CAPÍTULO 5

"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Art. 12 Declaración Universal de Derechos Humanos, 1948

AMENAZAS HUMANAS

Este capítulo trata sobre cada uno de los personajes que pueden ser potenciales atacantes de nuestro sistema: el mundo under y el personal perteneciente a la organización.

Será difícil mantener una posición objetiva de la situación global en cuanto a los hackers y las fuerzas de seguridad, ya que siempre he visto marcado mi camino de conocimiento por la curiosidad: principal ingrediente (como veremos) del hacker. Así mismo, siempre me he mantenido en la raya de la legalidad y la ética, siendo prueba de esto el presente documento.

Desde los primeros albores del hacking siempre se ha mantenido una extraña relación entre estos particulares personajes, lo legal, lo ético y lo moral, siendo estas característica, lo

que intentan resaltar para esclarecer la diferencia entre cada uno de los clanes existentes en la ReD (como se la llama comúnmente en la jerga).

En el presente sólo se tratará de exponer el perfil de la persona encargada de una de las principales, (publicitariamente), si bien no la mayor amenaza que asechan nuestro sistema informático; para luego sí entrar en las formas de ataques propiamente dichos.

5.1 PATAS DE PALO Y PARCHES

5.1.1 CARTA DE PRESENTACIÓN[1]

"Hola, soy Cybor. Probablemente no me conozcan. Tampoco pretendo salir en la prensa. Eso no me importa, sin embargo si hay otras cosas que me interesan mas que mi identidad. Por ejemplo, me interesan las aperturas de sistemas cifrados. Pero eso es algo que nadie te enseña. Eso tienes que aprenderlo por ti mismo. También me interesa que todos sepáis quienes somos y que no estamos solos en este peculiar mundo. Me interesa que sepan que no todos los Hackers somos iguales. También me interesa saber que la palabra Hacker tiene un significado muy curioso. En un articulo reciente se publicó que se nos conocían como piratas informáticos; es probable, pero creo que están tremendamente equivocados. Quiero reivindicar mi posición. Pero lo cierto es que cada vez que hablan de nosotros es para decir que hemos reventado el ordenador de tal multinacional con grandes perdidas o que hemos robado cierta información. Estas cosas suceden, y particularmente tengo que decir que estas cosas están al alcance de otros personajes más peligrosos que nosotros. En nuestro mundo habitan los Crackers y los Phreackers... para la mayoría todos somos iguales y todos somos piratas informáticos. Pero quiero ir por pasos. ¿Que te parece saber de donde procede la palabra Hacker?.

En el origen de esta palabra esta el término Hack –algo así como golpear con un hacha en inglés– que se usaba como forma familiar para describir como los técnicos telefónicos arreglaban las cajas defectuosas, asestándoles un golpe seco... Quien hacia esto era un Hacker. Otra historia relata como los primeros ordenadores grandes y defectuosos, se fallaban continuamente. Los que las manejaban se devanaban los sesos creando rutas para aumentar la velocidad y cosas parecidas. Estas cosas se denominaban Hacks y a los que lo hacían se les llamaban Hackers. Otra denominación se le hacia a aquel experto en cualquier campo que disfrutaba modificando el orden de funcionamiento del aparato. De esta forma siempre superaba las limitaciones y esto le producía una alta satisfacción. A estas personas también se les llamaban Hackers.

Pero pronto surgieron otros acrónimos como Crackers. Fue inventado por los propios Hackers para diferenciar a aquel que fisgaba en un ordenador con aquel que creaba un virus dañino o copiaba un software. Así, frente a un ordenador ajeno un Hacker y un Cracker no son la misma cosa. Por otro lado en algunas ocasiones un Hacker es muy útil porque siempre detecta un agujero en cualquier programa nuevo... El Cracker aprovecharía este error para entrar en el programa y copiarlo.

Aparte del Cracking existen otras formas de vandalismo tecnológico. Así, el Phreacking, por ejemplo es la manipulación de las redes telefónicas para no pagar las llamadas. El Carding se refiere al uso ilegal de las tarjetas de crédito. Y el Trashing consiste en rastrear la basura o residuos de los sistemas informáticos en busca de información como contraseñas.

Pero, volviendo a los Hackers. ¿Cómo son?. ¿Qué aspecto tienen?. Cuando alguien oye mencionar la palabra Hacker rápidamente se le viene a la cabeza un adolescente ojeroso, con los ojos inyectados en sangre que ha pasado las últimas 24 horas delante del ordenador. Esta imagen esta estereotipada. No es así. Un Hacker puede ser cualquier estudiante de informática o electrónica, que sale con los amigos y que tiene novia. Un Hacker es una persona normal como tu. Los Hackers son casi siempre gente joven. Quizás somos los que más nos interesamos por la tecnología. Un Hacker normalmente despierta el gusanillo a temprana edad. Y no se hace de la noche a la mañana. Cuando logra serlo después de realizar un Hack, se busca un apodo y no da la cara por cuestión de seguridad... Normalmente al final de todo somos contratados por empresas importantes para ayudarles en su trabajo. Y otra cosa que hacemos es contar como funciona la tecnología que se nos oculta. Este método se llama enseñar y creo que no es nada malo. De modo que si un Hacker escribe un libro es porque tiene algo que enseñar y nada más... Y sobre todo quiero que quede buena constancia de lo que somos.

Cybor, Bangor Diciembre del 96 Maine"

[1] HERNÁNDEZ, Claudio. Los Clanes de la Red. Publicación Virtual – Revisión 1. España 1999.

Se mueven en una delgada e indefinida barrera que separa lo legal de lo ilegal. Las instituciones y las multinacionales del software les temen, la policía los persigue y hay quien los busca para contratarlos. Se pasean libremente por las mayores computadoras y redes del mundo sin que ellas tengan secretos.

Como expresa Cybor, hay quienes los llama piratas y delincuentes. Ellos reivindican su situación e intentan aclarar las diferencias entre los distintos clanes del Underground asegurando que sus acciones se rigen por un código ético.

Alguien aseguró que el que no usa su PC para escribir cartas, lleva un hacker dentro. Esta afirmación es una falacia si entendemos como hacker a un pirata informático; o quizás después de aclarar lo que significa este término, el resultado sea que existan mayores cuestionamientos que respuestas pero, sin duda, estos serán de una índole radicalmente distinta a la planteada hasta ahora.

"La policía quiere creer que todos los hackers son ladrones. Es una acción tortuosa y casi insoportable por parte del sistema judicial, poner a la gente en la cárcel, simplemente porque quieren aprender cosas que les esta prohibido saber..."[2].

La familia es grande, y el término más conocido es hacker. Pero, ¿qué son?, ¿quiénes son?, ¿qué persiguen?, ¿existen?, ¿cuántos son?, ¿dónde están?...

Los años han hecho que esta palabra sea prácticamente intraducible, dando esto diversos resultados negativos y casi siempre acusadores sobre la persona que realiza hacking.

Actualmente el término acepta, según la "jergon"[3] (Jerga Hacker) hasta siete definiciones y variados orígenes de la palabra. En el presente se maneja la etimología más ampliamente aceptada en el Underground digital.

La palabra inglesa "hack" literalmente significa "golpear" o "hachear" y proviene de los tiempos en que los técnicos en telefonía "arreglaban" algunas máquinas con un golpe seco y certero: es decir que estos técnicos eran "Hackers" y se dedicaban a "hackear" máquinas.

Estos inocentes golpes no parecen tener nada en común con las fechorías que hoy se les atribuyen. Estos hackers tampoco parecen ser el estereotipo formado en la actualidad de ellos: un chico con gruesos lentes, con acné y ojeroso por estar todo el día delante de su computadora, vagando por Internet tratando de esconder su último golpe y gastando cifras astronómicas en cuentas de teléfono que pagará su vecino, alguien en otro continente o nadie.

Estudiemos historia y veamos los puntos en común que hacen que un técnico en telefonía sea hacker al igual que un chico curioso; y hace que cada uno de nosotros sea un pirata al fotocopiar un libro o copiar el último procesador de palabras del mercado.

En el MIT (Massachusetts Institute of Technology) existen diferentes grupos con intereses especiales, fraternidades y similares que cada año intentan reclutar a los nuevos estudiantes para sus filas. En el otoño de 1958, durante su primera semana en el MIT, Peter Samson, que siempre había estado fascinado por los trenes y en especial por los metros, fue a ver la espectacular maqueta que el TMRC (Tech Model Railroad Club) tenía instalada en el

[2] STERLING, Bruce. La Caza de Hackers. Freeware Literario – Traducción de la versión en Original en Ingles por el grupo kriptopolis.com. España. 1999. *http://www.kriptopolis.com*

[3] Jergon File de Eric Raymond: http://murrow.journalism.wisc.edu/jargon/jargon.html

Edificio 20 del Instituto, y se quedó inmediatamente prendado de la parte técnica de la instalación.

En el TMRC existían dos facciones claramente diferenciadas: aquellos que se encargaban de construir los modelos de los trenes, edificios y paisajes que formaban la parte visible de la instalación y; el Subcomité de Señales y Energía que tenía a su cargo el diseño, mantenimiento y mejora de "el sistema", todo aquello que quedaba bajo los tableros, hacía funcionar los trenes y que permitía controlarlos. El TMRC daba una llave de sus instalaciones a sus miembros cuando estos acumulaban 40 horas de trabajo en las instalaciones, y Samson obtuvo la suya en un fin de semana.

Los miembros del Subcomité de Señales y Energía no se limitaban a trabajar en las instalaciones del TMRC, sino que no era extraño encontrarlos a altas horas de la madrugada recorriendo edificios y túneles de servicio intentando averiguar cómo funcionaba el complejo sistema telefónico del MIT, sistema que llegaron a conocer mejor que quienes lo habían instalado.

En la primavera de 1959, se dictaba el primer curso de programación al que se podían apuntar alumnos en su primer año. Samson y otros miembros del TMRC estaban en él (...).

Fue en aquel entonces, cuando un antiguo miembro del TMRC y entonces profesor del MIT hizo una visita al club y le preguntó a los miembros del Subcomité de Señales y Energía si les apetecería usar el TX-0. Este era uno de las primeras computadoras que funcionaban con transistores en lugar de con lámparas de vacío.

El TX-0 no usaba tarjetas sino que disponía de un teclado en el que el propio usuario tecleaba sus programas, que quedaban codificados en una cinta perforada que luego se introducía en el ordenador. El programa era entonces ejecutado, y si algo iba mal, el mismo usuario se podía sentar en la consola del TX-0 e intentar corregir el problema directamente usando una serie de interruptores y controles.

Dado que sólo se disponía un equivalente a 9 KB de memoria, era fundamental optimizar al máximo los programas que se hacían, por lo que una de las obsesiones fundamentales de los que lo usaban y se consideraban hábiles era hacer los programas tan pequeños como fuera posible, eliminando alguna instrucción aquí y allá, o creando formas ingeniosas de hacer las cosas. A estos apaños ingeniosos se les llamaba "hacks" y de ahí es de dónde viene el término "Hacker", denominación que uno recibía de sus compañeros (...).

De esta historia podemos obtener el perfil principal:

- Un hacker es a todas luces, alguien con profundos conocimientos sobre la tecnología.
- Tiene ansias de saberlo todo, de obtener conocimiento.
- Le gusta (apasiona) la investigación.
- Disfruta del reto intelectual y de rodear las limitaciones en forma creativa.
- Busca la forma de comprender las características del sistema estudiado, aprovechar sus posibilidades y por último modificarlo y observar los resultados.
- Dicen NO a la sociedad de la información y SI a la sociedad informada.

Hoy los hackers se sienten maltratados por la opinión pública, incomprendidos por una sociedad que no es capaz de comprender su mundo y, paradójicamente, perseguidos por las fuerzas del orden y por multinacionales que desean contratarlos.

La policía compara su incursión en una computadora ajena con la de un ladrón en un domicilio privado; pero para ellos la definición valida es: "... no rompemos la cerradura de la puerta ni les robamos nada de sus casas, nosotros buscamos puertas abiertas, entramos, miramos y salimos... eso lo pintes como lo pintes, no puede ser un delito".

La opinión del abogado español, experto en delito informático, Carlos Sánchez Almeida parece coincidir con esta última posición al decir: "... si un Hacker entra en un sistema, sin romper puertas y sin modificar los contenidos no se puede penalizar su actuación" y va más allá al afirmar: "...que tampoco sería delito hacerse con contraseñas, siempre y cuando se demuestre que éstas no han sido utilizadas... pero será delito, en cambio, el robo de bases de datos privadas con información confidencial y... también es denunciable la "dejadez" que cometen algunas empresas que disponen de información y datos privados de usuarios y, sin embargo, no tienen sus sistemas de seguridad suficientemente preparados para evitar el robo..."[4].

5.1.2 LA ACTITUD DEL HACKER

Como en las artes creativas, el modo más efectivo de transformarse en un maestro es imitar la mentalidad de los maestros, no sólo intelectualmente, sino además emocionalmente.

Se deberá aprender a puntuarse, principalmente, en función de lo que los otros hackers piensan acerca de las habilidades obtenidas (éste es el motivo por el cual no se puede ser un hacker de verdad hasta que otros hackers lo denominen así de manera consistente). Este hecho está empañado por la imagen del trabajo de hacker como trabajo solitario; también por un tabú cultural de los hackers (si bien en la actualidad es menor, aún es fuerte) que impide que se admita al ego o la validación externa como elementos involucrados en la propia motivación.

El status y reputación se gana no mediante la dominación de otras personas, no por ser hermoso/a, ni por tener cosas que las otras personas desean, sino por donar cosas: específicamente su tiempo, su creatividad y el resultado de sus habilidades.

Específicamente, el hackerismo es lo que los antropólogos denominan "cultura de la donación". Existen básicamente cinco clases de cosas que un hacker puede hacer para obtener el respeto de otros hackers:

1. Lo primero (el aspecto central y más tradicional) es escribir programas que los otros hackers opinen son divertidos y/o útiles, y donar los fuentes del programa a la cultura hacker para que sean utilizados. Los más reverenciados semidioses del hackers son las personas que han escrito programas de gran magnitud, con grandes capacidades que satisfacen necesidades de largo alcance, y los donan, de tal manera que cualquiera pueda utilizarlos (free).
2. Ayudar a probar y depurar software libre. Son reconocidas aquellas personas que depuran los errores del software libre. Es considerado un buen Beta-Tester aquel

[4] Extraído de *http://www.kriptopolis.com*

que sabe cómo describir claramente los síntomas, que puede localizar correctamente los problemas, que tolera los errores en una entrega apurada, y que está dispuesto a aplicar unas cuantas rutinas sencillas de diagnóstico.

3. Recolectar y filtrar información útil e interesante y construir páginas Web o documentos como FAQs y ponerlos a disposición de los demás.
4. Ayudar a mantener en funcionamiento la infraestructura. La cultura hacker funciona gracias al trabajo voluntario. Los administradores de listas de correo, moderadores de foros de discusión y sitios donde se archivan grandes cantidades de software, desarrolladores de RFCs y otros estándares técnicos gozan de mucho respeto, porque se sabe que estos son trabajos consumidores de tiempo y no tan "divertidos". Llevar adelante este trabajo demuestra mucha dedicación.
5. Hacer algo por la cultura hacker en sí misma. Esta cultura no tiene líderes exactamente, pero tiene héroes culturales, historiadores tribales y voceros. La búsqueda visible de esa clase de fama es peligrosa, por lo que la modestia es siempre recomendada.

5.1.3 DEFINICIÓN DE HACKER

Un **Hacker** es una persona que está siempre en una continua búsqueda de información, vive para aprender y todo para él es un reto; no existen barreras, y lucha por la difusión libre de información (Free Information), distribución de software sin costo y la globalización de la comunicación.

El concepto de hacker, generalmente es confundido erróneamente con los mitos que existen acerca de este tema:

- Un hacker es pirata. Esto no es así ya que los piratas comercian con la información que obtienen, entre otras cosas, y un verdadero hacker solo obtiene esa información para su uso personal.
- Un hacker es el que entra en los sistemas ajenos y se dedica a destruir la información almacenada en ellos. El error consiste en que el que destruye información y sistemas ajenos, no es el hackers sino el Cracker[5].

Pero entonces veamos que **sí** es un **Hacker**[6]:

1. Un verdadero Hacker es curioso y paciente. Si no fuera así terminarían por hartarse en el intento de entrar en el mismo sistema una y otra vez, abandonando el objetivo.
2. Un verdadero Hacker no se mete en el sistema para borrarlo todo o para vender lo que consiga. Quiere aprender y satisfacer su curiosidad. Esa es la única finalidad de introducirse en el sistema. Buscan dentro de un lugar en el que nunca han estado, exploran todos los pequeños rincones de un mundo diferente del que ya conocen y que les aburre. ¿Porqué destruir algo y perderse el placer de decir a los demás que hemos estado en un lugar donde ellos no han estado?.

[5] Crack (en inglés) Grieta. La traducción del término Cracker al español es "el que produce una grieta"
[6] Definición extraída y traducida del Jergon File de Eric Raymond. *http://murrow.journalism.wisc.edu/jargon/jargon.html*

3. Un Hacker es inconformista, ¿porqué pagar por una conexión que actualmente cuesta mucho dinero, y además es limitada? ¿Porqué pagar por una información que solo van a utilizar una vez?.
4. Un Hacker es discreto, es decir que cuando entra en un sistema es para su propia satisfacción, no van por ahí cantándolo a los cuatro vientos. La mayoría de los casos de "Hackers" escuchados son en realidad "Fantasming". Esto quiere decir, que si un amigo se entera que se ha entrado en cierto sistema; "el ruido de los canales de comunicación" hará que se termine sabiendo que se ha entrado en un sistema cinco veces mayor, que había destruido miles de ficheros y que había inutilizado el sistema.
5. Un Hacker disfruta con la exploración de los detalles de los sistemas programables y aprovecha sus posibilidades; al contrario de la mayoría de los usuarios, que prefieren aprender sólo lo imprescindible.
6. Un Hacker programa de forma entusiasta (incluso obsesiva), rápido y bien.
7. Un Hacker es experto en un programa en particular, o realiza trabajos frecuentemente usando cierto programa. Por ejemplo "un Hacker de Unix programador en C".
8. Los Hackers suelen congregarse. Tiende a connotar participación como miembro en la comunidad global definida como "La ReD".
9. Un Hacker disfruta del reto intelectual de superar o rodear las limitaciones de forma creativa.
10. Antiguamente en esta lista se incluía: Persona maliciosa que intenta descubrir información sensible: contraseñas, acceso a redes, etc. Pero para este caso en particular los verdaderos Hackers han optado por el término Cracker y siempre se espera (quizás inútilmente) que se los diferencie.

"Nótese que ninguna definición define al Hacker como un criminal. En el mejor de los casos, los Hackers cambian precisamente la fabricación de la información en la que se sustenta la sociedad y contribuyen al flujo de tecnología. En el peor, los Hackers pueden ser traviesos perversos o exploradores curiosos. Los Hackers NO escriben dañinos virus de computadora. Quienes lo hacen son los programadores tristes, inseguros y mediocres. Los virus dañinos están completamente en contra de la ética de los Hackers"[7].

En el presente se usará la palabra Intruso para definir a las personas que ingresan a un sistema sin autorización y preservará la palabra Hacker; evitando producir falsos conceptos que contribuyan a la confusión aportada por el amarillismo de la prensa, la mitología y la mitomanía de algunas personas.

5.1.4 LA CONEXIÓN HACKER – NERD

Contrariamente al mito popular, no es necesario ser un nerd para ser un hacker. Ayuda, sin embargo, y muchos hackers son nerds. Al ser un marginado social, el nerd puede mantenerse concentrado en las cosas realmente importantes, como pensar y hackear.

[7] Rich Crash Lewis, Hacker Test, 1992. Texto extraído y traducido de Electronic Frontier of Compuserve. *http://www2.vo.lu/homepages/phahn/humor/hacker30.txt*

Por esta razón, muchos hackers han adoptado la etiqueta nerd" e incluso utilizan el término "Geek" como insignia de orgullo: es una forma de declarar su propia independencia de las expectativas sociales normales.

5.1.5 CRACKERS

Los **Crackers**, en realidad, son hackers cuyas intenciones van más allá de la investigación. Es una persona que tiene fines maliciosos o de venganza, quiere demostrar sus habilidades pero de la manera equivocada o simplemente personas que hacen daño solo por diversión. Los hackers opinan de ellos que son "... Hackers mediocres, no demasiados brillantes, que buscan violar (literalmente "break") un sistema".

5.1.6 PHREAKERS

Otro personaje en el Underground es el conocido como **Phreaker**[8]. El Phreaking, es la actividad por medio de la cual algunas personas con ciertos conocimientos y herramientas de hardware y software, pueden engañar a las compañías telefónicas para que éstas no cobren las llamadas que se hacen.

La realidad indica que lo Phreakers son Cracker de las redes de comunicación. Personas con amplios (a veces mayor que el de los mismo empleados de las compañías telefónicas) conocimientos en telefonía.

Se dice que el Phreaking es el antecesor del Hacking ya que es mucho más antiguo. Comenzó en los albores de la década de los '60 cuando un tal Mark Bernay descubrió como aprovechar un error de seguridad de Bell[9] basaba en la utilización de los mecanismos para la realización de llamadas gratuitas. Lo que Bernay descubrió, fue que dentro de Bell existían unos números de prueba que servían para que los operarios comprobaran las conexiones. Hasta aquí todos eran simples adolescentes que hacían llamadas gratuitas a sus padres en otro estado.

La situación cambió cuando se descubrió que MamaBell (como suele llamarse a Bell) era un universo sin explorar y al que se le podría sacar más partido que el de unas simples llamadas. Se comenzaron a utilizar ciertos aparatos electrónicos, los cuales son conocidos como "Boxes" (cajas). La primera fue la "Blue Box" que fue hallada en 1961 en el Washington State College, y era un aparato con una carcasa metálica que estaba conectada al teléfono. Estas Boxes lo que hacían era usar el nuevo sistema de Bell (los tonos) para redirigir las llamadas. Cuando se marcaba un número, Bell lo identificaba como una combinación de notas musicales que eran creadas por seis tonos maestros, los cuales eran los que controlaban Bell y por lo tanto eran secretos (al menos eso pretendían y creían los directivos de Bell).

El cómo los Phreakers llegaron a enterarse del funcionamiento de estos tonos fue algo muy simple: Bell, orgullosa de su nuevo sistema, lo publicó detalladamente en revistas que iban dirigidas única y exclusivamente a los operarios de la compañía telefónica. Lo que

[8] Fusión de las palabras Freak, Phone y Free: Mounstruo de los Teléfonos Libres (intento de traducción literal)
[9] Compañía telefónica fundada por Alexander Graham Bell

sucedió es que no cayeron en la cuenta de que todo suscriptor de esa revista recibió también en su casa un ejemplar que narraba el funcionamiento del nuevo sistema.

Al poco tiempo hubo en la calle variaciones de la Blue Box inicial que fueron llamadas Red Box y Black Box, la cuales permitían realizar llamadas gratis desde teléfonos públicos.

Las Blue Boxes no solo servían para realizar llamadas gratuitas, sino que proporcionaban a sus usuarios los mismos privilegios que los operadores de Bell.

Lo realmente curioso, y desastroso para Bell, es que algunas personas eran capaces de silbar 2600 ciclos (lo cual significa que la línea está preparada para recibir una llamada) de forma completamente natural.

El primer Phreaker que utilizó este método fue Joe Engressia, quien era ciego. A los 8 años, y por azar, silbó por el auricular de su teléfono cuando escuchaba un mensaje pregrabado y la llamada se cortó. Realizo esto varias veces y en todas se le cortaba. La razón es un fenómeno llamado Talk-Off, que consiste en que cuando alguien silba y alcanza casualmente los 2600 Hz, la llamada se corta, como si fuera una Blue Box orgánica. Joe aprendió como potenciar su habilidad para silbar 2600 Hz y ya con 20 años era capaz de producir los 2600 Hz con su boca y silbar los tonos del número con el que quería conectarse.

Otro Phreaker que utilizaba el método de Engressia, fue John Draper, más conocido por Capitán Crunch, que creo un silbato que regalaban con la marca de cereales Capitán Crunch, el cual, podría utilizarse como instrumento para hacer Phreaking. Draper hacia algo parecido a lo que hacia Joe Engressia: soplaba su silbato y la línea se quedaba libre.

Muchos Phreackers evolucionaron mas tarde al Hacking, como es el caso del pionero Mark Bernay, que bajo el nick de The Midnight Skulker (El Vigilante de Medianoche) se rió de todos los fallos de seguridad de muchas empresas.

Hoy, el Hacking y el Phreacking viven en perfecta armonía y en pleno auge con las nuevas tecnologías existentes. Es difícil delimitar el terreno de cada uno, ya que un hacker necesitara, tarde o temprano, hacer Phreacking si desea utilizar la línea telefónica mucho tiempo en forma gratuita y; de la misma forma un Phreaker necesitará del Hacking si desea conocer en profundidad cualquier sistema de comunicaciones.

5.1.7 CARDING – TRASHING

Entre las personas que dedicaban sus esfuerzos a romper la seguridad como reto intelectual hubo un grupo (con no tan buenas intenciones) que trabajaba para conseguir una tarjeta de crédito ajena. Así nació:

1. El **Carding**, es el uso (o generación) ilegitimo de las tarjetas de crédito (o sus números), pertenecientes a otras personas con el fin de obtener los bienes realizando fraude con ellas. Se relaciona mucho con el Hacking y el Cracking, mediante los cuales se consiguen los números de las tarjetas.
2. El **Trashing**, que consiste en rastrear en las papeleras en busca de información, contraseñas o directorios.

5.1.8 DESAFÍOS DE UN HACKER

1. El mundo está lleno de problemas fascinantes que esperan ser resueltos.
2. El esfuerzo requiere motivación. Los atletas exitosos obtienen su motivación a partir de una clase de placer físico que surge de trabajar su cuerpo, al forzarse a sí mismos más allá de sus propios límites físicos. De manera similar, un hacker siente un estremecimiento de tipo primitivo cuando resuelve un problema, agudiza sus habilidades, y ejercita su inteligencia.
3. Nadie debería tener que resolver un problema dos veces.
4. Los cerebros creativos son un recurso valioso y limitado. No deben desperdiciarse reinventando la rueda cuando hay tantos y tan fascinantes problemas nuevos esperando por allí.
5. Lo aburrido y lo rutinario es malo.
6. Los hackers (y las personas creativas en general) no deberían ser sometidas a trabajos rutinarios, porque cuando esto sucede significa que no están resolviendo nuevos problemas.
7. La libertad es buena.
8. Los hackers son naturalmente anti–autoritaristas. Cualquiera que le pueda dar órdenes, puede hacer que deba dejar de resolver ese problema con el cual está fascinado.
9. La actitud no es sustituto para la competencia.
10. Tener la actitud para ser hacker no alcanza, como tampoco alcanza para transformarse en un atleta campeón o en estrella del rock. Para transformarse en hacker necesitará inteligencia, práctica, dedicación, y trabajo pesado. Por lo tanto, debe respetar la competencia en todas sus formas.

5.1.9 HABILIDADES BÁSICAS EN UN HACKER.

El conjunto de habilidades cambia lentamente a lo largo del tiempo a medida que la tecnología crea nuevas tecnologías y descarta otras por obsoletas. Por ejemplo, hace tiempo, se incluía la programación en lenguaje de máquina y Assembler, y no se hablaba de HTML. Un buen hacker incluye las siguientes reglas en su itinerario:

1. Aprender a programar. Esta es, por supuesto, la habilidad fundamental del hacker. Se deberá aprender como pensar en los problemas de programación de una manera general, independiente de cualquier lenguaje. Se debe llegar al punto en el cual se pueda aprender un lenguaje nuevo en días, relacionando lo que está en el manual con lo que ya sabe de antes. Se debe aprender varios lenguajes muy diferentes entre sí. Es una habilidad compleja y la mayoría de los mejores hackers lo hacen de forma autodidacta.
2. Aprender Unix. El paso más importante es obtener un Unix libre, instalarlo en una máquina personal, y hacerlo funcionar. Si bien se puede aprender a usar Internet sin saber Unix, nunca se podrá ser hacker en Internet sin conocerlo. Por este motivo, la cultura hacker actual está centrada fuertemente en Unix.

5.1.10 ¿CÓMO LO HACEN?

Quizás esta sea la pregunta más escuchada cuando se habla de hackers y los ataques por ellos perpetrados (ver Anexo I).

Para contestarla debemos ser conscientes de cada una las características de los hackers entre las que se destacan la paciencia y la perseverancia ante el desafío planteado. Será común ver a algunos de ellos fisgonear durante meses a la victima para luego recién intentar un ataque que además de efectivo debe ser invisible.

En capítulos posteriores se analizarán las técnicas (si bien no las herramientas específicas) por ellos utilizadas para perpetrar un ataque, así como también las utilizadas por los expertos en seguridad a la hora de descubrir y tirar por tierra las ambiciones hackers.

5.1.11 LA ÉTICA DEL HACKER[10]

Desde el principio los hackers desarrollaron un código de ética o una serie de principios que eran tomados como un acuerdo implícito y no como algo escrito o fijo:

I. El acceso a las computadoras debe ser ilimitado y total.
II. El acceso a la información debe ser libre y gratuito.
III. Desconfíen de la autoridad, promuevan la descentralización.
IV. Los hackers deben ser juzgados por su habilidad, no por criterios absurdos como títulos, edad, raza o posición social.
V. Se puede crear arte y belleza en una computadora.
VI. Las computadoras pueden cambiar tu vida para mejor.

Así también se desarrollaron los algunos "Mandamientos" en los cuales se basa un hacker a la hora de actuar sobre los sistemas que ataca:

I. Nunca destroces nada intencionadamente en la PC que estés hackeando.
II. Modifica solo los ficheros que hagan falta para evitar tu detección y asegurar tu acceso futuro al sistema.
III. Nunca dejes tus datos reales, tu nombre o tu teléfono en ningún sistema, por muy seguro que creas que es.
IV. Ten cuidado a quien le pasas información. A ser posible no pases nada a nadie que no conozcas su voz, número de teléfono y nombre real.
V. Nunca dejes tus datos personales en un BBS, si no conoces al SysOp, déjale un mensaje con la lista de gente que pueda responder por tí.
VI. Nunca hackees en computadoras del gobierno. El gobierno puede permitirse gastar fondos en buscarte, mientras que las universidades y las empresas particulares no.
VII. No uses Blue Box a menos que no tengas un PAD local o número gratuito al que conectarte, si se abusa de la Blue Box, puedes ser cazado.
VIII. No dejes en mucha información del sistema que estas hackeando. Di sencillamente "estoy trabajando en ..." pero no digas a quien pertenece, ni el número de teléfono, dirección, etc.
IX. No te preocupes en preguntar, nadie te contestara. Piensa que por responderte a una pregunta, pueden cazarte a ti, al que te contesta o a ambos.
X. Punto final. Hasta que no estés realmente hackeando, no sabrás que es...

[10] Maximum Security. A Hacker's guide to protecting your Internet Site and Network. Macmillan Computer Publishing©. 1999. EE.UU. *http://sams.net*
http://www.itlibrary.com/reference/library/1575212684/ewtoc.html

5.1.12 MANIFIESTO HACKER[11]

En los principios, un grupo hackers llamado Legión of Doom, dirigido por The Mentor, quería demostrar hasta donde era capaz de llegar. Para ello modificaron la página principal del sitio web de la NASA, durante media hora, con el siguiente "manifiesto":

> (...) "Hoy he hecho un descubrimiento. He encontrado una computadora. Esperad, esto es lo mejor. La computadora hacía lo que yo quería. Si cometía un error era porque yo me equivocaba. No porque yo no le gustara... Y entonces ocurrió... una puerta se abrió al mundo, surcando la línea telefónica igual que la heroína surca las venas del adicto, el impulso eléctrico te envía a un refugio a salvo de las incompetencias del día a día... la BBS ha sido encontrada. Es... es a donde pertenezco. Conozco a todo el mundo aquí, incluso sin haberlos visto antes, sin haber hablado con ellos y puede que a algunos no vuelva a verlos jamás... Os conozco a todos... Éste es nuestro mundo... el mundo del electrón y el conmutador, la belleza del baudio. Hacemos uso de un servicio ya existente sin pagar por lo que podría ser gratis si no estuviera en manos de unos glotones aprovechados, y tú nos llamas a nosotros criminales. Nosotros exploramos... y tú nos llamas criminales. Existimos sin color de piel, sin nacionalidad, sin inclinaciones religiosas... y tú nos llamas criminales. Tú que construyes bombas atómicas, tú que haces la guerra, tú asesino, nos engañas y mientes intentando hacernos creer que es por nuestro propio bien, sin embargo somos criminales. Si, soy un criminal. Mi crimen es la curiosidad. Mi crimen es juzgar a la gente por que lo que ellos dicen y piensan, no por como ellos aparentan ser exteriormente. Mi crimen es ser más inteligente que tú, algo por lo que nunca me perdonarás." (...)
>
> +++ The Mentor +++

Fermín (alias) es un estudiante universitario español, trabaja en una empresa de seguridad informática ganando un sueldo impactante. Este trabajo lo consiguió siendo hacker y según dice él por "... nacer y ser curioso, por hacer del hacking una forma de vida, un espíritu de superación y un reto de intelectual continuo (...)". También declara que en la red hay gente con los mismos conocimientos que él que los utilizan para delinquir e incluso son buscados y pagados para ello, "... pero este no es un hacker."[12]

Un ejemplo de este accionar puramente hacker lo demuestra al denunciar a un hospital sus fallos de seguridad (luego de haber penetrado el sistema) y recibiendo "como premio" una denuncia por intrusión ilegal. Acciones como estas son comunes en el mundo hacker pero "tapados" y generalmente distorsionados en contra de "estos personajes siniestros".

5.1.13 OTROS HABITANTES DEL CIBERESPACIO

5.1.13.1 GURÚS

Son considerados los maestros y los encargados de "formar" a los futuros hackers. Generalmente no están activos pero son identificados y reconocidos por la importancia de sus hackeos, de los cuales sólo enseñan las técnicas básicas.

5.1.13.2 LAMERS O SCRIPT–KIDDERS

Son aficionados jactosos. Prueban todos los programas (con el título "como ser un hacker en 21 días") que llegan a sus manos. Generalmente son los responsables de soltar virus

[11] La Conciencia de un Hacker escrito por The Mentor Volumen 1–Capítulo 7–3° Párrafo.
[12] Declaraciones de Fermín para *http://www.kriptopolis.com*

y bombas lógicas en la red sólo con el fin de molestar y que otros se enteren que usa tal o cual programa. Son aprendices que presumen de lo que no son aprovechando los conocimientos del hacker y lo ponen en práctica sin saber.

5.1.13.3 COPYHACKERS

Literalmente son falsificadores sin escrúpulos que comercializan todo lo copiado (robado).

5.1.13.4 BUCANEROS

Son comerciantes sucios que venden los productos crackeados por otros. Generalmente comercian con tarjetas de crédito y de acceso y compran a los copyhackers. Son personas sin ningún (o escaso) conocimiento de informática y electrónica.

5.1.13.5 NEWBIE

Son los novatos del hacker. Se introducen en sistemas de fácil acceso y fracasan en muchos intentos, sólo con el objetivo de aprender las técnicas que puedan hacer de él, un hacker reconocido.

5.1.13.6 WANNABER

Es aquella persona que desea ser hacker pero estos consideran que su coeficiente no da para tal fin. A pesar de su actitud positiva difícilmente consiga avanzar en sus propósitos.

5.1.13.7 SAMURAI

Son lo más parecido a una amenaza pura. Sabe lo que busca, donde encontrarlo y cómo lograrlo. Hace su trabajo por encargo y a cambio de dinero. Estos personajes, a diferencia de los anteriores, no tienen conciencia de comunidad y no forman parte de los clanes reconocidos por los hackers. Se basan en el principio de que cualquiera puede ser atacado y saboteado, solo basta que alguien lo desee y tenga el dinero para pagarlo.

5.1.13.8 PIRATAS INFORMÁTICOS

Este personaje (generalmente confundido con el hacker) es el realmente peligroso desde el punto de vista del Copyright, ya que copia soportes audiovisuales (discos compactos, cassettes, DVD, etc.) y los vende ilegalmente.

5.1.13.9 CREADORES DE VIRUS

Si de daños y mala fama se trata estos personajes se llevan todos los premios. Aquí, una vez más, se debe hacer la diferencia entre los creadores: que se consideran a sí mismos desarrolladores de software; y los que infectan los sistemas con los virus creados. Sin embargo es difícil imaginar que cualquier "desarrollador" no se vea complacido al ver que su "creación" ha sido ampliamente "adquirida por el público".

5.2 PERSONAL (INSIDERS)

Hasta aquí se ha presentado al personal como víctima de atacantes externos; sin embargo, de los robos, sabotajes o accidentes relacionados con los sistemas informáticos, el 70%[13] son causados por el propio personal de la organización propietaria de dichos sistemas ("Inside Factor").

Hablando de los Insiders Julio C. Ardita[14] explica que "(...) desde mitad de 1996 hasta 1999 la empresa tuvo dos casos de intrusiones pero en el 2000 registramos siete, de las cuales 5 eran intrusos internos o ex–empleados (...)".

El siguiente gráfico detalla los porcentajes de intrusiones clasificando a los atacantes en internos y externos.

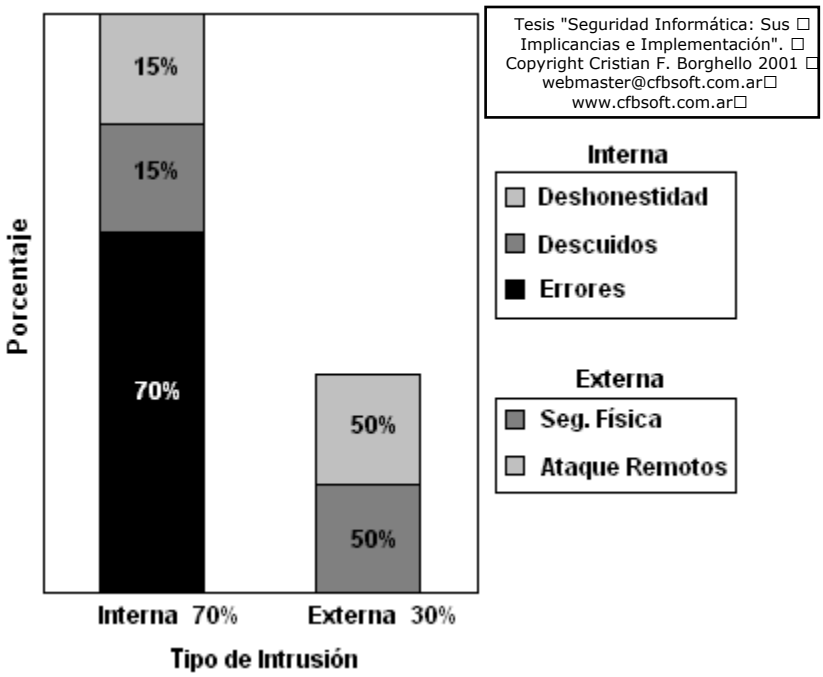

Gráfico 5.1 – Intrusiones. Fuente: *http://www.cybsec.com*

Esto es realmente preocupante, ya que, una persona que trabaje con el administrador, el programador o el encargado de una máquina conoce perfectamente el sistema, sus puntos fuertes y débiles; de manera que un ataque realizado por esa persona podrá ser más directo, difícil de detectar y más efectivo que el que un atacante externo pueda realizar.

Existen diversos estudios que tratan sobre los motivos que llevan a una persona a cometer delitos informáticos contra su organización, pero sean cuales sean, estos motivos existen y deben prevenirse y evitarse. Suele decirse que todos tenemos un precio (dinero, chantaje, factores psicológicos, etc.), por lo que nos pueden arrastrar a robar y vender información o simplemente proporcionar acceso a terceros.

[13] Fuente: Cybsec S.A. *http://www.cybsec.com*

[14] ARDITA, Julio César. Director de Cybsec S.A. Security System y ex–Hacker. Entrevista personal realizada el día 15 de enero de 2001 en instalaciones de Cybsec S.A. *http://www.cybsec.com*

Como ya se ha mencionado los ataques pueden ser del tipo pasivos o activos, y el personal realiza ambos indistintamente dependiendo de la situación concreta. Dentro de este espectro podemos encontrar:

5.2.1 PERSONAL INTERNO

Las amenazas a la seguridad de un sistema, provenientes del personal del propio sistema informático, rara vez es tomada en cuenta porque se supone un ámbito de confianza muchas veces inexistente. Generalmente estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad; pero también pueden ser del tipo intencional.

Es de destacar que un simple electricista puede ser más dañino que el más peligroso de los piratas informáticos, ya que un corte de energía puede causar un desastre en los datos del sistema. Al evaluar la situación, se verá que aquí el daño no es intencionado pero ello no esta en discusión; el daño existió y esto es lo que compete a la seguridad informática.

5.2.2 EX–EMPLEADO

Este grupo puede estar especialmente interesado en violar la seguridad de nuestra empresa, sobre todo aquellos que han sido despedidos y no han quedado conformes; o bien aquellos que han renunciado para pasar a trabajar en la competencia. Generalmente se trata de personas descontentas con la organización que conocen a la perfección la estructura del sistema y tienen los conocimientos necesarios como para causar cualquier tipo de daño. También han existido casos donde el ex–empleado deja Bombas Lógicas que "explotan" tiempo después de marcharse.

5.2.3 CURIOSOS

Suelen ser los atacantes más habituales del sistema. Son personas que tienen un alto interés en las nuevas tecnologías, pero aún no tienen los conocimientos ni experiencia básicos para considerarlos hackers o crackers (podrían ser Newbies). En la mayoría de los casos son estudiantes intentando penetrar los servidores de su facultad o empleados consiguiendo privilegios para obtener información para él vedada. Generalmente no se trata de ataques de daño pero afectan el entorno de fiabilidad con confiabilidad generado en un sistema.

5.2.4 TERRORISTAS

Bajo esta definición se engloba a cualquier persona que ataca el sistema para causar daño de cualquier índole en él; y no sólo a la persona que coloca bombas o quema automóviles. Son ejemplos concretos de este tipo, ataque de modificación[15] de los datos de clientes entre empresa competidoras, o de servidores que albergan páginas web, bases de datos entre partidos políticos contrarios, etc.

[15] Por **Modificación** se entiende cualquier cambio de los datos incluyendo su borrado.

5.2.5 INTRUSOS REMUNERADOS

Este es, sin duda, el grupo de atacantes más peligroso, aunque también el menos habitual. Se trata de crackers o piratas con grandes conocimientos y experiencia, pagados por una tercera parte para robar "secretos" (código fuente de programas, bases de datos de clientes, información confidencial de satélites, diseño de un nuevo producto, etc.) o simplemente para dañar, de alguna manera la imagen de la entidad atacada.

Suele darse, sólo, en grandes multinacionales donde la competencia puede darse el lujo de un gran gasto para realizar este tipo de contratos y contar con los medios necesarios para realizar el ataque.

5.2.6 RECOMENDACIONES

Una norma básica, sería verificar cada aspirante a ser nuevo empleado; aunque tampoco debemos olvidar que el hecho de que alguien entre "limpio" a la organización no implica que vaya a seguir así durante el tiempo que trabaje en la misma, y mucho menos cuando abandone su trabajo.

Para minimizar el daño que un atacante interno puede causar se pueden seguir estos principios fundamentales:

- **Necesidad de conocimiento (Need to Know):** comúnmente llamado mínimo privilegio. Cada usuario debe tener el mínimo privilegio que necesite para desempeñar correctamente su función, es decir, que sólo se le debe permitir que sepa lo necesario para realizar su trabajo.
- **Conocimiento parcial (dual control):** las actividades más delicadas dentro de la organización deben ser realizadas por dos personas competentes, de forma que si uno comete un error en las políticas de seguridad el otro pueda subsanarlo. Esto también es aplicable al caso de que si uno abandona la organización el otro pueda seguir operando el sistema mientras se realiza el reemplazo de la persona que se retiró.
- **Rotación de funciones:** la mayor amenaza del conocimiento parcial de tareas es la complicidad de dos responsables, de forma tal, que se pueda ocultar sendas violaciones a la seguridad. Para evitar el problema, una norma común es rotar (dentro de ciertos límites) a las personas a lo largo de diferentes responsabilidades, para establecer una vigilancia mutua.
- **Separación de funciones:** es necesario que definan y separen correctamente las funciones de cada persona, de forma que alguien cuya tarea es velar por la seguridad del sistema no posea la capacidad para violarla sin que nadie se percate de ello.
- **Cancelación inmediata de cuenta:** cuando un empleado abandona la organización se debe cancelar inmediatamente el acceso a sus antiguos recursos y cambiar las claves que el usuario conocía. Quizás este último punto sea el más difícil de implementar debido a la gran cantidad de usuarios que se deben informar de los nuevos accesos y de la movilidad de alguno de ellos.

En estos puntos se encuentran las mayores vulnerabilidades de un sistema ya que, por ejemplo, suelen encontrarse cuentas de usuario que hace años que no se utilizan, y por ende tampoco se han cambiado sus passwords.

Si bien estas normas pueden aplicarse a las organizaciones, no podrán hacerlo en instituciones como una universidad, donde la mayoría de los atacantes son alumnos y no podrá verificarse los antecedentes de miles de alumnos (y tampoco ético prohibir su acceso por ser estos dudosos). De esta forma, en las redes de Investigación y Desarrollo (I+D) de acceso público debemos ceñirnos a otros mecanismos de control y casi siempre se opta por las sanciones a todos aquellos que utilicen el centro para cometer delitos informáticos.