HACKER ETICO vs. DELINCUENTE INFORMATICO

- *Una mirada en el contexto Colombiano* -

Federico Iván Gacharná Gacharná[1]

Resumen— Este artículo aborda el apasionante mundo del Hacking Ético, buscando precisar que un hacker no es un delincuente, como es el imaginario general, ubicando la disertación en el contexto colombiano. Para esto se recurre al planteamiento de dos perfiles que son producto de la experiencia y trayectoria del autor: Concluyendo que en Colombia hay talento humano para formar grandes profesionales en Hacking Ético, pero hace falta una oferta educativa que evite que los participantes confundan el propósito y terminen cayendo en la ilegalidad.

Palabras Claves— 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.

Index Terms— Ethical Hacking, cyber crime, computer crime, computer security, hackers

I. INTRODUCCIÓN

Históricamente cuando las sociedades desean desestimular una actividad se usa los medios de comunicación para "satanizar" un concepto, una profesión o un oficio. Es el caso, que en mi concepto, se esta viviendo 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. Desde el concepto de la palabra "Hacker" es posible ver que se trata de una persona entusiasta o apasionado por la tecnología[2], es decir, 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 produce el imaginario de una persona que "golpea" una red de información, llevando los elementos tecnológicos al limite para hacerlos fallar, "*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 [1] el mantener el anonimato y la discreción de sus actividades; pero en esta comunidad surgieron personas que se desviaron de los principios y propendieron, no por el conocimiento, sino por su propio beneficio económico, dando lugar a que los medios de comunicación distorsionaran el concepto y se creara el mito 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 será perseguido por la Ley. DELITO: Toda conducta regulada en la Ley que sea rípica, 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 Colombia 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.

[1] 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, U. Minuto de Dios, Organizador del Congreso Nacional de Hacking Ético, CEO Comunidad Hackers Colombianos, Docente, Investigador. Experto en Inteligencia Informática, Computo Forense y Hacking Ëtico.
e-mail: Federico.gacharna@hackingetico.info

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

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 ya se encuentran posicionadas en el país, en segundo lugar están aquellos que trabajan en las áreas de sistemas de las empresas y finalmente, aquellos que se dedican a otras actividades comerciales y aprovechan los espacios fuera de sus trabajo para prácticar el hackerismo.

Sin embargo, aunque no se le da el reconocimiento debido, si se sabe que un profesional con los conocimientos requeridos para hacer hacking resulta bastante costoso, además que son un grupo al que muy pocos pueden acceder, para solicitar sus conocimientos en la solución de un problema específico, o en la asesoría y tutoría para formar nuevos hackers, principalmente, porque dentro de la cultura hacker es un principio no publicitarse como hacker, en segundo lugar porque no se dan espacios académicos que permitan formar nuevos hackers, que faciliten la interacción entre los profesionales ya posicionados y aquellos que de manera empírica desean profundizar.

Uno de los mitos 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 mismos estudiantes ataquen sus sistemas o para evitar posibles dificultades legales.

Entonces se puede 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 conocen en profundidad los temas, se relacionan con sus iguales, usan 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, 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 mas 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, tienen conocimientos empíricos pero les falta la profundización y rigurosidad científica requerida, desean tener mas tiempo para dedicar al hacking, sin embargo, deben trabajar para sobrevivir, su mayor fuente de información es Internet, deben luchar con la barrera idiomática ya que la mayoría de la información se encuentra en inglés y alemán, en resumen, tienen la pasión por el hacking pero siempre les falta algo para llegar ser los grandes investigadores, sin embargo 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 para tener un mejor nivel social o simplemente porque está de moda, su curiosidad sobre el tema es tan grande que buscan por diferentes medios aprender, están desorientados o desinformados sobre que significa ser un hacker, son todos aquellos que demandan la creación de espacios que los formen y les de 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 hoja de vida se destacan certificaciones importantes como CISM, CISA, CISSP, SANS, EC-COUNCIL, tienen dominio de diferentes idiomas, en general, 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 acceder a los expertos y a los recursos necesarios para un exitoso desempeño en el campo de la seguridad, todo esto aunado a su falta de integración con su propio grupo.

III. PERFIL DE UN DELINCUENTE INFORMATICO.

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, que por lo general no denuncian el delito, sino que hacen sus propias investigaciones, evitando que se conozca lo sucedido para proteger su derecho al buen nombre. Por 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 encripción y borrado seguro de datos. Finalmente, están a 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[3].

Los anteriores corresponden a criminales cuyo fin es el bien económico, pero hay otros delincuentes informáticos, para quienes el dinero no es un fin, su búsqueda de nuevos retos y la adrenalina de penetrar sistemas no autorizados es 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. En mi concepto, este segundo grupo no son maliciosos, es decir, 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 pueden 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 se refiere 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 a este término *ningún* tipo de señalamiento delincuencial, pues la actividad del Hacking no está acompañada de ilegalidad en cuanto su principio conceptual, más en la interpretación que el público en general le da, se acompaña de distintos estereotipos contrarios a la realidad. Desde el momento mismo en que se diferencia Hacking de Hacking Etico, 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 Etico 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 Etico 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, debe comenzar a preocuparse ya que al incrementarse los hackers con fines éticos, se estará cerrando el campo de acción para este tipo de conductas.

Finalmente, si se logra en Colombia, crear conciencia 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 a un importante 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.com, más información en Facebook grupo Hackers colombianos. Otros Enlaces de interés: www.cursohacker.com ESPAÑA, www.hackersporcristo.com GUATEMALA

REFERENCIAS.

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

[3] A.256 CPC- **Defraudación de fluídos.** 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.