UNIVERSIDAD DE PANAMÁ
CENTRO REGIONAL UNIVERSITARIO DE VERAGUAS

2º CONGRESO REGIONAL DE INVESTIGACIÓN Y EXTENSIÓN

PONENCIA: ***HACKERS: PERSONALIDAD E INTENCIONES.***

EXPOSITOR: ***RAÚL ENRIQUE DUTARI DUTARI.***

FECHA: ***31 DE AGOSTO DE 2005.***

HORA: ***02:30 P. M.***

LUGAR: ***AUDITÓRIUM DEL CENTRO REGIONAL UNIVERSITARIO DE VERAGUAS.***

DIRIGIDA A: ***PROFESORES UNIVERSITARIOS, PROFESIONALES Y ESTUDIANTES QUE PARTICIPARON EN EL EVENTO.***

DURACIÓN: ***20 MINUTOS.***

OBJETIVOS GENERALES

1. Elevar el nivel de cultura informática de los participantes.

2. Despertar el interés de los participantes en la temática de la seguridad informática.

3. Diferenciar los tipos de Hackers que podemos identificar.

OBJETIVOS ESPECÍFICOS

1. Describir las acepciones que tiene el concepto Hacker,

2. Enunciar el código de ética Hacker,

3. Diferenciar los roles en que se desenvuelven los Hackers,

4. Mencionar algunos hechos históricos importantes donde han participado Hackers.

5. Categorizar las acepciones dadas al concepto Hacker.

Resumen De La Ponencia

Hacker es un individuo al que se define de muchas formas:

- Hay quienes los definen como tecno-terroristas, capaces de desactivar las redes de computadoras de los gobiernos, en el momento que consideren más conveniente.

- Otras personas los consideran como piratas o corsarios informáticos, en capacidad de robar cualquier información que se encuentre inadecuadamente protegida en la Internet.

- En otros entornos se les considera como personas que simplemente destruyen la información de otras personas o instituciones por el mero placer de hacer daño a los demás.

- También hay quienes les consideran como una subcultura que se dedica a la búsqueda constante de información que consideran, debe ser pública y de acceso ilimitado por todos.

En realidad, el hacker verdadero sigue un código de ética más o menos definido, que esencialmente se resume en:

- El ser humano tiene el derecho a conocer la información pública, así como los mecanismos que se siguen para recolectar y procesas dicha información.

- El ser humano tiene la responsabilidad de evitar dañar a sus otros individuos mientras ejerce su derecho a conocer la información.

- El ser humano tiene la responsabilidad de compartir el conocimiento y las habilidades que sirven para revelar la función de los mecanismos de procesamiento de información, mientras guarda estrictamente la confidencialidad de la información que ha sido confiada o entregada a dichos mecanismos por partes privadas.

- El ser humano debe decir NO a la sociedad de la información, SI a una sociedad informada.

Personas como Bill Gates, Steven Wozniak y Steven Jobs, entre otros, fueron considerados hackers en su momento, y actualmente son empresarios de éxito y fama mundial. ¿Entonces, los hackers son un peligro?

Esta ponencia pretende ofrecer al auditorio una panorámica objetiva de los que es el movimiento hacker desde sus inicios, hasta la actualidad.

TABLA DE CONTENIDOS

1. ACEPCIONES DEL CONCEPTO HACKER.

Hacker es un término que ha nacido de la mano con el nacimiento de Internet. Acepta una muy diversa gama de de acepciones, entre ellas tenemos:

- **Tecno-terroristas:** capaces de desactivar las redes de computadoras de los gobiernos, en el momento que consideren más conveniente.

- **Piratas o corsarios informáticos:** en capacidad de robar cualquier información que se encuentre inadecuadamente protegida en la Internet.

- **Destructores de información:** Personas que destruyen la información de otras personas o instituciones por el mero placer de hacer daño a los demás.

- **Subcultura:** Se dedica a la búsqueda constante de información que consideran, debe ser pública y de acceso ilimitado por todos.

- **Expertos en seguridad:** Se dedican a buscar fallas de seguridad en software de empresas importantes, que luego les pueden contratar como asesores.

2. ORIGEN DE LOS HACKERS

Según **[HE01]** el movimiento hacker original surge en el Instituto Tecnológico de Massachussets -MIT-, entre 1955 y 1965. Eran los tiempos de los primeros programadores de computadoras Mainframes.

Muchos de los nombres célebres de la informática formaron parte de esos grupos de Hackers cuando jóvenes, entre ellos encontramos a:

- **Dennis Ritchie, Ken Thompson y Brian Kernighan:** Mundialmente célebres como creadores del lenguaje de programación C y del sistema operativo Unix.

- **Richard Stallman:** Quien actualmente trabaja en Inteligencia Artificial en el MIT, y es el fundador de la Free Software Fundation, una gran organización a nivel mundial que promueve el uso y la difusión del software libre.

- **Kevin Mitnick**: Se hizo hacker desde los 10 años de edad, cuando logró, violar la seguridad de los sistemas de defensa de EUA; posteriormente fue asesor de seguridad cuando se presentó la epidemia del virus informático “I Love You”.

- **Bill Gates y Paul Allen**: Creadores de la empresa multimillonaria Microsoft Corporation. Integraban la “People Computer Company”, y se encargaron de desmitificar a las computadoras Mainframes. Fueron los creadores de la primera implementación del lenguaje BASIC, que se ejecutaba en un PC – Altair 8800 -. Fue la semilla de la gran empresa Microsoft.

3. CÓDIGO DE ÉTICA HACKER

Según **[RB96]** existen ciertos principios éticos que deben regir las acciones de cualquier persona que se considere un “buen hacker”, esencialmente dicen:

- El ser humano tiene el derecho a conocer la información pública, así como los mecanismos que se siguen para recolectar y procesas dicha información.

- El ser humano tiene la responsabilidad de evitar dañar a sus otros individuos mientras ejerce su derecho a conocer la información.

- El ser humano tiene la responsabilidad de compartir el conocimiento y las habilidades que sirven para revelar la función de los mecanismos de procesamiento de información, mientras guarda estrictamente la confidencialidad de la información que ha sido confiada o entregada a dichos mecanismos por partes privadas.

- El ser humano debe decir NO a la sociedad de la información, SI a una sociedad informada.

Estos principios fueron enunciados en Ámsterdam, el 4 de agosto de 1989, por Lee Felsestein, en la celebración de la primera Reunión Internacional de Hackers, y tuvieron la aprobación unánime de los participantes.

4. ROLES EN QUE SE DESENVUELVEN LOS HACKERS.

Esencialmente, las acciones de los hackers se dirigen hacia dos objetivos básicos siempre ellos son:

- **Robo de servicios telefónicos e información confidencial:** es decir, utilizar la redes telefónicas existentes sin tener que pagar los correspondientes derechos de uso de esos servicios. Son legendarias las Cajas Azules que utilizar

- **Penetración en Sistemas Informáticos de Alta Seguridad:** Es muy conocida la película “Juegos de Guerra” de John Badham, que además de ser un éxito taquillero en su momento, provocó una verdadera invasión de curiosos dirigida hacia todos los sistemas de seguridad militares norteamericanos, tales como el Pentágono, la CIA, la NSA, entre otros. La película, en sí misma, esta muy bien documentada y presenta técnicas reales que utilizan habitualmente los hackers, tales como discadores de teléfonos aleatorios.

5. CLASIFICACIÓN DE LOS HACKERS.

El término hacker engloba en sí, toda una sub-clasificación, dependiendo de factores tales como: experticia y valores éticos. Así, se encuentran:

- **Hackers:** Son los expertos en las tecnologías de la información, seguridad y comunicaciones, generalmente, alertan a las empresas del sector acerca de los fallos de seguridad que presentan sus productos. Son los menos ofensivos.

- **Crackers:** También son expertos en tecnologías de información, seguridad y comunicaciones. Se dedican a romper los sistemas de seguridad existentes y a “divulgar públicamente en la red sus hallazgos”. Son los autores de los archiconocidos “cracks” y “key generators”, utilizados por todos aquellos que instalan una versión de evaluación o

"demo" de un producto cualquiera, y posteriormente, la "crackean" para eliminarle las restricciones y tener a disposición el producto con todas sus capacidades completas.

- **Lamers y Script Kiddie:** es el grupo más difundido en la red. Quieren hackear sistemas, pero no saben como hacerlo. Actúan indiscriminadamente, con tal de realizar sus "Hazañas". Son los pulsa-botones clásicos, y de hecho, son los más peligrosos.

- **Copyhackers y bucaneros:** Se dedican a hacer dinero gracias a la tecnología desarrollada por los hackers verdaderos. Ellos actúan fuera de la red. Entre ellos tenemos a los clonadores de tarjetas de crédito.

- **Newbie:** Son los hackers aprendices. Al contrario de los Lamers y los Script Kiddie, aprenden con cautela el uso correcto de las tecnologías y no se mofan de sus logros en la red, simplemente aprenden.

6. HECHOS HISTÓRICOS IMPORTANTES DONDE HAN PARTICIPADO HACKERS.

Son muchos los hechos históricos en los que han participado hackers, entre ellos tenemos:

- Durante la segunda guerra mundial, Alan Turing y su equipo de colaboradores, al servicio de las fuerzas aliadas, lograron romper los esquemas de seguridad del sistema de comunicaciones de las fuerzas del eje alemán – la máquina enigma -, garantizando la victoria aliada con sus acciones (1939-1945).

- Un hacker de 15 años de edad rompió el sistema de encriptación de los DVD's (1999-2001).

- Un hacker de 10 años logró violar el sistema de seguridad de cobro de llamadas telefónicas en EUA en la compañía Bell Telephone (años 60).

- Hackers contratados por la NSA y la CIA han desarrollado las redes de espionaje "Echelon" y "UKUSA", que en conjunción con los satélites de comunicaciones y espionaje, que permiten espiar las comunicaciones a escala mundial, desde el final de la Segunda Guerra Mundial.

7. CATEGORIZACIÓN DE LAS ACEPCIONES DADAS AL CONCEPTO HACKER.

Categorizar a un hacker simplemente como bueno o malo es una acción muy relativizada. Se debe recordar que pueden ser identificados bajo muy diversos roles, tales como:

- Científicos Independientes,

- Los vaqueros del ciberespacio,

- Anarquistas,

- Simplemente Tecno-terroristas.

En realidad, el Hacker es bueno o es malo, esencialmente, dependiendo de:

- El tipo de acciones que realiza,

- Cual es su motivación a realizarlas,
- Para quién las realiza,
- Donde y cuando las realiza.

Cada caso debe ser evaluado objetivamente y por separado de otros casos, contextualizándolo adecuadamente, para lograr una categorización imparcial.

8. CONCLUSIONES.

- El buen Hacker es un experto en Sistemas de Seguridad, Redes e Informática, con conocimientos profundos del tema, que actúa bajo el código de ética Hacker, de manera responsable.
- Los roles de anarquista, tecno-terrorista y espía de las potencias mundiales no les son excluyentes.

9. REFERENCIAS BIBLIOGRÁFICAS.

[HE01] **HERNÁNDEZ, C. Hackers:** *Los Piratas Del Chip Y De Internet.* Segunda Edición. vLex, 2001.

[MH02] **MeTa-HaCkEr.** *Guía de Hacking para Normal Users.* Sin Editora. 2002.

[RB96] **ROBERTI, R.; BONSEMBIANTE, F.** *Llaneros Solitarios, Hackers, La Guerrilla Informática.* Fin De Siglo, 1996. Visitado el 2005-08-09. http://www.geocities.com/Area51/Orion/4015/llaneros.htm.