparatos y servicios digitales de informática o comunicaciones y compartirlo con otros y/o los fabricantes mismos de esos productos.