Hacker ético vs. delincuente informático. Una mirada en el contexto colombiano

Federico Iván Gacharná G.

Recibido el 26 de febrero de 2009. Aprobado el 30 de abril de 2009

Resumen
El presente artículo aborda el singular mundo del Hacking Ético, buscando establecer que un hacker no es un delincuente tal y como se define en el imaginario general, haciendo especifica la disertación para el contexto colombiano. Con este fin se recurre al planteamiento de dos perfiles que son producto de la experiencia y trayectoria del autor, para concluir que en Colombia hay talento humano para formar grandes profesionales en Hacking Ético, pero hace falta una formación clara que evite que los participantes distorsionen el propósito y terminen irrumpiendo en la ilegalidad.

Palabras clave
Hacking ético, delito informático, ciber crimen, seguridad informática, hackers.

Abstract
This article is about the amazing world of ethical hacking, making clear that hacker is not a criminal, this is a popular thinking about that, but is not true; Placing the discussion in Colombian context. For this approach to the use of two profiles that are a product of experience and track record of the author: Concluding that there is human talent in Colombia to train highly qualified specialists in ethical hacking, but without good educational offer that prevents participants confuse the purpose and falling into illegally.

Key words
Ethical Hacking, cyber crime, computer crime, computer security, hackers

I. Introducción

Históricamente cuando las sociedades buscan desestimular una actividad, se usan los medios de comunicación para "satanizar" un concepto, una profesión o un oficio. Es el caso, que se está presentando con el término HACKER. En los eventos donde se reúnen expertos en seguridad de la información, es común que se genere discusión acerca de la diferencia entre

los perfiles de comportamiento de un Hacker Ético y un delincuente informático. A partir de la definición de la palabra "Hacker" es posible concluir que se trata de una persona entusiasta o apasionado por la tecnología[1], en ese sentido, todos en algún momento hemos sido hackers cuando usamos de forma recursiva los diferentes elementos tecnológicos que están a nuestro alcance. Sin embargo, dentro del ambiente informático cuando se habla de hacker se asocia a la idea de una persona que "golpea" una red de información, llevando los elementos tecnológicos al límite para hacerlos fallar. Sin embargo "la tarea de un hacker no es dañar, es conocer". Este interesante concepto fue acogido por toda una comunidad de expertos, quienes tienen dentro de sus reglas (Rios, 2003) mantener el anonimato y la discreción de sus actividades; pero al interior de esta comunidad surgieron personas que se desviaron de los principios y propendieron, no por el conocimiento, sino esencialmente y entre otras cosas por su propio beneficio económico, dando lugar a que los medios de comunicación distorsionaran el concepto y se creara la imagen de que "todo Hacker es un delincuente".

Es importante, antes de continuar, clarificar los conceptos aquí tratados. HACKING ETICO, es una actividad que incluye diversos ataques a redes de computadores en ambientes controlados donde los responsables de los sistemas a atacar han sido previamente informados y han autorizado los mismos con el fin de establecer el estado de inseguridad de su sistema y conocer detalladamente sus vulnerabilidades y que son practicados por profesionales en Seguridad Informática. También se conocen como Penetration Test, Vulnerability Test o simplemente Pentest. Cualquier otra forma de comisión de ataques contra un sistema informático se considera ilegal y en ocasiones delito y es perseguido por la Ley. DELITO: Toda conducta regulada en la Ley que sea típica, antijurídica y culpable. DELINCUENTE: Persona que viola una conducta establecida en la Ley como delito. DELITO INFORMÁTICO: se da cuando en la comisión de un delito se utiliza un recurso computacional o dispositivo electrónico como fin o como medio.

A continuación, se profundizará sobre el perfil de un hacker ético, en contraste con los rasgos de comportamiento de un delincuente informático y la visión que desde la perspectiva colombiana se tiene.

II. Perfil de un hacker ético

Cuando se quiere definir un perfil es necesario hablar de qué se hace y para qué se hace, dentro de un entorno particular o general, según sea el caso. En este caso, el perfil de hacker ético se definirá desde el entorno colombiano.

En Colombia aun no se reconoce el hacking ético a nivel profesional, por lo tanto, se pueden reconocer tres áreas laborales en las cuales es posible encontrar un hacker. En primer lugar los profesionales que se encuentran laborando con las empresas de seguridad informática que son reconocidas en el país. En segundo lugar están aquellos que trabajan en las áreas de sistemas de las empresas. Finalmente se encuentran aquellos que se dedican a otras actividades comerciales y aprovechan los espacios fuera de sus trabajos para practicar el hackerismo.

Sin embargo, aunque aun no se cuenta con el reconocimiento debido, se sabe que un profesional con los conocimientos requeridos para hacer hacking resulta bastante costoso, además de ser un grupo al que muy pocos pueden acceder con la intención de solicitar sus conocimientos en la solución de un problema específico, o la asesoría y tutoría para formar nuevos hackers. En cuanto a este último punto, resulta necesario establecer que dentro de la cultura hacker es un principio no publicitarse como hacker, así como el innegable hecho de no contar con espacios académicos que permitan formar nuevos hackers, los cuales facilitarían la interacción entre los profesionales ya posicionados y aquellos que de manera empírica desean profundizar.

Una de las falsas ideas que más ha entorpecido el desarrollo del hacking ético en Colombia es el estigma de qué todo hacker es un delincuente, por lo tanto, las instituciones educativas evitan estos temas por temor a que sus estudiantes ataquen sus sistemas o para evitar posibles consecuencias de índole legal.

Con base en esto, se pueden reconocer tres grandes grupos de hackers éticos en Colombia, así:

- Los afortunados. Son aquellos que se encuentran vinculados a empresas de seguridad, particulares o del estado, que cuentan con conocimientos a profundidad en los distintos temas; se relacionan con sus iguales, desarrollan y dan uso a su propio software, laboran, generalmente, como consultores, podría decirse que fungen como los "PhD" de la seguridad, sus aportes se encuentran en la frontera del conocimiento, por sus ocupaciones es muy complejo acceder a su conocimiento directo, en general, son personas de un alto nivel académico, humano, profesional, que cuentan con reconocimiento nacional e internacional. Además,

[1] Para más información, consultar: Erich Reymond, Richard Stallman

una de las características más significativas es su compromiso en la lucha, altruista, contra la pornografía infantil y la pedofilia.

· Los entusiastas. Este puede considerarse uno de las más numerosos grupos de hackers éticos, está compuesto por personas con educación superior en diferentes áreas (no necesariamente afines con sistemas) o por aquellos apasionados por la tecnología que no han logrado acceder a una universidad, usan software desarrollado por otros, trabajan en el área de los sistemas o actividades afines, y cuentan con conocimientos empíricos pero a los que les falta profundidad y la rigurosidad científica propia de la disciplina. A este grupo pertenecen personas que desean tener más tiempo para dedicar al hacking, sin embargo, deben trabajar para sobrevivir, su mayor fuente de información es la Internet, y dada su baja educación formal deben luchar con la barrera idiomática si se tiene en cuenta que la mayoría de la información se encuentra en inglés y alemán. En resumen, tienen la pasión por el hacking pero adolecen de una cultura amplia que les permita llegar a ser los grandes investigadores aunque no se desaniman y se mantienen en constante estudio.

· El semillero. Son todos aquellos que se apasionan con el tema, desean saber sobre hacking porque puede ser una opción de vida, lograr un mejor nivel social o simplemente porque se trata de un tema que se halla de moda. Su curiosidad sobre el tema es tan grande que buscan por diferentes medios aprender, están desinformados sobre lo que verdaderamente significa ser un hacker. En este grupo se ubican aquellos que demandan la creación de espacios que los formen y les brinden claridad sobre el hacking.

En general, se puede decir que al primer grupo pertenecen profesionales de excelentes capacidades económicas, que participan en encuentros internacionales como BlackHat o DefCon, asesoran multinacionales o gobiernos, dentro de su experiencia se destacan certificaciones importantes como CISM, CISA, CISSP, SANS, EC-COUNCIL, tienen dominio de diferentes idiomas, son profesionales de éxito en el área de seguridad de la información. El segundo grupo esta conformado por profesionales, cuya ocupación principal no es el hacking o la seguridad, pero que tienen habilidades, que aunque incipientes, son fundamentales para que logren formar parte del primer grupo, además de contar con una diferencia fundamental para su desarrollo, como lo es el trabajo en equipo y el interés permanente por el estudio. Finalmente están los semilleros, formados por aquellos que quieren llegar a ser, pero su norte no es muy claro, además de las dificultades que afrontan para lograr acceder a los expertos y a los recursos necesarios para un exitoso desempeño en el campo de la seguridad, todo esto aunado a la falta de integración con sus similares.

III. Perfil de un delincuente informático

Un delincuente informático es aquella persona que tiene un perfil muy similar a los expertos en hacking ético, pero que por razones diversas se dedican a servir a organizaciones delincuenciales, la subversión o intereses económicos propios. Aquellos que pertenecen a organizaciones delincuenciales, generalmente, se dedican al fraude financiero, cuyas victimas son entidades bancarias o aseguradoras, las cuales no denuncian el delito, sino que hacen sus propias investigaciones, evitando que se conozca lo sucedido para proteger su derecho al buen nombre. De otra parte, los que se encuentran al servicio de la subversión se dedican a la extorsión, robando información de las empresas y exigiendo dinero a sus victimas para recuperar sus datos. Otra modalidad es el "aseguramiento" de la informaron con encriptación y borrado seguro de datos. Finalmente, están los delincuentes independientes que tienen como principal modo de fraude el carding, consistente en la clonación de tarjetas de crédito, fraude por Internet y todo tipo de defraudación de fluidos[2].

Los anteriores corresponden a criminales cuyo fin es el bien económico, pero existe otro tipo de delincuentes informáticos, para quienes el dinero no es un fin; su propósito esta en la búsqueda de nuevos retos y la emoción de vulnerar sistemas no autorizados convirtiéndose en su mayor incentivo. Estos personajes no se mantienen en la clandestinidad, en ocasiones hacen grupos y comunidades para imponerse nuevos retos. Sus ataques más comunes son: webdefacement, para alterar la imagen electrónica de organizaciones, intrusión a sistemas de información que cuentan con altos niveles de seguridad (gobierno, militares, bancos), cambian claves, interceptan señales de comunicación para hacer escucha pasiva, dejando en muchos casos sus firmas, ya que no son conscientes que están cometiendo un delito, generalmente son "personajes traviesos" que pueden terminar incriminados en procesos legales.

[2] A.256 CPC- **Defraudación de fluidos.** El que mediante cualquier mecanismo clandestino o alterando los sistemas de control, se apropie de energía eléctrica, agua, gas natural, o señal de telecomunicaciones, en perjuicio ajeno, incurrirá en prisión de 1 a 4 años y en multa de 1 a 100 SMLMV.

En apariencia este segundo grupo no es malicioso, en otras palabras no buscan hacer daño, sino demostrar sus capacidades, aunque lo hagan de una forma incorrecta. Sin embargo, hay que aclarar que este tipo de actividades son perseguidas por la ley y puede conllevar a sus practicantes a ser detenidos, enjuiciados y encarcelados.

IV. Conclusiones

· El término "Hacker", hace alusión una persona apasionada por el conocimiento en profundidad de alguna técnica u oficio. También hace referencia al interés en llevar al límite de su funcionamiento dispositivos de todo tipo o llevarlos a cumplir funciones para las cuales no fueron creados originalmente.

· No es correcto asociar este término a ningún tipo de señalamiento delincuencial, pues la actividad del Hacking no está concebida como una actividad ilegal desde su principio conceptual.

· Desde el momento mismo en que se diferencia Hacking de Hacking Ético, se presenta una realidad deformada puesto que el Hacking es en esencia ético; esta diferenciación no debería existir.

· En general, se puede decir que el Hacking Ético en Colombia, se divide en tres grupos: los "afortunados", profesionales de excelente posición social y económica, que se destacan en el área de seguridad de la información. Los "entusiastas" cuyas habilidades, trabajo en equipo e interés creciente por la formación los proyecta como el futuro del Hacking Ético en Colombia. Finalmente los semilleros, con quienes existe un compromiso de oferta educativa de calidad y democrática.

· En contraste con lo anterior, la delincuencia que recurre a la tecnología como fin o como medio, se ira reduciendo en la medida en que al incrementarse los hackers con fines éticos, se estará cerrando el campo de acción para este tipo de conductas.

· Finalmente, si se logra que en Colombia se cree la conciencia de que a través de la formación en técnicas de Hacking, se contribuirá para una sustancial reducción en la comisión de delitos tecnológicos, se estará aportando significativamente al progreso social.

Se recomienda a los lectores consultar los siguientes grupos que ya están aportando en la formación e integración de los hackers éticos en Colombia: www.hackingetico.info, www.hackstudio.net,www.low-noise.org,www.dragonjar.org, www.hackerscololmbianos.org; Otros Enlaces de interés: www.cursohacker.com ESPAÑA, www.hackersporcristo.com GUATEMALA

V. Referencias

[1] Ríos, R. H. (2003). *La Conspiración Hacker.* 1ª.Ed. Bnos Aires. Longseller

Federico Iván Gacharná G. *Ingeniero de Sistemas, U. Autónoma de Colombia, Especialista en Seguridad Informática, Diplomado en Docencia Universitaria, Master en Seguridad Informática, U. Ouberta de Catalunya (en curso), Director del Área de Seguridad de la Información, Corporación Universitaria Minuto de Dios (UNIMINUTO), organizador del Congreso Nacional de Hacking Ético, CEO Comunidad Hackers Colombianos, docente, investigador. Experto en inteligencia informática, cómputo forense y hacking ético. Federico.gacharna@hackingetico.info*