UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA

LA FILOSOFÍA HACKING & CRACKING

MONOGRAFÍA

Que Para obtener el título de:

Licenciado en Sistemas Computacionales

Presenta:

PLSC. Benjamín Martínez Alarcón.

Asesor:

L.C. Luis Islas Hernández.

Pachuca, Hidalgo. Abril 2006.

ÍNDICE

ÍNDICE

INTRODUCCIÓN

En la época actual, el desarrollo acelerado en los sectores de la computación y las telecomunicaciones ha afectado notablemente el manejo de la información en prácticamente todas las actividades humanas. Entre otros aspectos, las redes digitales como Internet hacen posible la consulta simultánea de información contenida en el mismo sitio, así como la constante intercomunicación entre seres humanos, sin importar la distancia que los separe. Esta comunicación impersonal, aunada a la posibilidad de conocer la información oculta o secreta que grandes compañías y gobiernos poseen, han hecho florecer una actitud crítica y en búsqueda de la libertad, ante los privilegios que obtienen los poseedores de la información, y ante la veracidad de la misma. Tal posición se manifiesta a través de la contracultura digital llamada cibercultura.

En la Cibercultura, aparecen grupos con diferentes concepciones acerca del uso de la información digital, entre los que destacan los hackers como uno de los grupos con ideales más optimistas. Así, al igual que en otras etapas de la historia, se han forjado leyendas heroicas protagonizadas por individuos subversivos que buscan cómo recoger información valiosa para su amplia utilización. El hacker se concibe como un ciberrebelde que utiliza sus cualidades en materia informática para dialogar, jugar y transgredir en el ciberespacio, con el principal fin de democratizar el uso de la información.

Como simpatizantes de la cibercultura, los hackers comparten la fascinación por la alta tecnología y el rechazo a utilizarla convencionalmente. Por ejemplo están a favor de la simbiosis hombre-máquina y de la creación de universos virtuales. En este sentido, pretenden mostrar cómo la ética planteada por los hackers en el manejo de la información, es producto tanto del ambiente cibercultural que se vive en el mundo, como de las propuestas hechas por otros grupos de ciberrebeldes, que en ocasiones manifiesta nuestras perspectivas respecto de la ética hacker.

INTRODUCCIÓN

A través de distintas épocas, las revoluciones tecnológicas han impuesto modelos de producción basadas en diferentes recursos. Actualmente esa materia abstracta llamada información, es la que dicta numerosos cambios en prácticamente todos los ámbitos de la vida humana.

El primer escalón de una sociedad "delictiva" según la prensa. Estos personajes son expertos en sistemas avanzados. En la actualidad se centran en los sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica con lo que logran comprender sistemas tan complejos como la comunicación móvil. Su objetivo principal es entender el funcionamiento de los sistemas. Les encanta entrar en ordenadores remotos con el fin de decir "he estado aquí" pero no modifican ni se llevan nada del ordenador atacado. Normalmente son quienes alertan de un fallo en algún programa comercial, y lo comunican al fabricante. También es frecuente que un buen Hacker sea finalmente contratado por alguna importante empresa de seguridad.

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 solo habita en los suburbios de una gran red como lo es Internet, ni navega continuamente entre los discos duros de los ordenadores, que aunque se les conocen en estos entornos mayoritariamente, los Hackers también fisgonean sistemas fuera de una CPU. Solo tenemos que echar una ojeada a nuestro pc para saber cuantas cosas más atentan contra la curiosidad.

Hacker nació en momentos en que las computadoras eran grandes armatostes, tan grandes como habitaciones de una casa victoriana. En su interior, cientos de cables se caldeaban junto a las válvulas de vacío; lámparas mágicas se apresuraban a decir los técnicos. Eran tiempos del Eniac, de la TX-0 y del MIT, y de ser cierto, los Hackers surgieron en esa época.

OBJETIVOS

Objetivo General:

Proporcionar la información que muestre la importancia que hoy en día la filosofía Hacking y Cracking representa, la cual es capaz de manipular la información a través de la tecnología.

Objetivos Específicos:

Mostrar los aspectos de la Cultura y Contracultura del Hacking y Cracking. Y motivar el aprendizaje de la Filosofía del Hacking de una manera Ética.

Describir las herramientas más comunes de defensa para poder evitar un ataque, dadas las amenazas constantes en la red.

Puntualizar como el Hacking y Cracking se utiliza en el Ciberterrorismo y de que manera la Política y los movimientos Sociales generan el Hactivismo.

Exponer como el Hacking y Cracking, se pueden convertir en la excusa para la invasión a la privacidad.

JUSTIFICACIÓN.

Si los hackers son hoy en día importantísimos, es precisamente por la naturaleza abierta del código que elaboran. Gracias a dicha apertura se genera el enorme crecimiento de lo que se puede hacer con la tecnología. Precisamente por la importancia que despliegan dentro de la sociedad y el desarrollo de la misma humanidad es de vital importancia informarnos sobre la Filosofía Hacking & Cracking. Proporcionar este trabajo dada la incertidumbre que puede generar dicha filosofía.

Basado en la incomparable eficiencia y eficacia del Internet como medio de comunicación, el Hacking y Cracking es ya una realidad comprobada. Por lo que debemos integrarnos a un nuevo mundo con el único fin actualizarnos en los terrenos del orbe subterráneo del hacking, además de la seguridad que involucra esta filosofía.

Brindar un contexto de la amenaza constante del ciberterrorismo y la inseguridad que este conlleva; para obtener un contexto general del ciberespacio.

Capítulo 1

Conceptos de Hacker y Cracker

El Ciberespacio es una alucinación social consensuada. La matriz tiene sus raíces en las primitivas galerías de juego, en los primeros programas gráficos y en la experimentación militar con conexiones craneales.

The New York Times.

CONCEPTOS DE HACKER Y CRACKER.

TÉRMINO HACKER.

Hacker es una palabra prácticamente intraducible que ha revestido, a lo largo de los años, diversos significados. Pero parece ser que este acrónimo se vincula muy especialmente a los llamados Hacks, se llama así a 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 quiénes lo hacían se denominaban Hackers. De cualquier forma nunca se sabrá con certeza el origen de esta palabra, pero eso hoy por hoy prácticamente da igual, ya que la mayoría de nosotros sabemos que es un Hacker según se nos muestran en los medios de comunicación.

Lo que no se nos ha dicho sobre el Hacking, es quienes son en realidad y que hacen. A menudo leer sorprendentes fechorías o bromas que un grupo de chicos tímidos de gafas gruesas han hecho a tal o cual ordenador, es a su vez una vaga forma de camuflar el verdadero Hacking. Sin embargo hay que reconocer que eso también es una forma de Hackear, pero estamos entrando en otros terrenos que van más allá de la especulación y el saber. Si bien es un grado de clandestinidad o delito introducirse en otro ordenador remoto, lo es también hacer una *fotocopia* en cualquiera página de cualquier libro. De cualquier forma ante unas leyes, la mayoría de nosotros somos unos verdaderos delincuentes.

Los hackers se consideran a si mismos algo así como una élite (en la que los méritos se basan en la habilidad), aunque suelen recibir amablemente a nuevos miembros. Por lo tanto, hay una parte de satisfacción del ego por considerarse a si mismo un hacker. Este grupo es él más experto y menos ofensivo, ya que sus miembros no pretenden serlo, a pesar de que poseen conocimientos de

programación, lo que implica conocer la creación de virus y crack en un software o sistema informático.

Existe otro grupo de personas que se llaman a sí mismos hackers, pero que no lo son, generalmente varones adolescentes que se divierten irrumpiendo ilegalmente en ordenadores y haciendo "phreaking" en el sistema telefónico. Los auténticos hackers tienen un nombre para esas personas: "crackers", y no quieren saber nada de ellos. Los auténticos hackers opinan que la mayoría de los crackers son perezosos, irresponsables y no muy brillantes, y fundamentan su crítica en que ser capaz de romper la seguridad no le hace a uno un hacker, de la misma manera que ser capaz de arrancar un coche con un puente en la llave no le convierte en ingeniero de automotores.

Desafortunadamente, muchos periodistas y escritores utilizan erróneamente la palabra "hacker" para describir a los crackers; esto causa enorme irritación a los auténticos hackers. La diferencia básica: los hackers construyen cosas; los crackers las destruyen.

Según Eric Raymond, el término Hacker hace referencia a "un programador hábil", pero no sólo se queda en la conceptualización, también señala cinco características posibles que definen a un hacker.

1. Una persona que disfruta al aprender los detalles de un lenguaje o sistema de programación.
2. Una persona que disfruta al hacer la programación real en vez de sólo teorizar sobre ella.
3. Una persona capaz de apreciar el hackeo de otro.
4. Una persona que aprende rápidamente a programar.
5. Una persona que es experta en un lenguaje o sistema de programación específico, como ejemplo "un hacker de UNIX". [40]

Pero tal vez una de las más importantes aclaratorias que hace Raymond en relación al término Hacker es desligarlo de cualquier acto delictivo. Al no haber traducción literal al castellano del término, se popularizaron frases como la de "pirata informático", no haciendo justicia a la idea original. De modo que comenzó a darse a conocer el uso de un término para quienes tratan de entrar por la fuerza en los sistemas de otras personas o para quienes, usando sus conocimientos de programación, actúan maliciosamente. Para este grupo de expertos informáticos atraídos por el "lado oscuro de la fuerza", actualmente se utiliza el término "cracker".

Los crackers tienden a agruparse en grupos pequeños, muy secretos y privados, que tienen poco que ver con la poli-cultura abierta y enorme que manejan los hackers; aunque los crackers a menudo se definen a sí mismos como hackers, la mayor parte de los auténticos hackers los consideran una forma de vida inferior.

Un especialista, autor de un extenso cuestionario de 500 preguntas *llamado "The Hacker Test"* y que sirve para que el aficionado evalúe si se encuentra o no en esa peculiar categoría de la cibernáutica, considera:

"El término hacker ha sido terriblemente distorsionado y confundido por los medios estadounidenses en los pasados diez años. Ahora la prensa internacional también ha aprovechado el término para referirse a 'criminales comunes' que se distinguen por usar computadoras. Esas personas NO son hackers EN NINGÚN sentido del término y es trágico que el promedio de la gran mayoría de personas estén expuestos sólo al significado corrupto del orgulloso término hacker. Esta definición de hacker fue creada por Beth Lamb hace mucho tiempo. Ella sabía por experiencia de primera mano lo que realmente son los hackers".

"HACKER, n., un término para designar a alguien con talento, conocimiento, inteligencia e ingenuidad, especialmente relacionadas con las operaciones de computadora, las redes, los problemas de seguridad, etcétera."[59]

Por lo tanto, hay mucho menos en común entre el mundo de los hackers y de los crackers de lo que el lector mundano creé, que confundido por el periodismo sensacionalista, pueda suponer.

En resumen: un hacker es simplemente alguien capaz de manejar con gran habilidad un aparato, no necesariamente un ordenador, con el fin de sacarle más partido o divertirse. ¿Qué hay hoy en día que no sea programable? Desde el reloj de pulsera hasta el vídeo o la radio del coche. Y todos esos pequeños aparatos pueden ser programados y "hackeados" para que hagan cosas que se supone que no pueden hacer. Existe una comunidad, una cultura compartida, de programadores expertos y magos de las redes, cuya historia se remonta décadas atrás a los tiempos de los primeros miniordenadores de tiempo compartido y los tempranos experimentos con ARPAnet. Los miembros de esta cultura crearon el término "hacker". Los hackers construyeron Internet. Los hackers hicieron de Unix el sistema operativo que es hoy día. Los hackers hacen andar Usenet. Los hackers hacen funcionar la www.

Llegados a este punto un Hacker descubre que todo es una farsa y una gran manta secreta que lo oculta todo. El mundo esta lleno de misterios y de demasiados secretismos.

La actividad del Hacking fuera del pc y de la red de Internet, ha cobrado fuerza y es quizás aun más peligrosa que tal como la conocemos a través de los medios de información.

TÉRMINO CRACKER.

Éste fue creado por la comunidad Hacker para referirse a aquellos que usan sus conocimientos con fines poco éticos. Según el diccionario del Hacker el Cracker es una "forma inferior de vida" y a veces es llamado protohacker. Esto se debe a que algunos Hacker pasan por una etapa Cracker, pero al madurar encuentran objetivos más interesantes.

Es el siguiente escalón y el primero de una familia rebelde. Cracker es aquel Hacker fascinado por su capacidad para romper sistemas y software y que se dedica única y exclusivamente a crackear sistemas.

Para la prensa y los grandes fabricantes de sistemas este grupo es el más rebelde de todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica ahí, sino en que normalmente difunden esa rotura por la red para conocimiento de otros, así compartir las ideas y la filosofía de los Hackers.

En la actualidad es habitual ver como se muestran los cracks de la mayoría de softwares, gratuitamente a través de internet. Así es fácil comprender que, un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es, la parte de programación y la parte física de la electrónica.

El tema Cracker también ha quedado suficientemente claro, pero podemos recordar que se trata de un experto Hacker en cuanto a conocimientos profundos de programación y dominio de la tecnología. El Cracker diseña y fabrica programas de guerra y hardware para reventar softwares y comunicaciones como el teléfono, el correo electrónico, o el control de otros ordenadores remotos. Muchos Crackers "cuelgan" páginas web por diversión o envían a la red su última creación de virus polimórfico. También existen Crackers que se dedican a crear cracks para softwares importantes y negocia con ellos. Existen cracks para tarjetas shareware, DVD y las consolas Playstation, X box entre otros.

El noble arte del crakeo es una herramienta para distribuir la riqueza entre la sociedad. Si necesitas un programa (que tienes en un CD-ROM) y no tienes una cuenta en un banco, ni 30 dólares, ¿por qué tenemos que esperar y pagar si lo necesitas?, crackealo y publica el crack en Internet. Así ayudarás a la gente menos afortunada que está asfixiada por esta sociedad desigualitaria.[52]

Además, un programa crakeado es más conocido y utilizado que uno que no lo esté. Digamos que el crack es una forma de publicidad. Basta recordar el compilador de Pascal de la casa Borland. Originalmente fue multicopiado y distribuido casi libremente hasta la saciedad. Borland conocía este hecho y por eso no introdujo ningún tipo de protección. Al cabo de poco tiempo, esos estudiantes se convirtieron en programadores que reclamaban a sus empresas la compra del compilador que sabían utilizar, el Pascal de Borland.

Si las casas de software ya son ricas sin nuestro dinero, ¿a que estado de corrupción se llegaría si lo tuvieran?.

De esa manera muchos jóvenes programadores escriben virus como parte de su aprendizaje, pero la mayoría deja de hacerlo al crecer. Aun así, son responsables de algunos de los virus más complejos que hay. También son responsables de los "Kits de creación de virus" que permitan que casi cualquier novato o neófito cree su propio virus, como fue el caso de el virus Kournikova, creado con un Kit de un programador argentino que usa el apodo de "{k}".

La velocidad con que se suceden los avances tecnológicos, ha provocado en el ser humano una avidez por la información. Junto con ese intentar por conocer cada vez más y asociado también a la informática han aparecido una serie de conductas no validas, que atentan precisamente contra la intimidad del hombre y por ende a la seguridad, y el orden público.

Hasta culminar con una proeza delictiva. Violar los secretos de una comunicación convierten a uno en un Cracker, algo más devastador que un simple fisgoneo de Hacker. Como una extensión mas, surge el **Carding**, otro fenómeno capaz de clonar las tarjetas de crédito bancarias y tarjetas de acceso inteligentes de canales de pago. Después se crean los **Warez**, programas informáticos duplicados para sobrevivir en este devastador mundo de la información.

Así, la clandestinidad impera por todas partes.

CAZA DE HACKERS.

La Caza de Hackers de 1990 fue mayor, mejor organizada, más intencionada, y más decidida que cualquier otra acción previa en el valiente nuevo mundo del delito informático. El Servicio Secreto de Estados Unidos, civiles expertos en seguridad telefónica, y departamentos y brigadas de policía estatales y locales unieron sus fuerzas en un decidido esfuerzo por aplastar la cabeza del underground [1] electrónico americano. Fue una campaña fascinante, con resultados muy dispares.

La Caza de Hackers tuvo otro efecto sin precedentes; provocó la creación, dentro de la "comunidad informática", de la *Electronic Frontier Fooundation*, un nuevo y extraño grupo de presión, tenazmente dedicado al establecimiento y la protección de los derechos civiles electrónicos. La Caza, notable por sí misma, creó un tumultuoso debate sobre el delito electrónico, las penas, la libertad de prensa, y cuestiones referentes a registros y confiscaciones de bienes. La política ha entrado en el ciberespacio. [40]

[1] El término *underground* tuvo su momento de difusión alrededor del primer lustro de los sesenta, con tal término, lo clandestino y lo subterráneo parecían tener el objetivo de efectuar una lenta pero radical conspiración en contra de la cultura oficial y dar paso a una nueva cultura. Es todo tipo de Información cubierta por el Gobierno, la NASA, el FBI, la CIA, la KGB, la DEA, los Bancos y todo aquel que esta en contra del flujo de información.

Tampoco es cierto que el Hacker surja a raíz de la nueva era informática, ya que el Hacker siente gran interés por averiguar, y eso puede aplicarse a las comunicaciones, que existieron mucho antes que los ordenadores. Así, se desmiente que los Hackers surjan en era temprana, puesto que ya en la Segunda Guerra Mundial se trataba de descifrar mensajes del enemigo.

Sin embargo, es ahora cuando proliferan los Hackers dada la importancia que cobran la informática y la red de internet hoy día. Los verdaderos Hackers aprenden y trabajan solos y nunca partiendo de las ideas de otros.

CIBERCULTURA.

Bajo el influjo de las nuevas tecnologías de la información, se está dando impulso a la llamada *economía de redes*, que a decir de los expertos, dependerá en gran medida de cuatro grupos de tecnologías: de cómputo, telecomunicaciones, biotecnología y nanotecnología. La nueva economía sustentada en las tecnologías digitales, poco a poco da paso a otras realidades sociales.

La cibercultura puede ser entendida como un proceso de digitalización del mundo, que permite nuevas formas de control sobre el planeta, así como nuevas posibilidades de poderosos vínculos entre seres humanos, naturaleza y máquinas. La cibercultura es la cultura de la producción informativa y al ser un movimiento cultural alternativo, ha provocado grandes innovaciones en cuanto al modo de tratar, manejar y difundir la información, y sobre todo ha implicado una mayor democratización en el manejo de la misma a nivel internacional.

El estilo de vida cibercultural ha implicado una proliferación de comunidades virtuales, las cuales basan su teoría y practica en los principios de libertad, igualdad y fraternidad, conceptos que han sido, en diferentes perspectivas, los ideales de diversas utopías, movimientos anarquistas y revoluciones.

Las comunidades virtuales pretenden potenciar un ambiente de democracia, educación, ciencia y vida intelectual en donde prevalezca la libertad de expresión, la tolerancia y una diversidad cultural. Los grupos que luchan por tales ideales, tienen sus orígenes en la contracultura, fenómeno social, especialmente juvenil, surgido en las sociedades capitalistas.

La contracultura se opone al contexto establecido por la cultura dominante, sin llegar a propugnar la barbarie o ausencia total de cultura; supone un rechazo u oposición al establecimiento cultural y ofrece una opción a los modelos conservadores.

Vinculados con tales movimientos, se encuentran los grupos de hackers, cypherpunks y zippies -entre otros- , quienes manifiestan concepciones diversas sobre el flujo de la información digital a través de las redes.

Aunque no es exactamente "real", el "ciberespacio" es un lugar que existe. Hay cosas que ocurren allí y que tienen consecuencias muy reales.

Pero en los últimos veinte años, este "espacio" eléctrico, que antes era delgado, oscuro y unidimensional - poco más que un estrecho tubo, estirándose de un teléfono a otro - se ha abierto explosivamente. Hoy en día tiene sentido hablar del ciberespacio como de un lugar. Porque ahora la gente vive en él. [39]

Capítulo 2

Los Habitantes del Ciberespacio.

...Sólo en el último año había crackeado más de veinte Sistemas de televisión de paga. Su habilidad para localizar los códigos le permitía abrir con cierta facilidad el algoritmo que las tarjetas de acceso contenían en su interior. Con poco más que un DataLogger y un PC de sobremesa, Danker se pasaba horas y horas buscando los Key Updates de la tarjeta de control de abonados. Era una tarea que requería cierta paciencia, y eso era precisamente lo que más tenía Danker. Sin embargo no ocurría así con la policía de Ciberdelitos informáticos. Ésta, al contrario de Danker, tenía muy poca paciencia, y nada digamos de la habilidad de conseguir códigos. Su afán era simplemente dar con la guarida de Danker, pero éste era demasiado escurridizo para los novatos policías y además no cometía el error de comercializar los códigos bajo ningún soporte. Simplemente alguien se encargaba de ello y Danker cobraba su cheque en dinero negro…

La Machi David

2. LOS HABITANTES DEL CIBERESPACIO

Habría muchas formas de clasificar a los habitantes del ciberespacio, pero la más corriente de ellas es según los conocimientos de que disponen en cuanto al medio en el que circulan. Así, hay usuarios caseros, gente relativamente informada sobre el funcionamiento de las cosas, usuarios medios, técnicos, programadores y Hackers. De ahí la confusión con el verdadero rol de los Hackers.

2.1. PHREAKER.

Se caracterizan por poseer bastos conocimientos en el área de telefonía terrestre y móvil, incluso más que los propios técnicos de las compañías telefónicas; Se le podría llamar el cracker de los teléfonos. Sin embargo, últimamente un buen Phreaker deberá contar con amplios conocimientos de informática, ya que la telefonía celular y el control de pequeñas centrales telefónicas es la parte primordial a tenerse en cuenta, y/o emplean la informática para el procesamiento de datos y para clonar tarjetas de prepago en telefonía celular.

Sobre todo emplea sus conocimientos para poder utilizar las telecomunicaciones gratuitamente.

2.2. WIZARD.

Definitivamente es algo superior a un hacker. La diferencia es que éste se especializa en un área muy específica en software o hardware.

Es la persona que conoce a fondo como funciona una pieza compleja de equipo. Especialmente si puede reparar un sistema rápidamente en casos de emergencia, tal vez con algo de magia profunda, es decir usando instrucciones o técnicas que resultan completamente incomprensibles a los simples mortales. Mientras que un Hacker puede usar algunas técnicas avanzadas, es el Wizard el que entiende como o por que funcionan.

2.3. GURUS.

The best of the best. Lo más alto que se puede llegar a ser. Son los maestros y enseñan a los futuros Hackers. Normalmente se trata se personas "adultas", se dicen "adultas", dado que la mayoría de Hackers son personas jóvenes, que tienen amplia experiencia sobre los sistemas informáticos o electrónicos y están de alguna forma para enseñar o sacar de cualquier duda al joven iniciativo al tema. El guru no esta activo, pero sigue absorbiendo conocimientos ya que sigue practicando, pero para conocimientos propios y solo enseña las técnicas más básicas.

2.4. LAMER.

Este grupo es tal vez el más numeroso y quizá con mayor presencia en la red. Normalmente son individuos con ganas de hacer hacking, pero carentes de todo conocimiento. Habitualmente son individuos que apenas si saben lo que es un ordenador, pero su uso y las grandes oportunidades que brinda internet, convierten al nuevo internauta en un ser obsesivo que lee, busca y rebusca en internet toda la información que pueda encontrar. La posibilidad de entrar en otro sistema remoto o la posibilidad de girar un gráfico en la pantalla de otro ordenador los fascina totalmente.

Pero solo es un aficionado al tema. Es aquel que ha visitado varias páginas web sobre hacking y fascinado, se ha bajado unos cuantos programas (virus, troyanos). Después los usa indebidamente sin tener conocimientos; destruye su propio ordenador lo mismo que otros de la red, y cuando eso sucede se siente alguien superior a los demás. Este tipo de personaje es el que emplea los BackOrifice[2],

[2] **BackOrifice:** Puerta trasera de entrada a una computadora, programa o sistema en general. Es utilizado para acceder sin usar un procedimiento normal.

Netbus[3] y Virus con el fin de fastidiar y sin tener conocimiento de lo que realmente está haciendo. Es el último eslabón de la nueva cibersociedad.

Es el típico tipo que dice ser un hacker, pero que no tiene ni vaga idea, se creen dioses por enviar un virus por internet (que ellos no han programado, no han escrito ni una línea de código).

Éste es quizá el grupo que más peligro representa para la red ya que los Lamers ponen en práctica todo el software de hackeo que encuentran en la red. Es fácil ver como un Lamer prueba a diestro y siniestro un "bombeador de correo electrónico" esto es, un programa que bombardea el correo electrónico ajeno con miles de mensajes repetidos hasta colapsar el sistema, y después se mofa autodenominándose Hacker.

También emplean de forma habitual programas sniffers[4] para controlar la red, interceptan contraseñas y correo electrónico y envían después varios mensajes con dirección falsa amenazando el sistema. En realidad no pueden hacer nada más, pero poseen el control de tu disco duro aún teniendo el ordenador apagado. Toda una negligencia en un terreno tan delicado.

2.5. COPYHACKERS.

Es una nueva raza sólo conocida en terrenos del crackeo de hardware, mayoritariamente en el sector de las tarjetas inteligentes empleadas en sistemas de televisión de pago. Este mercado mueve al año más de 150 millones de euros sólo en Europa. [55]

[3] **NetBus:** Al igual que BackOrifice, ambos son los troyanos mas conocidos que abren una puerta trasera a un equipo basado en Windows 95, Windows 98, Windows NT o Windows XP.

[4] **Sniffer:** Es un programa que permite "escuchar furtivamente" en redes de medios de comunicación compartidos (tales como Ethernet). Se ejecuta como una maquina que esta conectada a la red, en modo Promiscuo y captura el tráfico de todo el segmento de la red.

En 1994 los Copyhackers vendieron tarjetas por valor de 96 millones de euros, en pleno auge de los canales de pago como el grupo SKY y Canal+ plus.
Estos personajes usan la ingeniería social para convencer y entablar amistad con los verdaderos Hackers, les copian los métodos de ruptura y después los venden a los "bucaneros", personajes que se detallarán más adelante.

Los Copyhackers deambulan en la sombra, entre el verdadero Hacker y el Lamer. Estos personajes poseen conocimientos de tecnología y viven dominados por la obsesión de ser superiores, y no terminan de aceptar su posición. Por ello "extraen" información del verdadero Hacker para terminar su trabajo. La principal motivación de estos nuevos personajes es el dinero.

En la actualidad el número de CopyHackers ha crecido de forma alarmante debido a los Hacks de los sistemas Mediaguard, Nagra, Irdeto o Viacces. Estos acrónimos se corresponden a los principales sistemas de Encriptación empleados por las más importantes Plataformas de Televisión Digital Europeas. Toda esta situación ha propiciado negocios ilícitos en este sentido lo que ha disparado el interés por conocer estas técnicas fraudulentas.

2.6. NEWBIE.

Es el típico "cacharrero" de la red, sin proponérselo tropieza con una página de Hacking y descubre que en ella existen áreas de descarga de buenos programas de Hackeo, baja todo lo que puede y empieza a trabajar con ellos. A veces se introduce en un sistema fácil y a veces fracasa en el intento, porque ya no se acuerda de ciertos parámetros y entonces tiene que volver a visitar la página WEB para seguir las instrucciones de nuevo. Es el típico tipo, simple y nada peligroso.

Al contrario de los Lamers, los Newbies aprenden el hacking con paso cauto y no se mofan con sus logros sino que aprenden.

2.7. SCRIPT KIDDIE.

Denominados Skid kiddie o Script kiddie, son el último escalón. Se trata de simples usuarios de internet, sin conocimientos sobre hack ni sobre crack en su estado puro. En realidad son devotos de esos temas, pero no los entienden, simplemente son internautas que se limitan a recopilar información de la red. En realidad se dedican a buscar en la red programas de hacking y los ejecutan sin leer primero los ficheros "readme" de cada aplicación. Son los responsables de muchos ataques sin sentido. Con esta acción liberan virus que hacen colapsar ellos mismos su propio ordenador. Esta forma de actuar con total desconocimiento del tema los lleva a probar y probar aplicaciones de hacking. Podrían llamarse "pulsabotones" de la red. En realidad los Kiddies no son útiles para el progreso del hacking.

Kiddies, sinónimo de pulsar botón y generar caos. Normalmente jóvenes ávidos de fama, con pensamientos desbordados y confusos y sobre todo, defensores de los Ataques de Denegación de Servicio.

2.8. BUCANEROS.

Son los comerciantes de la red más no existen en ella; Pero son peores que los Lamers, ya que no saben de tecnología ni aprenden nada. Comparados con los piratas informáticos, los bucaneros sólo buscan el comercio negro de los productos entregados por los Copyhackers. Los bucaneros sólo tienen cabida fuera de la red, ya que dentro de ella los que ofrecen productos "crackeados" pasan a denominarse "piratas informáticos". Así las cosas, el bucanero es simplemente un comerciante sin escrúpulos a la hora de explotar un producto de cracking a nivel masivo.

2.9. PIRATA INFORMÁTICO.

Comúnmente confundido con un Hacker, el pirata informático es el que hace copias de software en CD o fabrica tarjetas ISO 7816 piratas y comercializa con ellas. No posee más conocimientos que los necesarios para duplicar discos, y es el grupo que más ensucia la nueva sociedad de Hackers, después de los Lamers. A pesar de toda la información que existe a estas alturas, todavía se les contempla como Piratas Informáticos a los que de alguna u otra manera realizan cualquier tarea con el ordenador que consideran no ilícita. En definitiva, para algunos medios de comunicación, preferentemente Televisiones, todos son Piratas Informáticos, el que escribe un virus, el copia un CD o el manipula Tarjetas de Crédito.

Capítulo 3

Historias de Hackers & Crackers

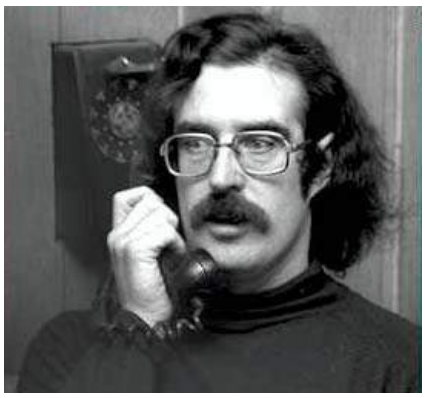
Solo unos pocos conocen la tecnología
y muchos son los que la ponen en práctica de una manera sencilla.

3.0. HISTORIAS DE HACKERS & CRACKERS

En la década de los 70¨ las computadoras se volvieron importantes al igual que los Hackers, también en esta época el ser Hacker prometía puestos y sueldos importantes aunque al verdadero Hacker esto le importaba poco, los Hackers dejaban importantes ganancias pidiendo muy poco a cambio, los creadores del procesador de palabras, el correo electrónico y la hoja de calculo nunca ganaron ni un centavo.

Justamente por esta época nació la ética del Hacker. El primer hack clásico, no tiene que ver nada con las computadoras, sino con los sistemas telefónicos.

3.1. DRAPER JOHN, "CAPTAIN CRUNCH"



En septiembre de 1970 John Draper, también conocido como Captain Crunch, descubre el obsequio (un silbatito) ofrecido en las cajas de cereal *Captain Crunch*, curiosamente este silbato generaba la frecuencia de tono de 2600 hertzios, que resulta que era exactamente el tono de control de los sistemas de telefonía de larga distancia de los teléfonos Bell (AT&T más tarde). Practicando con el silbato logro reproducir las secuencias de control y conseguir llamadas de larga distancia gratis. Pronto descubrió como hablar consigo mismo (una llamada que daba la vuelta al mundo tenia un retraso de 20 segundos). (Ver fig. 2.1)

El hack no consiste en hacer llamadas telefónicas gratuitas, sino poder utilizar un simple silbato para tener acceso a todo el sistema telefónico, actualmente se le conoce como prheaker al experto en entrar a los sistemas telefónicos y sistemas de comunicación.

Este descubrimiento llevo a John a crear la primera "Blue Box" una caja electrónica mágica para los teléfonos. En su *honor*, se fundo la revista 2600 de la comunidad hacker.

"Esquire Magazine" publica los secretos de la pequeña caja azul con las instrucciones para construirla, el fraude fue ocasionado a AT&T en los Estados Unidos. Algunos de ellos son los universitarios *Steve Wozniak* y *Steve Jobs*, los futuros fundadores de Apple, quienes inician una empresa personal que se dedica a vender y construir blue boxes.

En Mayo de 1972 John Draper (Capitán Crunch) es arrestado por delitos de phreaking y es condenado a cuatro meses en la prisión de Lompoc de California.

3.2. DENNIS RITCHIE, KEN THOMPSON Y BRIAN KERNIGHAN. Estos tres mosqueteros del chip son buenos programadores y trabajan para Bell Labs. Es como si esa empresa sólo gestara buenos Hackers. Los tres están especializados en el entorno UNIX y en el lenguaje C.

Estos hombres han tenido que ver, y mucho, con el nacimiento de Internet y su desarrollo. De no haber estado ellos en ese proyecto, Internet quizás no existiría ahora, y de existir sería muchísimo más lento. En la actualidad Ritchie está trabajando en el Plan 9 de Bells Labs, un sistema operativo de última generación que vendrá a sustituir a UNIX. Thompson y Kernighan siguen trabajando todavía como Hackers, algo que siempre los motivó a seguir viviendo con cierta ilusión.

3.3. MARK ABENE, AKA PHIBER OPTIK. Abene se afiló los dientes en una Radio Shack TRS-80 (Trash-80) y escaló posiciones en la red de telecomunicaciones nacional de EE.UU. hasta que se encontró a sí mismo en la lista de las 100 personas más listas de una revista neoyorquina. Abene fue miembro fundador de Master of Deception y se le atribuye la inspiración de toda una generación de hackers.

3.4. HOLLAND WAU Y WENERY STEFFEN. *"Lo logramos, por fin … Sólo hay algo seguro, la infinita inseguridad de la seguridad".* Fue lo que escribió Wau Holland, en su cuaderno de notas, el 2 de mayo de 1987. Los 2 hackers alemanes, de 23 y 20 años respectivamente, habían ingresado sin autorización al sistema de la central de investigaciones aeroespaciales más grandes del mundo (NASA).

¿Por qué lo hicieron?, "Porque es fascinante, la única aventura posible está en la pantalla de un ordenador", respondieron.

Cuando Wau y Steffen advirtieron que los técnicos los habían detectado, les enviaron un telex, avisando de su intrusión.

3.5. ING – HOU CHEN. Taipei, Taiwan, Abril 30 de 1999. El autor del virus "Chernobyl", dijo a los investigadores que el creó el bug con la esperanza de humillar y vengarse de los que llamo "proveedores incompetentes de antivirus software". Pero él admitió que no esperaba que CIH (iniciales del autor) causaran daño alrededor del mundo. Este virus devastó cientos de miles de computadoras alrededor del mundo. Chen creó el virus en Abril, cuando todavía era estudiante de ingeniería computacional en el Instituto Tecnológico de Taiwán. Este inusual virus destructivo, programado para funcionar el 26 de Abril, (13° aniversario del desastre nuclear de Chernobyl), trata de borrar el disco rígido y escribir "basura" en algunos otros componentes, evitando de este modo el futuro encendido de la computadora.

3.6. LEVIN VLADIMIR

Matemático ruso de 24 años, desde su computadora instalada en la empresa *AO Saturn*, de San Petersburgo irrumpió los sistemas informáticos centrales del banco Citybank en Wall Streat, este pirata logro transferir a diferentes cuentas de E.E.U.U., Rusia, Finlandia, Alemania, Israel, Holanda y Suiza fondos por un valor de 10 millones de dólares, según el FBI. Detenido en el Reino Unido a principios de 1995, Levin espera que los tribunales británicos se pronuncien sobre una demanda de extradición solicitada por E.E.U.U. (Ver fig. 2.2)

A pesar de que la sustracción fue superior a los 10 millones de dólares, Levin fue sentenciado a 3 años de prisión y a pagar la suma de 245.000 dólares a favor del Citibank, ya que las compañías de seguros habían cubierto los montos de las corporaciones agraviadas.

3.7. KEVIN Y RONALD. Kevin y Ronald, con los nombres de guerra Makeveli y TooShort en el ciberespacio, asaltaron los ordenadores del Pentágono en Marzo del año 1998, a la edad de 17 años. Estos dos forajidos virtuales, con sus conocimientos y con un equipo básico informático, se introdujeron en cuatro sistemas de la Marina y siete de las Fuerzas Aéreas, relacionados con centros digitales de Estados Unidos y Okinawa.

3.8. LA MACHINA DAVID. En 1994 David La Machina, estudiante de 20 años del prestigioso y serio MIT (Institución Universitaria), reconoce que ha distribuido en Internet multitud de programas informáticos obtenidos sin licencia y por un valor de un millón de dólares. Para ofrecerlos a los cibernautas monto su propia Vd.

3.9. MITNICK KEVIN, "EL CÓNDOR", "EL CHACAL DE LA RED". Kevin David Mitnick es quizás el más famoso hackers de los últimos tiempos. Nacido el 6 de Agosto de 1963 en Van Nuts, California. Como Hacker, la carrera de Mitnick tiene sus inicios en 1980 cuando apenas contaba con 16 años y, obsesionado con las redes de computadoras, rompió la seguridad del sistema administrativo de su colegio, pero no para alterar sus notas, lo hizo "solo para mirar".

La primera vez que lo detuvieron fue en 1981 por robar manuales de la Pacific Telephone. La información robada tenía un valor equivalente a los 200 mil dólares y tuvo que cumplir una condena de tres meses de cárcel y un año bajo libertad condicional. (Ver fig. 2.3)

En 1982 Kevin entró de forma ilegal en un servidor del ministerio defensa y en aquella ocasión, tuvo la precaución de modificar el fichero de rastreo de llamadas, para no ser localizado. Sin embargo, un año más tarde si fue localizado y arrestado, tras entrar a través de Arpanet, a los ordenadores del pentágono. En esta ocasión fue condenado a seis meses en un reformatorio. Y fue a partir de aquí cuando Kevin, se convirtió en leyenda. El hecho de haber entrado y romper las barreras del *"North América Air Defense Command Computer"* le convirtió en el Cóndor y la nueva leyenda.

En 1983 intento ingresar en las computadoras de la Universidad de California del Sur y poco después penetró el sistema de la agencia de créditos TRW. En 1987 lo condenaron a tres años de libertad condicional por robo de software, tras hackear los sistemas del Departamento de Defensa de E.E.U.U. y la NASA.

Durante este tiempo le negaron el acceso a los teléfonos y a lo largo de los doce meses de rehabilitación no pudo acercarse a una computadora. Más tarde, y ya en libertad, se apodero de 16 códigos de seguridad de MCI y junto a un amigo, Jenny Di Cicco, entraron en la red del laboratorio de investigaciones de Digital Corporation, conocida como Easynet.

Ambos hackers querían obtener una copia del prototipo del nuevo sistema operativo de seguridad digital llamado vms. El personal de seguridad de Digital se dio cuenta inmediatamente del ataque y dieron aviso al FBI, comenzando a rastrear hackers.

Mitnick fue arrestado en 1988 por invadir el sistema de Digital Equipment. La empresa acuso a Mitnick y a DiCicco ante un juez federal de causarles daños por 4 millones de dólares en el robo de su sistema operativo. Fue declarado culpable de un cargo de fraude en computadoras y de uno por posesión ilegal de códigos de acceso de larga distancia.

Adicional a la sentencia, el fiscal obtuvo la orden de la corte que prohibía a Mitnick el uso del teléfono en la prisión alegando que el prisionero podría obtener acceso a las computadoras a través de cualquier teléfono. A petición de Mitnick el juez lo autorizo a llamar únicamente a su abogado, a su esposa, a su madre y a su abuela y solo bajo supervisión de un oficial de la prisión.

Este caso produjo revuelo en los estados unidos no solo por el hecho delictivo sino por la táctica que utilizo la defensa. Su abogado convenció al juez que Mitnick sufría de una gran adicción por las computadoras equivalente a la de un drogadicto, un alcohólico o un apostador. Gracias a esta maniobra de la defensa solo fue sentenciado a solo un año de prisión y al salir de allí debía seguir un programa de seis meses para tratar su "adicción a las computadoras".

Durante su tratamiento le fue prohibido tocar una computadora o un modem y llego a perder más de 45 kilos.

Para 1991 ya era el hacker que había ocupado la primera plana del New York Times y uno de sus reporteros, John Markoff, decidió escribir un libro de estilo Cyberpunk narrando las aventuras de Mitnick. Al parecer a Mitnick no le gusto el libro, ya que luego de salir a la venta, la cuenta de Internet de Markoff fue invadida, cambiando su nivel de acceso, de manera que cualquier persona en el mundo conectada a Internet podía ver su correo electrónico.

En 1992, y luego de concluir su programa, Mitnick comenzó a trabajar en una agencia de detectives. Pronto se descubrió un manejo ilegal en el uso de la base de datos y fue objeto de una investigación por parte del FBI quien determino que había violado los términos de su libertad condicional. Se ofreció una recompensa de un millón de dólares a quien arrestara a Mitnick.

Luego de convertirse en prófugo de la justicia cambio de táctica y concluyo que la mejor manera de no ser rastreado era utilizando teléfonos celulares.

Después de varios intentos infructuosos, en cuanto a calidad de información, se encontró con la computadora de Tsutomu Shimomura norteamericano de origen japonés, la cual invadió en la Navidad de 1994.

Shimomura, físico computista y experto en sistemas de seguridad del San Diego Supercomputer Center, Shimomura estaba considerado como uno de los hackers de "sombrero blanco" más cualificados de los Estados Unidos, ya que cuando hallaba una falla de seguridad de algún sistema lo reportaba a las autoridades, no a otros hackers.

Shimomura noto que alguien había invadido su computadora en su ausencia, utilizando un método de intrusión muy sofisticado y que el nunca antes había visto. El intruso le había robado su correo electrónico, software para el control de teléfonos celulares y varias herramientas de seguridad en Internet. Allí comenzó la cuenta regresiva para Mitnick. Shimomura se propuso con orgullo personal atrapar al hacker que había invadido su privacidad.

Mas tarde, el 16 de febrero de 1995, Mitnick fue capturado, juzgado y condenado a 25 años de prisión, lejos de computadoras y teléfonos. Pero, el 22 de Marzo de 1999, se consigue un acuerdo de jueces y fiscales. (Ver fig. 2.4)

Los términos concretos se desconocen, pero se sabe que en marzo del 2000 Mitnick quedaría en libertad con la condición irrevocable de no poder acercarse a una computadora.

Kevin Mitnick, este sencillo nombre, oculta la verdadera identidad de uno de los mayores crackers de la historia. Fue una de las mayores pesadillas del Departamento de justicia de los Estados Unidos. Entro virtualmente en una base de misiles, llego a falsificar 20,000 números de tarjetas de crédito y a causar pérdidas millonarias a varias empresas.

Cuando fue liberado en enero de 2000 y en virtud del acuerdo al que había llegado con las autoridades, pagaría 4125 dólares (nada comparado con el millón y medio de dólares que pedía la Fiscalía, o con los cientos millones que reclamaban las compañías perjudicadas) y debía mantenerse alejado durante dos años de ordenadores, teléfonos móviles y similares "artefactos". Aconsejado por sus abogados, en marzo de 1999, para evitar ser enjuiciado, reconoció haber entrado nada más y nada menos que en Motorola, Sun Microsystems Inc., NEC Corp., Novell, Pacific Bell entre otras compañías gigantescas.

Si el Cóndor ha sido domado es una cuestión que podrá comprobarse en el futuro, ha mostrado su interés por estudiar informática en una universidad norteamericana, parece que prepara un libro y ha colaborado con el Senado norteamericano como asesor de seguridad.

Ahora, ya libre, fundó su propia compañía de seguridad *Defensive Thinking Inc*. en Los Angeles, California, y bajo la idea de *"¿Quién mejor que yo, puede decirte como protegerte?"* creó una idea comercial para vender, lo que llamó "Pensamiento defensivo" y son una serie de cursos en donde, en teoría, enseñan a protegerse de los ataques por Ingeniería Social.

Pero... siempre hay peros... resulta que la leyenda y su nueva empresa de seguridad sufrieron la indignidad de ser victimas de hackers en dos ocasiones durante los primeros meses del 2003. Un hacker que se hace llamar "BugBear" el 30 de enero del 2003 agregó una página al sitio web de la empresa de Mitnick que decía *"Welcome back to freedom, Mr. Kevin"* (Bienvenido a la libertad Sr. Kevin) y el intruso agregó *"it was fun and easy to break into your box."* (fue divertido y fácil irrumpir en tu sitio).

El segundo ataque fue un domingo de febrero del mismo año, por un hacker texano, que después de su proeza, el hacker le mandó un mail a Kevin en el cual le pedía que lo contratara como Jefe de Seguridad de su empresa.

Kevin Mitnick declaró a la prensa:

"All the hackers out there figure if they can hack Kevin Mitnick's site, they're the king of the hill."

(Todos los hackers que andan ahí afuera se imaginan que si ellos pueden hackear el sitio de Kevin Mitnick, serán el Rey de la Colina.)

3.10. MURPHY IAN, "CAPTAIN ZAP". En Julio de 1981 Ian Murphy, un muchacho de 23 años que se autodenominaba "Captain Zap", gana notoriedad cuando entra en los sistemas en la Casa Blanca, el Pentágono, BellSouth Corp. TRW y deliberadamente deja su currículum.

Ian Murphy hizo historia convirtiéndose en el primer hacker a quien se le consideró culpable de felonía por atacar hardware militar. También logró cambiar el reloj de facturación de los ordenadores de AT&T, para conseguir llamadas más baratas durante el día. Inspiración de la película "Sneakers" de 1992, Murphy se ocupa ahora de negocios legales en IAM/Secure Data Systems.

3.11. "PAINT" Y "HAGIS". Son los seudónimos de los dos hackers que el 10 de Diciembre de 1997 accedieron a uno de los buscadores mas utilizados en Internet. Los terroristas informáticos autodenominados "Paints & Hagis", ¡accedieron al servidor del popular navegador Yahoo! y dejaron un mensaje amenazante:

"¡Todos los que el mes pasado utilizaron el motor de búsqueda Yahoo! han adquirido una bomba lógica que se activará el día de Navidad,

Sembrando el caos en todas las redes informáticas del planeta". Y añadían que solo entregarían el antídoto del virus si Mitnick, condenado a 35 años de prisión, quedaba en libertad. El efecto de llamar la atención sobre el caso Mitnick se había conseguido.

Si cumplían con sus requisitos, el programa antídoto, oculto en un ordenador, sería suministrado a los cibernautas. Todo se quedó en palabras, porque según la portavoz de Yahoo, los hackers accedieron a la página de la empresa, pero no destruyeron ni infectaron nada. Todo fue una falsa alarma... pero ¿y sí hubiera sido cierto?.

Este no resulto ser más de una modificación de una página web, y un ejemplo temprano de las muchas que se modifican hoy día a día.

3.12. "ON THE FLY". Recientemente un joven holandés que utiliza el seudónimo de "OnTheFly", bajó de la red un Kit llamado "Vbs Worm Generator", se puso a jugar y en 5 minutos armo un virus, y luego se olvido de el. Al día siguiente se entero por las noticias que su virus, conocido ahora como "El virus Ana Kournikova" estaba causando estragos por todo el mundo. Asustado se entrego a las autoridades de su pueblo, quienes felices porque la publicidad había atraído notoriedad al pequeño pueblo de "Sneek", lo regañaron y luego le ofrecieron empleo. Ante este ejemplo, se desato una ola de virus creados en estos Kits, la mayor parte muy mal hechos.

3.13. ONEL DE GUZMAN. En contraste hay jóvenes que toman el código de los virus y lo modifican, a veces sin comprender su alcance, por lo que son llamados aprendices de brujo. Un ejemplo es Onel, un estudiante de programación filipino, el resintió mucho que su tesis, que trataba sobre un virus que robaba passwords, fuera rechazada por poco ética, así que tomo el virus de Valiant, lo modifico y lo libero al mundo (según el por accidente).

Este estudiante no se puede considerar un verdadero Hacker, sus habilidades de programación no parecen ser muy buenas, muchos expertos que analizaron el código llegaron a la conclusión de que estaba sin acabar o que estaba muy mal escrito. Sin embargo eso no impidió que **I love You** causara estragos en la red. Ahora Onel fue capturado y apresado, pero resulta que en Filipinas no hay ninguna ley para su caso. Eventualmente fue dejado en libertad y se le ofreció trabajo como programador. (Ver fig. 2.5)

3.14. POULSEN KEVIN, "DARK DANTE". En 1982 este hacker de los Angeles, se introdujo en la red de intercambio de datos Arpa del Pentágono, la precursora de la actual Internet. La primera opción, en el esquema virtual que poseían, era adivinar la palabra clave de acceso al sistema. Lo lograron al cuarto intento, utilizando las letras UCB, las iniciales de la Universidad de California, en Berkeley. Este saqueador, aumento la capacidad del usuario ordinario UCB, diseñando una subrutina para "captar" los privilegios del "súperusuario".

Su "ciberpaseo" terminó al intentar ojear unos ficheros "cebo", preparados para mantener el mayor tiempo posible conectados a los hackers, pero no sin antes sacar algo de provecho: el manual de Unix, el sistema operativo multitarea, diseñado por los laboratorios Bell (organismo de investigación de la ATT) la mayor compra a la compañía telefónica de EE.UU.

Como Cracker, siguió el mismo camino que Kevin Mitnick, pero fue mas conocido por su habilidad para controlar el sistema telefónico de Pacific Bell. Incluso llego a ganar un "Porsche" en un concurso radiofónico, si su llamada fuera la 102, y así fue, realizo 2000 llamadas simultáneas a la estación de radio.

3.15. THE MENTOR Y GRUPO H4G13. El autodenominado grupo H4G13, con Mentor a su cabeza quería demostrar hasta donde eran capaces de llegar, y lo dejaron plasmado de una manera efectiva, colocando en la pagina principal de la NASA, durante media hora, el "manifiesto" hacker mas conocido hasta el momento.[5]

3.16. BARAM PAUL. Posiblemente el mayor hacker de la historia. Ya hackeaba Internet antes de que existiera. El fue quien introdujo el concepto de hacker. Baran comenzó a construir lo que hoy día es un navegador.

3.17. GATES, BILL Y ALLEN, PAUL. En sus tiempos de aprendices, estos dos hombres de Washington se dedicaban a hackear software. Grandes programadores. Empezaron en los 80 y han creado el mayor imperio de software de todo el mundo, *MICROSOFT*.

---

5 "Las últimas palabras del Mentor": Otro ha sido detenido hoy. Todo está reflejado en los papeles. "Joven arrestado en un escándalo informático" "loco de las computadoras arrestado por meterse en un Banco". Están todos iguales. ¿Desearías saber qué le hacía tic-tac?, ¿qué fuerzas lo formaron y qué lo había amoldado? Yo soy un hacker, entra en mi mundo. Todo comienza en la escuela. Soy más inteligente que la mayoría de los otros niños (...). Este es mi mundo ahora. El mundo del electrón y de la conexión, de la belleza del baudio. Hacemos uso de un servicio ya existente sin pagar, y para qué hacerlo más barato si no puede moverse por culpa de unos aprovechados glotones, y tú nos llamas a nosotros criminales. Nosotros exploramos... y tú nos llamas criminales. Ambicionamos el conocimiento... y tú nos llamas criminales. Nosotros existimos sin color de pelo, sin nacionalidad, sin religión predispuesta... y tú nos llamas criminales. Construyes bombas atómicas, emprendes guerras, asesinas, timas y nos mientes, y tratas de hacemos creer que es por nuestro propio bien, sin embargo, nosotros somos los criminales...

Si, soy un criminal. Mi crimen es el de la curiosidad. Mi crimen es el de juzgar a personas por lo que dicen o piensan, no por lo que parecen. Mi crimen es el de ser más listo que tú, algo que no me perdonarás nunca. Soy un loco de las computadoras, soy un hacker... y éste es mi manifiesto. Detendrán a este individuo, pero no podrán detenernos a todos, después de todo, estamos todos igual. Firmado: El Mentor.

3.18. RICHARD STALLMAN. Stallman creó el sistema operativo GNU, con el intrigante título de *GNU Not Unix* y siempre ha brillado por su gran capacidad para programar, todavía hoy utiliza para trabajar una máquina bastante antigua, se trata de una DEC PDP-10. Stallman se integró al laboratorio de Inteligencia Artificial del MIT en 1971, lo que le valió para crear sus propias aplicaciones de Inteligencia Artificial. Fue recompensado con el premio McArthur Genios por sus trabajos. En la actualidad Stallman se dedica a crear miles de utilidades gratuitamente para entornos UNIX.

Cuando el software empezó a desplazarse en dirección a Microsoft, Richard Stallman se empezó a preocupar sobre el desarrollo de propiedad restringida y estableció la *Free Software Foundation.*

Por supuesto que existe alguien más, y de ahí la confusión con el verdadero rol de los Hackers. Después de estos están los Crackers, "Hackers de élite, rebeldes," que difunden sus conocimientos por la red en forma de software que otros utilizarán indebidamente. Los Crackers revientan sistemas y roban información de los ordenadores ajenos. También están los Lamers y los Newbies, esto es, novatos que bajan de las páginas de otros "aficionados" programas sniffers, escaneadores o virus para luego emplearlos para usar con el ratón, ya que no hace falta ser un experto programador para dirigir el puntero del ratón sobre cada pestaña de un programa descargado.

Pero el grupo que mejor merecido tiene el nombre, es el formado por aquellos que no se denominan Hackers, en este caso son expertos en seguridad que detectan fallos o bugs en los sistemas y lo hacen público para que las empresas del software "dañado" les ponga remedio.

Capítulo 4

Términos Comunes y Herramientas.

La comercialización de Internet y los abusos de poder están en la diana de los "hacktivistas". La Red dejó de ser un mero medio de comunicación para convertirse en el campo y objetivo mismo de la contienda. Se trata siempre de gestos simbólicos para expresar la discrepancia, que no implican daño físico ni violencia.

Laura G. De Rivera

4. TÉRMINOS COMUNES Y HERRAMIENTAS

4.1. TÉRMINOS COMUNES.

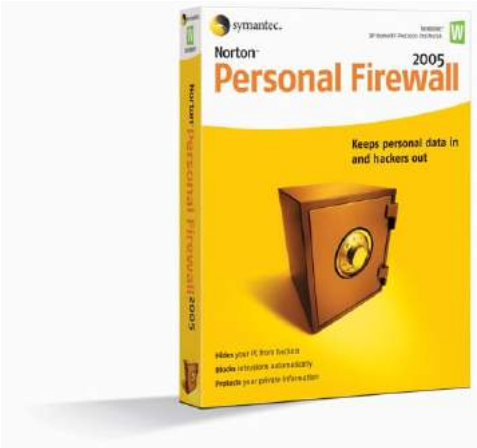
Es prescindible tener conocimiento de los términos más usados en este mundo underground, es por ello que estas definiciones se vuelven indispensables para un claro entendimiento.

4.1.1. TROYANO o CABALLO DE TROYA. El troyano tiene diversos significados y cometidos. Tiempo atrás, el troyano era un programa oculto que proporcionaba un cuadro de diálogo falso que debías aceptar, tras lo cual, el troyano se "quedaba" con lo que tecleabas después, en este caso la clave. Después, el troyano encriptába nuestra clave, y cuando empleábamos el correo electrónico, se enviaba automáticamente a un correo electrónico específico, fuera cual fuera la dirección. Ahora el troyano recibe el nombre de Back Orífice, Netbus o Deep Troath. Estos troyanos se dividen en dos grandes bloques, un servidor y un cliente ambos ejecutables. Colocando el fichero servidor a un ordenador remoto y ejecutando nuestro cliente podemos controlar cualquier función del otro ordenador. Esos son los troyanos, que han hecho "flaquear" la seguridad de Windows 95, 98, Me, 2000 y XP. (Ver fig. 4.1)

4.1.2. MAILBOMBING. Es el envío masivo de correo electrónico, comúnmente conocido como bombardeo, en el entorno del hacking. Los mailbombing son programas que permiten enviar miles de veces un mismo mensaje a una determinada dirección de correo electrónico. A veces el mailbombing permite también enviar correo fantasma, esto es, correo falso sin dejar rastro de quien lo envía, por lo que pasa inadvertido. A esto se llama correo anónimo. (Ver fig. 4.2 y 4.3)

4.1.3. IRC. Comúnmente conocido como canal de chateo o "forma de intercomunicarse con otros usuarios en tiempo real a través de textos y ahora de voz ", se ha convertido en un canal de guerra en el que entras para preguntar algo en concreto y recibes como respuesta una bomba lógica o un virus. Existen multitud de herramientas IRC en las páginas de hackeo y utilidades WAR o de guerra. Está de moda ir fastidiando por este canal. (Ver fig. 4.4)

4.1.4. FIREWALL. Un firewall es una utilidad o herramienta de seguridad, que impide a ciertos comandos o paquetes de datos "anormales" penetren en nuestro sistema[6]. Comúnmente se traduce como barreras de fuego, que detectan ataques o entradas forzadas en los puertos de nuestro sistema. Las descargas más peligrosas son las extensiones ZIP y EXE. El servidor de back orífice, puede renombrarse fácilmente y hacernos creer que estamos bajando otro fichero. Los firewall se denominan también nuke. (Ver fig. 4.5)



4.1.5. BACKORIFICE. Es un programa de control remoto del pc que funciona bajo un servidor y un cliente. Si colocamos el servidor a un ordenador remoto, es posible desde el cliente, gobernar cualquier función del pc remoto, entre los que se destacan abrir y cerrar programas, controlar el CD, leer y escribir ficheros y borrar parte del disco duro. Para ello el servidor se autoejecuta y se borra cada vez que el pc ajeno se enciende, nuestro cliente escanea el puerto elegido y cuando está abierto, actúa a través de él, desde un menú cliente repleto de pestañas y opciones de control remoto. El sistema es bueno para controlar un pc o pcs en una red LAN interna y a pesar de lo que se diga, podría ser menos nocivo que un virus, aunque dejar esa puerta abierta es toda una amenaza para Windows.

[6] El Firewall más popular que un usuario de a pie puede utilizar es ZoneAlarm, qué además conoce una versión totalmente Freeware para el usuario. Además, ya son varias las páginas Web que contemplan un Manual para conocer el uso y funcionamiento de esta popular aplicación, que puede ser completada con VisualRoute.

4.1.6. BOMBA LÓGICA. Es lo más parecido a un virus. Una bomba lógica es un programa autoejecutable que espera un determinado tiempo o una actividad sobre el teclado para explotar, o dicho de otra manera, para infectar el ordenador, modificando textos, mostrando gráficos o borrando parte del disco duro. (Ver fig. 4.6)

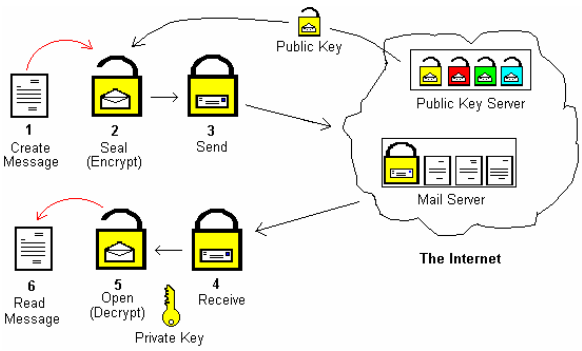
4.2. HERRAMIENTAS IMPRESCINDIBLES PARA UN HACKER

El Hacker necesita herramientas que le faciliten el trabajo en la red. Entre esas herramientas destacan los sniffers, escaneadores y programadores de tarjetas inteligentes. También es recomendable algún mailbombing y nukenabber para enfrentarse a aquellos que sólo actúan para fastidiar.

Para entrar en sistemas ajenos, "aunque sólo sea para ver y salir después" el Hacker debe echar mano a un buen diccionario para obtener la clave de acceso. Actualmente es necesario disponer también de utilidades de guerra IRC y WAR, para enfrentarse a otros enemigos. Un buen virus bajo la manga apartará al intruso que nos molesta. Pero lo más importante es la motivación y la intuición, sin ellas nada se puede hacer.

4.2.1. NUKENABBER. Es un programa que controla todos nuestros puertos y su estado, y es capaz de detectar una intrusión o nuke en cualquiera de los puertos seleccionados. En el caso de back orífice, podemos "vigilar" el puerto 12346 que es el empleado por este troyano y descubrir si alguien controla ese puerto.

4.2.2. PGP. PGP, de *Pretty Good Prívacy* es el programa de cifrado por excelencia para la mayoría de los usuarios que pretenden proteger su correo electrónico y sus ficheros de texto. Este programa, que conoce numerosas versiones y mejoras, fue inicialmente desarrollado por Philip Zinmermam, quien tuvo sus encuentros con la justicia americana. El programa de cifrado basado en RSA o en Diffie fue prohibido para su exportación, pero a alguien se le ocurrió publicarlo en internet en forma de texto, y alguien más lo compiló de nuevo en Europa. Así fue como PGP llegó a Europa. Actualmente va por la versión 6.0 e incluso se conoce una versión en español de este programa de cifrado altamente seguro. (Ver fig. 4.7)



4.2.3. WAREZ. Warez es en realidad un software "conocido" que lleva incluido un crack para su instalación sin número de serie o en varias máquinas sin pagar por él. En internet se encuentran infinidad de warez y números de serie para los programas más conocidos. Los warez son una forma de crackear software, apegado con el delito y que entra de lleno en él, ya que viola los derechos de autor.

4.2.4 ESCANEADORES. El más conocido es el Scanerport y como su nombre indica, se trata de programas que permiten rastrear la red en busca de puertos abiertos por los cuales acceder y manipular un sistema o introducir un troyano o un virus. PortScan es otra utilidad ampliamente conocida por los Hackers.

4.2.5. CRACK DE SOFTWARE. El crack de software, que lo convierte en Warez, es la inclusión de un código o varias líneas de códigos en los ficheros de registro del software, que impide que caduque el programa. Todas las versiones de evaluación o Shareware tienen caducidad. Los datos que lo permiten están normalmente encriptados y divididos en diversos ficheros *DLL, REG* e incluso *INI*. Cada programador oculta el código de tiempo donde le viene mejor. EL crack consiste en alterar esos datos u otros de forma que el programa no reconozca la fecha de caducidad.

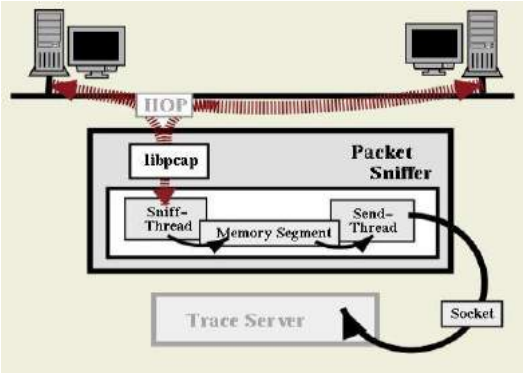
Por otro lado, crack es también la localización del número de serie del programa. Este número se localiza gracias a un generador de números de serie o *generator*, una utilidad muy ampliada por los Crackers para obtener logins y números de serie.

4.2.6. DICCIONARIOS. Existen dos tipos de diccionario entre la comunidad hacker y ambos son imprescindibles dado su contenido. El diccionario básico del Hacker detalla la extensión de los nuevos acrónimos que habitualmente se emplean en esta sociedad. Así, se describen acrónimos como spoofin, nuk, zombie y crash entre otros. Para poder moverse entre la nueva sociedad es necesario saber el significado de cada uno de los acrónimos que permiten conocer a fondo todo lo relacionado con el hacking, cracking, phreaking y otros servidores.

El otro gran diccionario de verdadera utilidad, para los Crackers más que para los Hackers, es el diccionario de palabras. Cuando se emplea la fuerza bruta para obtener los passwords o contraseñas de un programa, página web u ordenador remoto, es necesario y muy habitual emplear este diccionario, normalmente en formato software. El programa y/o diccionario electrónico compara miles de palabras hasta dar con la clave correcta; a lo que se denomina fuerza bruta ya que se comparan miles de palabras en menos de un segundo.

4.2.7. INGENIERÍA SOCIAL. Es quizás la base del Hacker para obtener los datos que le interesan de una conversación, y de distintas personas. Es la forma de engañar al otro, timarlo y hacerle creer que eres alguien en quien confiar, el técnico de la compañía de teléfono quizás. Buena muestra de ello es el engaño de Telmex, en el que te llaman haciéndose pasar por un técnico de la compañía y te piden que teclees un número después de colgar. Este comando llamado ATT, le permite al ingeniero social realizar llamadas a través de tu teléfono. Y en la actualidad puede suceder en cualquier país. Obviamente, a la fecha, ese *bug* se ha subsanado.

4.2.8. SNIFFER. Esta utilidad permite la monitorización de la red y detecta fallos de seguridad en ella o en nuestros sistemas. Dentro de los sniffers podríamos citar otras utilidades de control como KSA y SATAN, que además de buscar las debilidades de un sistema, se emplean como sniffers, esto es, monitorización de la red y la unidad central. Una navegación lenta en internet puede indicarnos que hay un sniffer en línea. (Ver fig. 4.8)



4.2.9. SISTEMA DE ACCESO CONDICIONAL. Se refiere al modelo seguido para el control de abonados de una Plataforma Digital. Así se conocen varios sistemas de Acceso Condicional como Directv y Sky en México. Ahora el Carding está siendo tan extendido entre los adeptos a lo desconocido, que incluso toma forma como HackCarding, por el gran número de seguidores que tiene esta afición.

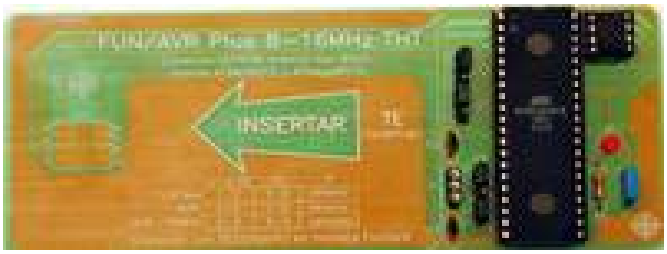
El HackCarding ha permitido influir en el número de suscriptores de cada Plataforma Digital afectada, a veces para aumentar beneficios y otras para perderlos. No está muy claro quien gana o quien pierde, pero lo cierto es que se ha desatado una verdadera batalla en este sector. Actualmente los proveedores de servicios de *Pago por evento* están modificando sus sistemas de Acceso Condicional.

4.2.10. CARDING. Es una extensión más de esta nueva cibersociedad en constante búsqueda por controlar todos los sistemas informáticos y electrónicos de la sociedad actual. Hoy por hoy la implantación de las tarjetas de crédito es masiva y está presente en casi todos los sectores como operaciones bancarias, acceso a sistemas de televisiones de pago, sistemas de pago electrónico y acceso controlado.

El carding es el estudio de tarjetas chip, magnéticas u ópticas y comprende su lectura y la duplicación de la información vital. Actualmente se clonan tarjetas GSM, tarjetas de canales de pago y visa por este procedimiento. (Ver fig. 4.9)

4.2.11. HACKCARDING. El arte de Hackear una SmartCard va más allá del Carding tradicional. En la actualidad es cada vez mayor el número de personas que se suman a esta adicción de Hackear Smartcards. Esto es debido a que existen importantes foros donde se explica y comenta las técnicas para hacerlo. Tanta es la información que cualquier neófito en el tema, puede convertirse en un usuario avanzado en la manipulación y/o conocimiento de una SmartCard. Así cualquiera es capaz de realizarse un Emulador, interpretar código.

4.2.12. WHASER. En la actualidad se denominan Whasers a los Webmasters de páginas que alojan en ellas archivos HEX, los cuales son utilizados para programar tarjetas del tipo ISO 7816, a fin de Emular una SmartCard original de un sistema de Acceso Condicional. *Directv, Sky* entre otras son plataformas fuertemente golpeadas por la piratería de códigos emuladores. Los Whasers no son los creadores de estos códigos, ni tampoco son capaces de modificar estos códigos para cambiar su funcionamiento. Los Whasers están extendidos por todo el mundo ofreciendo en cada país los archivos HEX correspondientes a cada Sistema, Irdeto, Conax, Cryptoworks. Algunos Whasers pueden llegar a tener muy buenos conocimientos de todos estos sistemas. (Ver fig. 4.10)



4.2.13. DUMP. Dentro del Carding, el Dump es el volcado de la información de la ROM y la Eprom de una SmartCard que está siendo atacada por un Gusano externo. El volcado de esta información le permite al Hacker conocer el funcionamiento del algoritmo interno, códigos y tablas. Para un Cracker esta información le permitirá descubrir Bugs que exploten más adelante la misma SmartCard frente a defensas de esta. Para el HackCarding esto es un gran paso ya que con esta información es posible crear los emuladores clonados de tarjetas.

4.2.14. BACKDOOR EN CARDING. Una BackDoor aquí es una clave de acceso que le permite al sector HackCarding acceder al interior de una SmartCard, obteniendo así el Dump de la Zona correspondiente. Las BackDoor no tienen porqué estar presentes en todas las SmartCard. Esto depende del sistema y Acceso Condicional atacado. Revelar que sistemas la poseen y cuales no, así como la clave BackDoor es tipificado como delito.

4.2.15. MOSC EN CARDING. En Carding MOSC es la propiedad de poder modificar en una Tarjeta de Acceso Inteligente las propiedades de suscripción a canales, obtener claves operacionales o claves secretas. El arte de hacer MOSC difiere entre cada sistema de Acceso Condicional. Así en ocasiones se habla de Datatypes y en otras de PBM para modificar canales contratados. Exponer esta información también es delito.

4.2.16. GUSANO DENTRO DE LOS WHASER. Aquí el gusano es el que genera un desbordamiento de pila dentro de una SmartCard. En el caso de las SmartCard de *Pago por evento*, el Gusano permite obtener la información de la zona Eprom de la tarjeta. Zona que contiene la información de claves privilegiadas e información de suscripción de canales contratados. Esta información forma parte del sistema de Acceso Condicional y por lo tanto acceder a ella o conocerla es un acto de delito, ya que esta información es considerada de secreto.

4.2.17. SHASER. Se les denomina Shaser a los usuarios de programas *"Per-to-Per"* , (par-a-par), como Kazaa[7], Gnutella, Imesh[8] u otros. Aquí basta con teclear que se desea buscar dentro de la aplicación, se localiza "normalmente archivos de música *.mp3" y se bajan al disco duro. Es la adicción prioritaria de los Shasers, pasarse el día delante de por ejemplo Kaaza y descargar el mayor número de archivos mp3 posible, así como mantenerlos en el disco duro para uso y disposición de otros internautas. También se les podría haber llamado coleccionistas de MP3, ya que estos usuarios realizan esta tarea de forma compulsiva.

[7] http://www.kazaa.com
[8] http://www.imesh.com

Capítulo 5

Hacktivismo y sus Alcances.

“ *Allí donde va la gente, la política va.* “

Anónimo.

5.0. HACKTIVISMO Y SUS ALCANCES

Se denomina hacktivismo (hacktivism, en inglés) a la convergencia del hacking con el activismo social o político. El hacktivismo incluye la desobediencia civil electrónica, que traslada al ciberespacio el concepto tradicional de desobediencia civil. Los orígenes del hacktivismo se remontan a mediados de los años ochenta, la prehistoria de la Web. La primera versión de PeaceNet (red electrónica mundial dedicada a la paz, la justicia social y económica, los derechos humanos y la lucha contra el racismo, aparecida en 1986), permitió por primera vez a los activistas políticos comunicarse unos con otros a través de las fronteras internacionales con relativa rapidez y facilidad.

Ese entorno, que operaba básicamente a través del sistema de BBS y donde predominaba el texto, se mantuvo hasta 1994, año en que se introdujeron los primeros navegadores con interfaz gráfica de usuarios. Por aquel entonces, el surgimiento del Netscape permitió, por primera vez, visualizar fácilmente en Internet páginas con fotografías e imágenes. La expresión "desobediencia civil electrónica" fue acuñada por un grupo de artistas y pensadores llamado Critical Art Ensemble.

Antes de 1998, la desobediencia civil electrónica no dejaba de ser, en su mayor parte, totalmente teoría. Pero tras la masacre de Acteal, en Chiapas, se produjo un giro hacia una posición más híbrida regida por la concepción de la infraestructura de Internet a la vez como un medio de comunicación y como un ámbito de acción directa. Con ese fin, se creó en 1998 el Electronic Disturbance Theater (EDT), por parte de tres artistas: Ricardo Domínguez (nació en Las Vegas en 1959, vive en Nueva York y es hijo de padres mexicanos), Brett Stalbaun (de San José, California) y Carmin Karasic.

5.1. LOS ZAPATISTAS Y EL PRIMER "BLOQUEO VIRTUAL” A GRAN ESCALA

Un "bloqueo virtual" es el equivalente electrónico de sus pares físicos. En ambos casos, el objetivo es centrar la atención sobre los manifestantes a través de la interrupción de las operaciones normales y del bloqueo en el acceso a determinados lugares.

Este concepto fue inaugurado por el Electronic Disturbance Theater, que en 1988 organizó una serie de acciones, primero contra el sitio del presidente mexicano Ernesto Zedillo, y luego contra los sitios de la Casa Blanca, el Pentágono, la Escuela de las Américas en México y las bolsas de valores de Frankfurt y México. El propósito fue demostrar solidaridad con los zapatistas mexicanos.

Todo comenzó cuando en enero de 1998, un grupo activista italiano, llamado Anonymous Digital Coalition hizo circular la propuesta de realizar un bloqueo virtual sobre cinco sitios de entidades financieras mexicanas. Su sugerencia fue, que si una gran cantidad de personas se ponían de acuerdo y apretaban el botón de Recargar de su navegador varias veces seguidas, los sitios podrían ser efectivamente bloqueados. Basándose en esa teoría de acción simultánea, colectiva y descentralizada con un sitio determinado, Brett Stalbaun, del EDT, diseñó un software especializado –al que llamó FloodNet- que se encargó de automatizar la tarea de recarga sobre los sitios escogidos.

Según Stalbaum, el Pentágono fue elegido debido a la creencia de que el ejército estadounidense entrenó allí a los soldados que llevaron a cabo varios abusos contra los derechos humanos en Latinoamérica. Por la misma razón fue elegida la Escuela de las Américas en México. La bolsa de Frankfurt, en cambio, fue escogida "porque representa el rol del capitalismo en la globalización utilizando las técnicas del genocidio y la limpieza étnica, la cual es la raíz de los problemas de

Chiapas. La gente de Chiapas debería tener un rol preponderante en determinar su destino, en vez de ser forzadas a una relocalización a punta de pistola, hecho que es actualmente financiado por el capital occidental".[15]

Los integrantes del EDT distribuyeron el nuevo software a través de Internet. Todo lo que los interesados en participar de estas acciones debían hacer era visitar uno de los sitios de FloodNet. Al hacerlo, su programa de navegación bajaba a sus computadoras el software (un *applet* de Java), que accedería al sitio elegido como objetivo varias veces por minuto.

Adicionalmente, el software permitía a los manifestantes dejar sus proclamas en el error log del servidor del sitio agredido. Por ejemplo, al apuntar sus navegadores hacia un archivo no existente tal como *human_rights* (derechos humanos) en el servidor atacado, el mismo les enviaba -y almacenaba- el mensaje *human_rights not found on this server* (derechos humanos no encontrados en este servidor).

El EDT estimó que unas 10.000 personas de todo el mundo participaron en el ataque realizado el 9 de septiembre de 1998 contra los sitios del presidente Zedillo, el Pentágono y la Bolsa de Frankfurt, enviando 600.000 *hits* por minuto a cada uno de ellos.

5.2. EL PENTÁGONO CONTRAATACA

El ataque ya había sido anticipado por el Pentágono. Cuando sus servidores detectaron la "invasión", lanzaron una contraofensiva contra los navegadores de los usuarios, redireccionándolos a una página con un *applet* (pequeña aplicación) llamado *"HostileApplet."* Una vez allí, el *applet* era bajado a sus navegadores, y les hacía recargar un mismo documento sin parar hasta que las computadoras fueran apagadas y vueltas a encender.

La bolsa de valores de Frankfurt reportó que estaba al tanto de la protesta, pero la misma no había afectado sus servicios. Según explicaron, normalmente reciben seis millones de visitas por día, por lo cual esta carga adicional no les generó inconvenientes.

El sitio del presidente Zedillo no contraatacó en esa ocasión, pero en un "bloqueo virtual" realizada en junio del año siguiente usó un software que provocó que los navegadores de los manifestantes abrieran una ventana detrás de otra hasta que sus computadoras debieran ser apagadas y vueltas a encender.

El EDT consideró al ataque como un verdadero éxito. "Nuestro interés es ayudar a la gente de Chiapas para que siga recibiendo el reconocimiento internacional que necesita para sobrevivir", dijo Stalbaum.

"El zapatismo digital es y ha sido uno de los usos de Internet políticamente más efectivos que conocemos. Ha creado una red de distribución de información con 100 o más nodos autónomos de soporte. Eso ha permitido al Ejército Zapatista de Liberación Nacional (EZLN) hablar al mundo sin tener que pasar por el filtro de los medios dominantes". [14]

Los zapatistas fueron elegidos por la revista Wired como uno de los 25 grupos online más importantes en 1998.

5.3. ACTOS DE HACKTIVISMO TRAS LOS ATENTADOS DEL 11 DE SEPTIEMBRE

Los atentados terroristas que tuvieron lugar en Estados Unidos el 11 de septiembre de 2001 generaron una rápida reacción entre algunos miembros de la comunidad hacker. La primera acción concreta difundida por los medios masivos tuvo lugar al día siguiente, el 12 de septiembre. Un hacker ruso llamado Ryden atacó al sitio *taleban.com*, correspondiente a la denominada "Misión Afgana de Talibán".

La página principal fue alterada y se colocó en la misma una foto de Osama Bin Laden, con un texto acusándolo por el atentado. El mismo hacker ya había atacado al sitio taleban.com en marzo y en julio de ese mismo año, según los registros mantenidos por www.alldas.de y www.safemode.org.

Pocos días más tarde se anunció públicamente la creación del grupo *The Dispatchers*, creado por 100 hackers de distintos países decididos a perturbar a través de Internet a aquellas naciones y organizaciones que apoyen al terrorismo islámico. Uno de los principales integrantes del grupo era un hacker canadiense que decidió llevar a cabo esa alianza al constatar que entre las víctimas de los atentados contra las Torres Gemelas figuraban amigos y familiares suyos.[13]

Posteriormente, según un cable de la agencia *France-Presse*, *The dispatchers* se atribuiría el haber puesto fuera de servicio a algunos sitios palestinos e iraníes. Otras acciones, cuya autoría es desconocida, fueron las siguientes:

- El sitio oficial del Palacio Presidencial de Estado Islámico de Afganistán (wwww.afghan.gov.af) permaneció un tiempo fuera de servicio, luego de que su dirección fuera publicada en distintos newsgroups (grupos de noticias) en Internet, en los que indirectamente se alentaba a atacarlo. "Que el gobierno afgano sepa que es lo que nosotros pensamos acerca del asilo que le dan a Bin Laden", decía un texto publicado en el newsgroup.

- El sitio de la República Islámica de Paquistán (www.pak.gov.pk) también estuvo por momentos fuera de servicio, a pesar de las declaraciones publicadas en el sitio, en la cuales el presidente paquistaní Pervez Musharraf condenó severamente los ataques terroristas. La dirección del sitio había sido exhibida poco tiempo antes en el newsgroup alt.hackers.maliciuous, en un mensaje titulado *"El gobierno pakistaní ama a los troyanos"* (en alusión a los virus conocidos como troyanos). [11]

5.4. YIHAT. YOUNG INTELLIGENT HACKERS AGAINST TERROR

Una de las iniciativas antiterroristas más llamativas procedentes del mundo de los hackers fue la llevada a cabo por Kim Schmitz, un hacker alemán transformado en consultor de seguridad, quien abrió un sitio en Internet para reclutar a otros hackers a fin de rastrear flujos de fondos y otras evidencias que vinculen a Bin Laden con los atentados del 11 de septiembre.

Poco tiempo después del lanzamiento de su grupo, al que llamó YIHAT (Young Intelligent Hackers Against Terror), Schmitz afirmó que 34 personas de 10 países, junto con tres traductores de idioma árabe, se habían sumado a su iniciativa. Schmitz había sido acusado de ingresar ilegalmente a computadoras de la NASA y el Pentágono durante los ´90. *"Creo que el mundo libre debe unirse ahora. Sólo podremos derrotar al terrorismo si luchamos contra el mismo en todas partes... en unos pocos años los terroristas tendrán armas biológicas y nucleares y no matarán a 5.000 personas sino a 5 millones con un solo golpe",* dijo Schmitz.

David Endler, un analista de la empresa de seguridad iDefense, de Virginia, Estados Unidos, le dijo a un periodista de France-Presse que hackers de YIHAT ingresaron en un banco sudanés y obtuvieron información sobre cuentas vinculadas con Bin Laden. Supuestamente le dieron esa información al FBI.

"Sus motivaciones tal vez sean justas, pero sus acciones pueden causar daño y pueden traer aparejadas otras implicancias para la privacidad de las personas", dijo Endler en relación con los hackers que decidieron "hacer justicia" por su propia cuenta.

El National Infrastructure Protection Center, del FBI, se hizo eco de esa opinión y señaló que las conductas descriptas "son ilegales y punibles, con penas que pueden llegar a los cinco años de prisión. Los individuos que creen que están un

servicio a la Nación a través de ese tipo de acciones, deberían saber que en realidad están jugando en contra".

No todos los hackers se adhirieron a la postura activista. La legendaria organización con sede en Alemania llamada Chaos Computer Club (CCC), fundada 20 años atrás en Hamburgo, manifestó su oposición categórica a los llamamientos de otros hackers para atacar y sitios islámicos en Internet.

En un e-mail, Andy Mueller-MaguHn, portavoz del CCC, afirmó: *"Precisamente ahora, los medios de comunicación electrónicos como Internet pueden contribuir de forma importante a la comprensión entre los pueblos. Con la tensión actual, no podemos bloquear los medios de comunicación y abrir así un terreno aún más amplio a la incomprensión"*, añadió.

Capítulo 6

CIBERTERRORISMO.

"La guerra infraestructural consiste en usar una combinación de medios virtuales y físicos de manera de lograr el máximo efecto posible. Pero para esto hace falta una organización y medios de magnitudes militares, y no un puñado de hackers"
FBI

6.0. CIBERTERRORISMO

6.1. ANTECEDENTES. JUEGOS DE GUERRA.

La película Juegos de guerra (1983) muestra a un joven e inocente hacker (Matthew Broderick) que accede ilegalmente a una computadora gubernamental para jugar a un juego de guerra termonuclear en un *mainframe* diseñado para simular estrategias de ataque y respuesta. Desde aquella película, estrenada en plena guerra fría, varios expertos en seguridad se comenzaron a preguntar qué posibilidades reales podría haber de que alguien pueda interferir los sistemas computacionales destinados a la defensa. [25]

En 1986, un libro llamado *Softwar* afirmó que los países del Pacto de Varsovia podrían incapacitar al mundo occidental lanzando ataques contra las computadoras militares y financieras de Estados Unidos y la OTAN. [68]

La primera acción preventiva importante a nivel oficial fue la creación por parte del gobierno estadounidense de *The Critical Technologies Institute* (1991), esponsoreado por la *National Science Foundation.* Este organismo elaboró una serie de recomendaciones divididas en acciones inmediatas, acciones a corto plazo y acciones a mediano plazo. Entre estas últimas figuraba la creación de mecanismos de alerta y de un organismo de coordinación. [9]

Cinco años más tarde, el ex Director de Inteligencia Central John Deutch, en su testimonio ante un comité del Congreso, afirmó: "Hackers criminales estuvieron vendiendo sus servicios a estados-villanos (rogue states)". Y agregó que "están analizando varios esquemas para agredir los intereses vitales de Estados Unidos a través de intrusiones ilegales en computadoras". [18]

[9] Scassa, David. Paper on Cyberterrorism..

6.2. BILL CLINTON, EL PRIMER PRESIDENTE DE LA ERA DE INTERNET

"Ahora que nos aproximamos al siglo XXI, nuestros enemigos han ampliado los campos de batalla del espacio físico al cibernético... En lugar de invadir nuestras playas o enviar bombarderos, estos adversarios pueden intentar ataques cibernéticos contra nuestros sistemas militares esenciales... Si nuestros hijos han de crecer libres, debemos afrontar esas nuevas amenazas con el mismo rigor y determinación que empleamos contra las amenazas a nuestra seguridad más severas de este siglo"

Bill Clinton, 22 de mayo de 1998

Clinton fue el primer presidente estadounidense de la era de Internet. De hecho, fue durante su gestión cuando la "red de redes" se difundió masivamente entre la población y los procedimientos de hacking -al igual que la cantidad de hackers- se multiplicaron.

Cuando Clinton asumió su primer mandato, un hacker era un especialista en informática -por lo general altamente capacitado- que invertía muchísimas horas en investigar y adquirir conocimientos vinculados al acceso a redes de computadoras. Cuando Clinton dejó el gobierno, existían al menos 15.000 sitios de Internet que ofrecían en forma gratuita manuales, instrucciones y programas para realizar distintos tipos intrusiones y ataques informáticos.

Fue en 1994 cuando, con la aparición del Netscape Navigator, la información a través de Internet se hizo más accesible (ya que permitió incorporar imágenes), con lo cual los hackers movieron toda su parafernalia instalada en los viejos BBS (Bulletin Board Sistems) a sitios de Internet accesibles a todo el mundo.

6.3. EL PLAN CYBER CORPS

Volviendo al tema de la prevención ante un eventual ataque, en enero de 1999, Clinton dio el próximo paso: el lanzamiento del plan Cyber Corps.

Dicho plan contemplaba iniciativas específicas tales como:

- La creación de redes de detección (detection networks). En primer lugar, dichas redes se crearían para el Departamento de Defensa, y luego para otras agencias clave. Su finalidad sería alertar al personal apropiado cuando un sistema computacional crítico ha sido invadido.

- La creación de centros de información en el sector privado de tal manera que las empresas estadounidenses puedan trabajar en forma conjunta con el gobierno para manejar las "ciberamenazas".

- Proporcionar financiamiento a fin mejorar las capacidades de los especialistas en computación del gobierno capaces de prevenir y responder a las crisis sufridas por las computadoras.

6.4. HIPÓTESIS Y PREDICCIÓN SOBRE EL CIBERTERRORISMO

6.4.1. LAS HIPÓTESIS DE BARRY COLLIN

Barry Collin, un investigador senior del Institute for Security and Intelligence en California, quien en los años 80 acuñó el término ciberterrorismo elaboró años atrás una serie de hipótesis sobre posibles actos ciberterroristas.

Esas hipótesis fueron -y todavía son- usadas masivamente por periodistas, políticos y funcionarios de organismos de seguridad, para referirse a la amenaza del ciberterrorismo. Por lo tanto, contribuyeron a formar una determinada idea en el imaginario colectivo estadounidense acerca de las posibles consecuencias de un atentado terrorista informático.

Las hipótesis de Barry Collin son las siguientes: [17]

• Un ciberterrorista podría acceder remotamente a los sistemas de control de procesamiento de una planta elaboradora de cereales, cambiar los niveles de ingestión de hierro, y enfermar (e incluso eventualmente matar) a los niños de Estados Unidos mientras disfrutan de su desayuno. También podría realizar alteraciones similares en plantas de alimentos para bebés. La supuesta ventaja potencial para el ciberterrorista de este tipo de ataque es que no tendría que estar en la fábrica para ejecutar ese tipo de atentado.

• Un ciberterrorista podría interferir a los bancos, las transacciones financieras de dinero y los centros bursátiles. Esa manera, los habitantes del país perderían su confianza en el sistema económico. Dice Collin:

> ¿Se atrevería un ciberterrorista a intentar ingresar físicamente al edificio de la Reserva Federal, u otro equivalente? Difícilmente, desde el momento en que sería inmediatamente arrestado. Es más, un gran camión estacionado cerca del edificio sería detectado en forma automática. Sin embargo, en el caso de un ciberterrorista, el perpetrador podría estar sentado en otro continente mientras que los sistemas económicos de la nación colapsan, alcanzando una situación de desestabilización. [59]

• Un ciberterrorista podría atacar a la próxima generación de sistemas de tráfico aéreo, y hacer que dos grandes aeronaves civiles choquen entre sí. "Ese es un escenario realista, desde el momento en que el ciberterrorista también podría interferir los sensores del interior de la cabina", dice Collin, y señala que maniobras similares pueden ser realizadas con las líneas de ferrocarriles.

• Un ciberterrorista podría alterar las fórmulas de remedios o productos farmacéuticos, causando una gran cantidad de pérdidas humanas.

• Un ciberterrorista podría cambiar remotamente la presión de los gasoductos, causando fallas en las válvulas, y desencadenando una serie de explosiones e incendios. "De la misma manera, la red eléctrica se vuelve cada día más vulnerable", afirma Collin.

En síntesis, el ciberterrorista, según Collin, se asegurará de que la población de un país no pueda comer, beber, viajar ni vivir:

Las personas encargadas de velar por la seguridad de la Nación no estarán advertidas ni podrán anular al ciberterrorista, que probablemente se encontrará en el otro lado del mundo.

Lamentablemente esos ejemplos no son de ciencia-ficción. Todos esos escenarios pueden tener lugar hoy. Como muchos saben, algunos de esos incidentes ya han ocurrido en varias naciones. Muchos de esos actos ocurrirán mañana.

Uno de los principales críticos de Barry Collin es el agente del FBI Mark Pollitt, quien a fines de los 90 escribió un ensayo titulado *Ciberterrorismo: ¿Fantasía o realidad?* (Cyberterrorism: Fact or Fantasy?), en el cual analiza las posibilidades reales de ataques ciberterroristas, dejando en claro que sus opiniones son estrictamente personales y no representan el punto de vista del FBI.

Al analizar la factibilidad de las hipótesis de Collin, Pollitt concluye que actualmente existe el suficiente involucramiento humano en los procesos de control como para que el ciberterrorismo no alcance el riesgo de riesgo que le atribuye Collin.

En el ejemplo el control de tráfico aéreo, Pollitt sostiene que las personas a cargo notarían los problemas y tomarían acciones correctivas. Los pilotos, dice Pollitt, son entrenados en lo que se denomina situational awareness. Desde el primer día de aprendizaje, se les enseña a ser conscientes no sólo se su ubicación, dirección

y altitud, sino también de las ubicación de otras aeronaves. Es común que los pilotos descubran errores cometidos por los controladores de tráfico aéreo. Son las fallas humanas las que derivan en colisiones aéreas. La formación básica de los pilotos incluye la hipótesis del colapso de los sistemas de tráfico aéreo, con lo cual los pilotos son entrenados para operar en la ausencia de todo control.

Pollitt no pretende afirmar en su análisis que las computadoras son seguras y libres de vulnerabilidades. Su idea es que, a pesar de esas vulnerabilidades, es casi imposible que un ciberataque pueda tener consecuencias devastadoras. "A medida que incorporamos más y más tecnología en nuestra civilización, debemos asegurarnos de que exista el suficiente control e intervención humana como para salvaguardar a aquellos a quienes la tecnología sirve", dice Pollit.

6.5. ¿UN PEARL HARBOR ELECTRÓNICO?

Como parte del apoyo retórico que acompañó al pedido de financiamiento para el plan FIDNET, en 1999 Clinton dijo: "Mientras que hasta ahora nuestros enemigos se apoyaron en bombas y balas, terroristas y potencias hostiles podrían transformar a una computadora laptop en un arma potente capaz de hacer un gran daño". [16]

La expresión Pearl Harbor electrónico fue lo suficientemente impactante como para pasar a formar parte del discurso habitual de la prensa y de la clase política. Incluso una vez completada la transición al 2000 y superada la "falla del milenio", La alusión al Pearl Harbor electrónico siguió siendo moneda corriente.

En abril de 2001, ya durante la presidencia de George Bush (hijo), el republicano Newt Gingrich, presidente de la Cámara de Representantes de Estados Unidos entre 1995-1999, escribió un artículo titulado.

La pregunta no es si habrá un *ciber Pearl Harbor*, sino cuando ocurrirá:

- La seguridad de las aerolíneas estaría seriamente comprometida si las computadoras que manejan el tráfico aéreo fueran dominadas por ciberterroristas. Una acción de ese tipo podría causar numerosas víctimas. Pensemos en el caos que se generaría si un grupo terrorista dominara las computadoras del aeropuerto internacional O´Hare (en Chicago) que controlan el congestionado corredor aéreo del medio oeste.

- Desde paralizar nuestros sistemas de comunicaciones hasta bloquear nuestro sistema financiero, pasando por la generación de apagones eléctricos, hay una cantidad de grandes de interrupciones que podrían perjudicar nuestra economía, disminuir nuestra calidad de vida y desestabilizar a la Nación.

- Imaginen un mundo en el cual la Alemania Nazi o la Unión Soviética de Stalin hubieran sido los primeros en desatar el poder destructivo del átomo. Bien, ahora imaginen un mundo en el cual los líderes electos democráticamente tienen menos imaginación y mayor resistencia que sus adversarios tiránicos a apostar por tecnologías aún no fueron testeadas. [32]

6.6. MITOS Y REALIDADES SOBRE LOS VIRUS INFORMÁTICOS

La utilización de virus informáticos como si fueran armas es una preocupación presente tanto en los organismos de seguridad estadounidenses como entre los funcionarios públicos y periodistas poco informados.

El siguiente extracto del libro Information Warfare: How to survive Cyber Attacks, mencionado en el apartado anterior, es un claro ejemplo del poder que el imaginario colectivo suele atribuir a los virus de computadoras.

Un ejemplo acerca de la desinformación que circula en torno a los virus es ilustrada en un artículo publicado en la edición de diciembre de 1996 del Law & Enforcement Bulletin del FBI. El artículo fue escrito por académicos de las universidades estatales de Michigan y Wichita. Luego de una introducción sobre el delito informático y la psicología de los hackers, el artículo presenta a varios virus como ejemplos de herramientas informáticas vandálicas.

"Un virus llamado Clinton -escribieron los autores- fue diseñado para infectar programas "pero se erradica a sí mismo cuando no puede decidir qué programa infectar". Tanto los autores como el FBI vivieron un papelón cuando se enteraron de que no existía un virus llamado Clinton. Había sido una broma, al igual que los demás ejemplos de virus citados en el artículo, todos los cuales habían sido publicados en la columna del Fool´s Day (un día en el cual se suelen hacer bromas, como ocurre con el día de los inocentes en México) de una revista de computadoras. [31]

El artículo del FBI era una versión condensada de una monografía presentada por los mismos autores en un encuentro de la Academy of Criminal Justice Sciences en Las Vegas en 1996. Titulado Tendencias y experiencias en el delito vinculado a la computación: hallazgos de un estudio nacional (Trends and Experiences in Computer-Related Crime: Findings from a National Study), el informe se refirió a una redada en la cual agentes federales arrestaron a una peligrosa banda de hackers. "Los hackers ingresaron a una computadora de la NASA responsable de controlar al telescopio Hubble y se sabe que también redireccionaron llamadas telefónicas de la Casa Blanca hacia la Universidad Marcel Marceau, un instituto de mímica", escribieron los autores. Esa anécdota también fue parte de una broma hecha con ocasión del Fool' s Day.

Cuando el FBI decidió hacer las correcciones, ya se había enviado la revista a 55.000 profesionales y analistas políticos, muchos de los cuales deben haber tomado al artículo como verdadero.

En un artículo de la revista Issues in Science and Technology publicado en 1998 y firmado por George Smith, se ofrece una clara explicación de por qué los virus no pueden ser utilizados como armas en el contexto de un ataque ciberterrorista de gran envergadura:

Ningún virus ha demostrado tener utilidad como arma, por razones fácilmente comprensibles. Primero, es casi imposible, incluso para el mayor programador de virus, anticipar la complejidad y heterogeneidad de los sistemas que el virus encontrará. Los virus informáticos representan el anatema de las exigencias militares. En la era de las bombas inteligentes, los virus están muy lejos de poder ser considerados como munición de precisión.

Los virus son tan impredecibles que probablemente infecten tanto a los enemigos como a los amigos o aliados. Dado que los militares alrededor del mundo usan programas antivirus enlatados que se venden en cualquier negocio, no hay forma de que se puedan prevenir de sus propias creaciones. Lo que puede infectar al enemigo, también te puede infectar a ti.

Además, cualquier grupo que planee un ataque terrorista por medio de virus, debería tener en cuenta la rápida reacción de industria mundial de programas antivirus, la cual, luego de varios años de experiencia, está muy bien preparada para proporcionar rápidos antídotos.

En cuanto a la hipótesis de que un grupo de profesionales empleados por alguna organización militar o terrorista pueda alcanzar un éxito mayor que el de un grupo de alienados hackers adolescentes, Smith señaló:

Armar ese equipo no sería sencillo. Si bien no es difícil para cualquiera con habilidades básicas en programación escribir un virus malicioso, desarrollar un virus verdaderamente sofisticado requiere un conocimiento íntimo de los sistemas operativos que está diseñado para infectar y que podría llegar a encontrar. Esos hechos reducen considerablemente el área de potenciales profesionales que podrían ser contratados.

El error humano está siempre presente. Es un desagradable hecho de la vida que todo software, sin importar cuán detalladamente haya sido concebido, esconda errores desapercibidos por sus autores. Y los virus no son la excepción. Normalmente contienen errores, a veces tan espectaculares como apenas llegan a funcionar.

6.7. CIBERGUERRA.

Internet es una pieza más de la guerra y no sólo una fuente de información. También se ha convertido en otro campo de batalla en el que luchan piratas cibernéticos (hackers) y militares, que aspiran a dominar la red y utilizarla en su favor.

Los hackers han comenzado su ciberguerra particular y paralela. Especialmente, los contrarios al conflicto están provocando "bajas" y "daños secundarios" que van desde el bloqueo de sitios web de empresas e instituciones con nacionalidad norteamericana e inglesa, hasta la publicación de informaciones falsas que pueden provocar desde una sonrisa hasta alarma social.

Aunque estos ataques electrónicos suelen ser habituales también en épocas de paz, la guerra ha servido de "excusa" para que los habituales saboteadores actúen con las espaldas cubiertas y para que muchos informáticos se lancen por primera

vez a estas actividades impulsados por una causa que consideran justa, sin saber que el gobierno federal de Estados Unidos lo considera un delito.

Los ataques digitales, incluyendo gusanos y virus, causaron daños por valor de más de 8,000 millones de dólares en todo el mundo durante el mes de enero, según un informe de la compañía británica de seguridad Mi2g.

A este ritmo, y según el informe de la firma, a lo largo del año se registrarían 180 mil ataques en línea en todo el mundo, lo que supondría un desembolso de entre 80 mil y 100,000 millones de dólares para las economías.

Aunque se preveía que las más atacadas iban a ser las redes norteamericanas (sitios web del gobierno, y de empresas como IBM ya los han sufrido), también servidores árabes y portales norteamericanos críticos del conflicto o que se atrevieron a mostrar las imágenes de los primeros soldados norteamericanos capturados han sufrido el boicot de los saboteadores informáticos.

El número de ataques ha pasado de mil diarios en período de paz a 20.000 durante el comienzo de la guerra.

Aunque la mayor parte de los saboteadores informáticos actúa de forma independiente, un número cada vez mayor de estos expertos es reclutado por los gobiernos de todo el mundo, conscientes de que se convertirán en un nuevo cuerpo de los sistemas de defensa.

Capítulo 7

HACKING & CRACKING ¿UNA EXCUSA PARA LA INVASIÓN GUBERNAMENTAL DE LA PRIVACIDAD?

"Tal vez el Senado quiera seguir adelante y adoptar medidas que permitan intervenir las comunicaciones de los ciudadanos", dijo Leahy. "Tal vez quieran contar con herramientas para ingresar en las computadoras privadas. Y tal vez esto nos haga sentir más seguros. Puede ser. Pero también es posible que esto mismo sea un ejemplo de la falta de seguridad que han logrado implantar los terroristas en nuestra sociedad. Es posible que hayan conseguido ampliar el alcance del Gran Hermano en nuestro país".

7. HACKING & CRACKING
¿UNA EXCUSA PARA LA INVASIÓN GUBERNAMENTAL DE LA PRIVACIDAD?

7.1. EL CHIP CLIPPER

El primer gran conflicto en torno a la privacidad en la era de las telecomunicaciones tuvo lugar en los años '80. El eje fue el chip Clipper, un pequeño artefacto criptográfico destinado a proteger las comunicaciones privadas pero dejando abierta la posibilidad de que agentes gubernamentales obtengan las "llaves electrónicas" necesarias para descifrar las comunicaciones tras obtener una autorización legal.

En 1984, el presidente Ronald Reagan decretó la controversial Decisión Directiva de Seguridad Nacional 145 (National Security Decision Directive 145). La misma le otorgó a la agencia secreta NSA el control sobre todos los sistemas de computación gubernamentales que contengan información "sensible pero desclasificada". Eso fue seguido por una segunda iniciativa promulgada por el consejero de la NSA John Poindexter, que extendió la autoridad de la NSA a los sistemas computacionales no gubernamentales.

A manera de respuesta, en 1987, el congreso estadounidense aprobó el Acta de Seguridad Computacional (Computer Security Act) con el fin de limitar el rol de la NSA en el desarrollo de estándares para las comunicaciones civiles. La NSA quedó limitada a proporcionar asistencia técnica en el área civil. El Congreso consideró que no era apropiado que un organismo de inteligencia militar tuviera control sobre la diseminación de información desclasificada. Desde entonces, la NSA buscó la forma de socavar la autoridad del NIST.

Dicho chip estaba destinado a la encriptación de llamadas telefónicas. Dos "agentes de custodia" (escrow agents) gubernamentales conservarían las "llaves" necesarias para que el gobierno pueda descifrar los mensajes de aquellos ciudadanos bajo vigilancia del FBI u otro organismo de seguridad.

La propuesta era utilizar el chip Clipper para las transmisiones de voz, y un artefacto similar, llamado Capstone.

En 1993, el presidente Bill Clinton anunció públicamente la iniciativa del chip Clipper. "Durante demasiado tiempo, no hubo prácticamente diálogo entre nuestro sector privado y los organismos de seguridad para resolver la tensión entre la vitalidad económica y los verdaderos desafíos que implica la protección de los ciudadanos estadounidenses", se explicó en el comunicado de prensa del lanzamiento; "En vez de usar a la tecnología para conciliar los intereses a veces contrapuestos del crecimiento económico, la privacidad y la seguridad, las políticas previas han enfrentado al gobierno con la industria y a los derechos a la privacidad con los organismos de inteligencia". [19]

Para conciliar los intereses mencionados, la iniciativa del chip Clipper fue lanzada como obligatoria para los organismos gubernamentales, pero optativa para las empresas y organismos civiles. El gobierno creyó que al definir esa tecnología como estándar gubernamental, los empresarios y los consumidores también la aceptarían y la utilizarían, a pesar de la posibilidad existente de que el gobierno, autorización legal de por medio, pudiera interceptar las comunicaciones.

En otras palabras, el éxito de la propuesta del Chip Clipper se basaba en la aparente falta de disponibilidad de softwares criptográficos potentes en el momento del lanzamiento de la iniciativa.

Sin embargo, ya en 1993 existían programas de encripción importantes distribuidos a través de Internet y disponibles fuera de los Estados Unidos. Tal era el caso del PGP, desarrollado por Phil Zimmerman.

7.2. PHIL ZIMMERMAN Y EL PGP

El programa de encripción Pretty Good Privacy, desarrollado por Phil Zimmerman, estuvo en el centro de uno de los mayores debates que se realizaron en los últimos años en Estados Unidos en torno a la privacidad electrónica.

Zimmerman estudiaba ciencias de la computación en la Florida Atlantic University cuando descubrió la potencial utilidad de las computadoras para crear métodos de encripción. La base seguía siendo la misma: modificar los mensajes de tal forma que nadie, salvo el destinatario, pudiera descifrarlos. Pero las computadoras hacían posible implementar sistemas mucho más dificultosos de descifrar que cualquier código que una persona pudiera inventar por su cuenta.

En 1976, dos investigadores de la Stanford University, Whitfield Diffie y Martin Hellman publicaron un ensayo sobre un nuevo tipo de criptografía, diferente a todo lo existente, llamado New Directions in Cryptography. En el mismo explicaron los fundamentos de la denominada criptografía de clave pública.[10]

Al leer esos escritos, Zimmerman se sintió inspirado: su sueño era encontrar un método de codificación a través de computadoras que pudiera ser utilizado por cualquier persona.

El primer problema que Zimmerman tuvo que sortear fue que las computadoras personales disponibles por esa época eran demasiado precarias. El algoritmo RSA (utilizado para el sistema de clave pública) requería una enorme cantidad de cálculos matemáticos con números de hasta 300 dígitos. Recién en 1986 Zimmerman pudo programar en lenguaje C el software necesario para ese tipo de operaciones. [20]

[10] En el modelo criptográfico de clave pública, denominado modelo Diffie-Hellman, cada uno de los usuarios tiene una clave pública (que no es secreta y puede ser difundida sin problemas) y una clave privada (que sí es secreta). De esa manera, Alice le manda un mensaje a Bob encriptándolo con la clave pública de Bob, quien lo puede descifrar utilizando su clave privada. A su vez, Bob le contesta a Alice encriptando el mensaje con la clave pública de ella. La única persona capaz de descifrarlo es Alice, utilizando su clave privada. Para mayor información, hacer una búsqueda con las palabras clave "public key" en el sitio del diccionario virtual de seguridad informática What Is?

Posteriormente, decidió alejarse del tema debido a que, como el algoritmo RSA estaba patentado, los programas que el escribiera no podrían ser vendidos. En 1991, el gobierno estadounidense presentó el proyecto de Ley del Senado 266, una medida antiterrorista que contenía una cláusula según la cual se establecerían severas limitaciones a las comunicaciones y la encripción de archivos a través de sistemas que carecieran de una "puerta trasera" (back door) que pudiera ser abierta por el Gobierno. Una medida de ese tipo haría ilegales a los programas de encripción desarrollados por particulares.

La ley fue modificada luego de un fuerte debate por parte de distintos organismos defensores de los derechos civiles. Sin embargo, ante la posibilidad de que el acceso a la encripción sea declarado ilegal, Zimmerman lanzó la primera versión de su programa de PGP y se la dio a un amigo, el cual la subió a una gran cantidad de carteleras electrónicas (BBS).

Rápidamente se difundieron copias por todo el mundo, aún a pesar de que por aquella época eran relativamente pocos los individuos que tenían acceso a los BBS fuera del área académica o gubernamental.

En febrero de 1993, Zimmerman fue informado de que el Departamento de Justicia Estadounidense lo estaba investigando para determinar si había exportado ilegalmente sistemas criptográficos que figuraban en la categoría de "municiones" en el International Traffic in Arms Regulations (ITAR), un tratado internacional para la regulación de ventas de armamentos. Tres años más tarde las investigaciones finalizaron y se declaró a Zimmerman libre de cargos.

Durante ese tiempo, el PGP se transformó en un estándar. Su reputación creció a medida que varios criptoanalistas intentaron quebrar la codificación y fallaron. En varios países se formaron equipos de programadores con el fin de mejorar el programa. De esa manera, la cuestión legal vinculada a la exportación caducó; si

un ciudadano británico bajaba una copia de la versión británica del programa de un BBS de Londres, no estaba en absoluto alcanzado por el ITAR.

Los asuntos legales vinculados con el planteamiento del algoritmo RSA [11] finalizaron en 1993 cuando Zimmerman hizo un trato con una compañía de Arizona llamada Lemcom, la cual había obtenido una licencia de RSA para ver software basado en ese algoritmo. Mediante el contrato, Lemcom obtuvo los derechos para vender una versión comercial del PGP, llamada Viacrypt, mientras que Zimmerman obtuvo los derechos legales para distribuir la versión gratuita.

Zimmerman se transformó en una especie de héroe para los fanáticos de las computadoras y para los activistas de los derechos civiles. Su caso generó una gran polémica que alcanzó estado público en todo Estados Unidos.

A lo largo de 1994, en un solo servidor de acceso público del MIT se bajaron entre 500 y 1000 copias diarias del PGP.

7.3. LA PRIVACIDAD EN LA ERA DE INTERNET

Los debates en torno a los límites a la invasión gubernamental de la privacidad en relación con las computadoras se acentuaron durante el gobierno de Bill Clinton (1993-2001), debido en parte a tres grandes hechos:

a) La penetración masiva de Internet
b) La democratización del hacking.
c) La llamada falla del milenio.

A mediados de 1999, a través de un proyecto de ley titulado Acta de Seguridad Electrónica del Ciberespacio (Cyberspace Electronic Security Act, CESA), el Departamento de Justicia propuso modificar la legislación de tal manera de que, bajo ciertas circunstancias, se "postergue" por 30 días el aviso de notificación a los

[11] Grossman, Wendy. Net.Wars. Capítulo 4. NY Press.

sospechosos cuyos hogares o lugares de trabajo van a ser allanados. La idea diseñada por la administración de Clinton era permitir que agentes federales ingresen de incógnito en las viviendas de los sospechosos para revisar sus computadoras, descifrar sus códigos de encripción y colocar "puertas traseras" para monitorear el flujo de información.

Finalmente, la iniciativa fue desestimada.

7.4. EL CARNIVORE

En julio de 2000 se informó públicamente sobre la existencia de un sistema de monitoreo de comunicaciones a través de Internet del FBI llamado Carnivore. Según el FBI, el Carnivore es "un sistema basado en computadoras destinado a permitir, en cooperación con los proveedores de acceso a Internet, que se cumplan las órdenes judiciales vinculadas con la recolección de datos y de cierta información sobre un usuario específico objeto de la investigación".

Según el FBI, el Carnivore filtra el tráfico de información y envía a los investigadores sólo aquellos paquetes de datos que ellos están legalmente utilizados a obtener.

Ante las acusaciones de que ese método de control era equivalente al wiretapping, el FBI negó que ambos sistemas pudieran ser comparables. Según fuentes oficiales, el Carnivore se parece más a los sistemas conocidos como pen-registers y trap-and-trace. [12]

El New York Times reveló que el sistema estadounidense de espionaje electrónico es dirigido por la NSA y lleva el nombre clave de *Echelon*.

[12] El pen-register es un artefacto que se coloca en las líneas para registrar todos los números telefónicos a los que llama el sujeto de la investigación, así como la duración de la llamada y otros datos. El trap-and-trace registra todos los números telefónicos desde los cuales se llama al sujeto investigado.

Echelon consiste en una vasta red de estaciones de espionaje electrónica localizada alrededor del mundo en la cual participan cinco países: Estados Unidos, Inglaterra, Canadá, Australia y Nueva Zelanda. Esos países, agrupados bajo un acuerdo secreto llamado UKUSA, espían a los ciudadanos interceptando diariamente las comunicaciones electrónicas. Las computadoras de la NSA se encargan luego de revisar esa información, buscando determinadas palabras clave, a través de los denominados "diccionarios Echelon".

La columna vertebral de Echelon se asienta sobre los satélites Intelsat e Inmarsat, los cuales son responsables de la gran mayoría de las comunicaciones telefónicas entre los países y los continentes. Los 20 satélites de Intelsat siguen una órbita geoestacionaria, fijada sobre distintos puntos definidos del Ecuador. Esos satélites transportan primariamente tráfico civil, pero también transmiten algunas comunicaciones diplomáticas y gubernamentales, de particular interés para los países que integran el UKUSA.

Los satélites ajenos a Intelsat son monitoreados desde distintas estaciones. La estación de Shoal Bay, en Australia, intercepta a una serie de satélites de Indonesia., y la estación de Leitrim, en Canadá, intercepta las comunicaciones de satélites latinoamericanos, incluyendo el de la compañía telefónica mexicana Morelos.

Estados Unidos negó sistemáticamente la existencia de Echelon. Sin embargo, un informe lanzado a principios de 2001 por el Temporary Committee on the Echelon Interception System (Comité Temporario sobre el Sistema de Intercepción Echelon) luego de siete meses de investigaciones, concluyó que Echelon "Sí existe". [21]

7.5. LA PRIVACIDAD DESPUÉS DE LOS ATENTADOS DEL 11 DE SEPTIEMBRE

Los atentados del 11 de septiembre de 2001 produjeron una suerte de "derechización de la opinión pública norteamericana", en palabras del especialista en relaciones internacionales Carlos Escudé [13], que fue aprovechada por el gobierno de derecha de Bush. Fue así como se inició una fuerte ofensiva tendiente a permitir que las investigaciones gubernamentales vinculadas al terrorismo puedan omitir algunos derechos civiles.

Poco después de los atentados, el fiscal general de los Estados Unidos, John Ashcroft, declaró que él, unilateralmente y sin informarlo a la prensa, había instituido el espionaje de las comunicaciones entre abogado y cliente para los sospechosos sin ciudadanía estadounidense dentro del territorio norteamericano. "De un plumazo violó las enmiendas cuarta y sexta de la Constitución, que prohíben efectuar registros y apropiaciones irrazonables (en este caso de información), y garantizan el derecho a la representación por un abogado", señaló Escudé. [14]

El 13 de septiembre de 2001, dos días después de los atentados, el Senado de ese país aprobó la Ley para combatir el terrorismo del 2001, que amplió los poderes de la policía para intervenir las comunicaciones y aumentó el rango de situaciones en las que puede supervisarlas.

El proyecto, presentado por Orrin Hatch (Partido Republicano, Utah) y Dianne Feinstein (Partido Demócrata, California), estableció que cualquier fiscal federal o de alguno de los estados puede disponer la instalación del sistema de vigilancia Carnivore del FBI. [22]

[13] Escudé, Carlos. Un lugar peligroso.
[14] Escudé, Carlos. La crisis de los derechos cívicos en los Estados Unidos.

"Es imprescindible ofrecer a los organismos de seguridad todas las herramientas posibles que permitan buscar y llevar ante la justicia a los individuos que han producido una masacre de semejante magnitud en nuestra misma casa", dijo Hatch durante el transcurso del debate. [15]

Según la nueva ley contra el terrorismo, los fiscales pueden autorizar períodos de vigilancia de 48 horas de duración como máximo sin orden judicial alguna. La vigilancia se limitó en principio a las direcciones de los sitios web que se visitan y los nombres y la dirección de correo electrónico de los usuarios. No abarca el contenido de las comunicaciones.

Entre las situaciones que no exigen una orden judicial se mencionan las siguientes: "Amenaza inmediata contra la seguridad nacional de Estados Unidos, amenaza inmediata contra la salud o la seguridad pública, o ataques contra la integridad o el funcionamiento de sistemas de computación protegidos". Quedan incluidas, pues, la mayor parte de las actividades de hacking.

Un comunicado de la organización no gubernamental Electronic Frontier Foundation, señaló que "las libertades civiles del pueblo estadounidense sufrieron un fuerte golpe con esta ley, especialmente en lo referido al derecho a la privacidad de nuestras actividades y comunicaciones online. No hay evidencia alguna de que las libertades civiles hasta ahora hayan obstaculizado la investigación o el juzgamiento de grupos terroristas".[41]

Posteriormente, por orden del poder ejecutivo se creó la Oficina de Seguridad de la Patria (Office of Homeland Security, OHS) que no está sujeta a la supervisión del Congreso y donde el nombramiento del personal es prerrogativa exclusiva del Poder Ejecutivo. "La misma palabra *homeland* es exótica en el léxico cívico y político norteamericano, y sus matices semánticos están más asociados a las

[15] McCullan, Declan. Aprueban ley que permite al FBI realizar espionaje en Internet.

dictaduras europeas que a la democracia liberal del Contrato Social", señaló Carlos Escudé. [23]

El EPIC solicitó un pedido de información sobre el Office of Homeland Security apelando al Acta de Libertad de Información. Sin embargo, en una respuesta enviada a la Corte de Distrito en Washington, el Departamento de Justicia argumentó que el Office of Homeland Security no es una "agencia" y por lo tanto no está sujeta al Acta de Libertad de Información. El escrito afirmó que las funciones de la OHS son "solamente aconsejar y asistir al Presidente, y no ejerce ninguna autoridad sustancial independiente". Así, buscó equiparar a la OHS con el National Security Council, el cual en 1996 fue ejemplo de cumplir con las obligaciones de información que establece el Acta de Libertad de Información.[24]

CONCLUSIONES.

Hay algo que no esta bien en la Sociedad de la Información. Hay algo mal en la idea de que la "información" es una comodidad como una silla o un escritorio. El conocimiento es poder. El crecimiento de las redes informáticas, de la Sociedad de la Información , esta haciendo cosas raras y desbaratadas a los procesos por los que el poder y el conocimiento están actualmente distribuidos. No creo que la democracia prospere en un entorno donde imperios vastos de datos son encriptados, restringidos, apropiados, confidenciales, top secret, y sensibles. Yo temo por la estabilidad de una sociedad que construye castillos de arena a partir de bits de datos e intenta parar una corriente global con regios mandatos.

(Sterling, 1992).

CONCLUSIONES

Es evidente que los grupos que contiene la red van en aumento día en día, y es muy fácil que surjan nuevos grupos en la gran familia de clanes de la red. La libertad de expresión que permite Internet en todos sus aspectos, despierta la curiosidad de miles de nuevos internautas. En este medio se derrocha información, y un ínter nauta cualquiera puede acceder a información "confidencial" en muchos aspectos, o a una información que antes era imposible de obtener.

Día a día se pueden formar en la red nuevos grupos y personajes que de una u otra manera hacen distinto uso de estos conocimientos y de esa información.

La libertad de expresión que permite Internet en todos sus aspectos, despierta la curiosidad de miles de nuevos internautas cada día. En un futuro, la posibilidad de nuevos miembros en la red y el Underground será infinita.

En el futuro, la posibilidad de nuevos habitantes en la red y el Underground será infinita.

Los hackers se sirven de una amplia gama de artimañas para conseguir colarse en un sistema.

La información permite al verdadero Hacker o aspirante a Hacker progresar en sus investigaciones, pulir sus técnicas y simplemente, mantenerse entre la leite. Pero también es cierto que tanta información permite a usuarios no aspirantes a Hacker manipular tecnologías que antes sólo eran accesibles a los técnicos e ingenieros de cada rama. Por citar un ejemplo, en la actualidad es posible romper un sistema de televisión de pago sin tener ningún conocimiento. Ello se debe a que existen páginas repletas de información sobre cómo hacerlo. Es más, en realidad el usuario de la red puede permitirse el lujo de bajarse ficheros de la red que le permitirán ver canales de pago.

Nuevas formas de hacer negocios como el comercio electrónico puede que no encuentre el eco esperado en los individuos y en las empresas hacia los que va dirigido ésta tecnología, por lo que se deben crear instrumentos legales efectivos que ataquen ésta problemática, con el único fin de tener un marco legal que se utilice como soporte para el manejo de éste tipo de transacciones.

La ocurrencia de delitos informáticos en las organizaciones alrededor del mundo no debe en ningún momento impedir que éstas se beneficien de todo lo que proveen las tecnologías de información (comunicación remota, Interconectividad, comercio electrónico, etc.); sino por el contrario dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información, en las organizaciones.

Se ha explorado la concepción del fenómeno del hacking informático como un movimiento social; como la proliferación de tendencias hacker anarquistas sugiere, esta cultura necesita desesperadamente alguna comprensión, así como un oído amigable.

Hemos visto que la industria corporativa rechaza los conocimientos y habilidades técnicas de los hackers; no se podría hacer realidad un mayor nivel tecnológico si estas dos partes trabajasen juntas.

La respuesta a esto se encontrara en el futuro. A medida que la posibilidad de una Sociedad de Información global se ve más cercana, la gente debe estar deseando traerse a sus manos su educación técnica. Todos podemos aprender una valiosa lección de los hackers: que el apetito intelectual y la búsqueda del conocimiento debe ser central en nuestra sociedad.

CONCLUSIONES

La noción de una sociedad electrónica libre, y democrática ha sido advertida como una especie de utopía, donde la información fluye sin trabas y la libertad de expresión es esencial.

El debate continua; podemos sentarnos, esperar pacientemente, y ver como resulta todo; lo podemos actuar, auto educarnos y educar a cada uno, y estar preparados para lo que sea que venga.

> *Si necesitas un manual sobre como llevar a cabo cualquiera de los métodos antes expuestos, lee un fichero acerca de ello por favor. Y sea lo que sea lo que hagas, continua la lucha. Lo sepas o no, si eres un hacker, eres un revolucionario. ("Doctor Crash", 1986)*

Que así sea.

BIBLIOGRAFÍA

Páginas Electrónicas:

[1] **URL.** http://www.seguridata.com ÁNGEL, José de Jesús Ángel. Criptografía para principiantes. España. 2003.

[2] **URL.** http://www.arcert.gov.arhttp://www1.iblnews.com/canales/boletines/lacronica/206/miercoles,27.htm ArCERT. Manual de seguridad en redes. Argentina. 2005.

[3] **URL.** http://www.seguridadcorporativa.org MANUNTA, Giovanni. Presentación del libro Seguridad. Revista Virtual Seguridad Corporativa.

[4] **URL.** http://www.rediris.es/ftp MONSERRAT COLL, Francisco Jesus. Seguridad en los protocolos TCP/IP. España. 2005.

[5] **URL.** http://www.nai.com PGP for Personal Privacy. Traducción al castellano. Network Associates Inc. EE.UU. 2003.

[6] **URL.** http://www.rediris.es/cert POYATO, Chelo. COLL, Francisco. MORENO David. Recomendaciones de seguridad. España. 2003.

[7] **URL.** http://www.hackrules.tk/ ROSTECK, Tanja S. Hackers, rebeldes con causa. 2005.

[8] **URL.** http://www.hackerss.com/index.php Foro de consulta, Dudas y Downloads.

[9] **URL.** http://www.thepentagon.com/paseante TAHUM. La Biblia del hacker. 2005.

[10] **URL.** http://www.set-ezine.org/ SET, Saqueadores Edición Técnica.

[11] **URL.** http://www.delitosinformaticos.com/ Noticias de delitos en la red, generalmente relacionadas con el hacking.

[12] **URL.** http://freneticmig.com Herramientas, artículos y recursos útiles para seguridad y contra-seguridad informática.

[13] **URL.** http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html

[14] **URL.** http://www.iespana.es/zzprohibida Programas, tutóriales, guías sobre hacking y vulnerabilidades.

[15] **URL.** http://www.hackuma.com/ Hacking, manuales, tutóriales y textos.

[16] **URL.** http://members.tripod.com/~rebeli0n/ Acceso a recursos de información, noticias y enlaces de tecnología.

[17] **URL.** http://afgen.com/terrorism1.html Información de Terrorismo Ciberterrorismo y Ciberguerra.

[18] **URL.** http://www.computer-forensics.com Computer Forensics Ltd.2006.

[19] **URL.** http://outerheavenklan.iespana.es Manuales y guías descargables.

[20] **URL.** http://www.statusroot.net Web con información y herramientas sobre hacking y seguridad.

[21] **URL.** http://www.hakim.ws/ Downloads, textos explicativos y varias ezines.

E-Zines Revistas Electrónicas

http://www.jjf.org JJF.

http://www.netsearch-ezine.com NetSearch.

http://www.0ri0n.org Ori0n.

http://www.cdlr.org Proyecto-R.

http://www.raza-mexicana.org Raza-Mexicana.

http://rebelion.cjb.net Rebelion.

http://www.imedia.es/set -

http://www.vanhackez.com/set

http://www.uha1.com UHA.

Revistas:

[31] Revista Issues in Science and Technology.

[32] Infosecurity Magazine, 2001

[33] 2600

[34] The Hacker Quarterly,Hack-Tic

[35] Wired

[36] Computer Virus Development Journal

[37] Virus Report

[38] Revista Wired en Español.

[39] Diarios y revistas de México.

[40] MEXICAN HACKERS MAFIA.

Libros:

[50] The Hacker Crackdown: Law and Disorder on The Electronic Frontier, por Bruce. 2003.

[51] Redes de Computadora. Andrew S. Tanenbaum 4ta edición Prentice Hall.

[52] Los piratas del chip: La mafia informática al desnudo.2002.

[53] Caballero Gil, Pino. "Seguridad informática. Técnicas criptográficas", 2003.

[54] Intranets. Usos y Aplicaciones, Randy J. Hinrichs, PRENTICE HALL, México, 2002.

[55] Aprueba de hackers; Lars Klander; Anaya Multimedia; 2003.

[56] "Notas de Álgebra", Enzo R. Gentile, Eudeba. 2001.

[57] Ciencias Forenses. Víctor Chapela. México 2005.

[58] Defensa de la intimidad y otros derechos personalísimos (Artículo). Medina de Leiva, Elsa Valentina. 2001

[59] 2004 Diccionario Larousse de Bolsillo.2005.

GLOSARIO

Acceso root. Entrar en un sistema con el usuario root.

Administrador. Persona que se encarga de todas las tareas de mantenimiento de un sistema informático.

Administrador, sysop, root. Persona que se encarga del mantenimiento del sistema. Tiene acceso total, sin restricciones.

Antivirus. Programa que encargado de evitar que cualquier tipo de virus entre a la computadora y se ejecute. Para realizar esta labor existen muchos programas, que comprueban los archivos para encontrar el código de virus en su interior.

Backdoor. Puerta de entrada trasera a una computadora, programa o sistema en general. Sirve para acceder sin usar un procedimiento normal.

Black Box. Aparato que engaña a la central telefónica haciéndole creer que no se levantó el tubo del teléfono cuando en realidad se está produciendo una comunicación.

Bombas ANSI. Utilizando los códigos ANSI, se asigna una acción destructiva a alguna tecla. Me explico, ANSI es un conjunto de códigos estándar. Si en tu computadora uno de estos códigos lo ejecutara. Los códigos ANSI se usan para varias cosas, entre ellas, cambiar los colores de la pantalla, posicionar el cursos, y el método que usan las bombas ANSI, asignar a una tecla una acción determinada. Si esta acción es dañina al pulsarla hará el daño.

Bug. Un error en un programa o en un equipo. Se habla de bug si es un error de diseño, no cuando la falla es provocada por otra cosa.

CERT. Es un equipo de seguridad para la coordinación de emergencias en redes telemáticas.
Clave. Es el sinónimo de password o contraseña en el ambiente computacional; también puede ser el código que permite desencriptar un dato.

Cookie. Es un pequeño trozo de información enviado por un servidor de Web al buscador de un usuario. Cuando se visita un servidor que utiliza el desarrollo denominado "Magic Cookie (MC)", éste instruye al buscador de la PC para crear un archivo Magic Cookie al que se lo suele nombrar como cookies.txt o similar. En él, ingresa y queda una pequeña cantidad de información, dicho bloque de datos podría contener un identificador exclusivo para el usuario generado por el servidor, la fecha y hora actual, la dirección IP del proveedor del servicio de acceso a Internet mediante el cual la PC del usuario se conecta a la red, o cualquier otro grupo de datos que se desee.

Criptografía. Criptografía proviene del griego y se puede traducir como "La manera de escribir raro" (criptos de extraño y graphos de escritura). Consiste en modificar los datos de un archivo o los que se transmiten por módem, radio, etc. Para evitar así que los puedan leer personas no deseadas. Esta técnica ha tenido su principal aplicación en los ejércitos y en la diplomacia.

Cyberpunk. Corriente literaria dentro de la ciencia ficción que, entre otras cosas, se destaca por incorporar a sus argumentos el uso de la tecnología de las redes de computadoras.

Falsificación de software. La falsificación de software ocurre cuando un programa es ilegalmente duplicado y luego vendido como si se tratara de un producto legitimo. Los falsificadores pueden copiar el producto completo, incluyendo documentación, discos, etiquetas y hasta elementos de seguridad como hologramas.

FTP. (File Transfer Protocol: Protocolo de transferencias de archivos) Un conjunto de protocolos mediante el cual pueden transferirse archivos de una computadora a otra. FTP es también el nombre de un programa que usa los protocolos para transferir archivos de ida y vuelta entre computadoras.

Guest o Invitado. Cuenta pública en un sistema, para que la use alguien que no tiene una cuenta propia.

Handle. Seudónimo usado en lugar del nombre verdadero.

Key logger. Grabador de teclas pulsadas. Se utiliza para cuando deseamos saber las contraseñas, este programa graba cuando el usuario ingresa su contraseña. También se utiliza para saber cuales han sido las acciones de los usuarios en el sistema.

Lamer. Tonto, persona con pocos conocimientos o con poca "NET-iqueta".

Login, Username, Usuario. Nombre de registro de entrada. En una red de computación, nombre único asignado por el administrador del sistema usuario, que se usa como medio de identificación inicial. El usuario debe usar el nombre, así como su contraseña (password), para tener acceso al sistema.

Password, Contraseña. Es una herramienta de seguridad empleada para identificar a los usuarios autorizados de un programa o de una red y para determinar sus privilegios, como el de solo lectura, el de lectura escritura, o el de copiado de archivos.

Patch. En inglés, parche. Modificación de un programa ejecutable para solucionar un problema o para cambiar su comportamiento.

Payload. Efecto visible de un software maligno.

Phreaker. Persona que usa comunicaciones sin pagarlas o pagando menos de lo que corresponde.

Pirateria de software. Copia ilegal de software con derecho de autor sin que medie el permiso expreso del editor.

Rabbit. En inglés, conejo. Programa que provoca procesos inútiles y se reproduce (como los conejos) hasta que agota la capacidad de la máquina.

Redirigir. Cambiar el destino de algo. Por ejemplo, redirigir una llamada es hacer que suene en un teléfono distinto del que se intentaba llamar.

Root. Cuenta del administrador en UNIX. Es la más poderosa: permite el acceso a todo el sistema.

SATAN. El SATAN, Herramienta para el Análisis de Administradores de Seguridad de Redes (Security Administrator Tool for Analyzing Networks) es una aplicación realizada por el informático norteamericano Dan Farmer y el gurú cibernético americano-holandés Wietse Venema. Esta es capaz de adivinar el nivel de vulnerabilidad de un host (ordenador servidor de Internet) y de todas las máquinas conectadas a él via Internet (su dominio), ya que permite conocer su nivel de encriptación, password, etc. SATAN también se puede obtener libremente por FTP

en la red, lo que significa que puede ser utilizado tanto por los propios servidores para ver su nivel de vulnerabilidad como por los hackers. Es por tanto un arma de doble filo.

Shell. Intérprete de comandos de un sistema operativo. Es el que se encarga de tomar las órdenes del usuario y hacer que el resto del sistema operati vo las ejecute.

Shoulder Surfing. Espiar por detrás de un hombro para tratar de ver información interesante. Al cual estamos muy expuestos, y es un método comúnmente usado para accesar cuentas de otras personas.

Sniffer. Un sniffer es un programa que escucha todo el trafico de la red a la que esta conectada la computadora, aunque los datos no sean para él. Esto es posible por que la mayoria de las tarjetas de red ethernet tienen un modo llamado promiscuo, que les permite aceptar todos los datos de la red.

Tempest. (Transient Electromagnetic Pulse Surveillance Tecnology), son especificaciones que los sistemas informáticos para el gobierno de EU deben cumplir.

Terminal. Puerta de acceso a una computadora. Puede tratarse de un monitor y teclado o de una computadora completa.

Trashing. Arte de revolver la basura para encontrar información útil.

UNIX. Sistema operativo utilizado por la gran mayoría de máquinas de Internet.

ZAPPER. Programa que se encarga de borrar los logs que graban las entradas, acciones y salidas de usuarios, por ejemplo cuando un hacker entra en un sistema debe ejecutar un zapper para no se cazado.