
# Los clanes de la ReD
# 2000

# Hackers

**Claudio Hernández**



**Los clanes de la ReD**
**2000**

# Copyright

# Agradecimientos

**El primer agradecimiento es siempre para esos lectores fieles, los cuales están puntualmente donde deben de estar, en su sillón favorito o en este caso delante del monitor leyendo cada una de las paginas que componen este libro. Para todos ellos, he aquí una obra que les enseñara muchas cosas. Sobre todo, conocer la nueva cibercultura y protegerse de ella...**

**El siguiente agradecimiento es para Kriptopolis, la mejor WEB de temas de seguridad y criptografía.**

**Finalmente mis agradecimientos a todos los profesionales y editores que siempre han confiado en mi, publicando todo aquello que escribo.**

**A todos ellos, gracias**

# Índice general

## 11. Echelon, espías en el cielo

11.1 Enemigo publico

11.2 Espías desde el cielo

11.3 Conexo a Echelon, la NSA y otros espías

## Glosario de términos

# Preliminares

Se que es difícil querer explicar en pocas palabras el porque de esta obra que tiene delante de su monitor, o con toda probabilidad entre sus manos, ya sea porque lo ha impreso o alguien se lo ha pasado. De cualquier forma usted ya tiene este ejemplar y mi obligación es explicarle el porque de esta obra y de su difusión gratuita.

En la actualidad se escribe y mucho sobre el tema de los Hackers, una tradición iniciada por mi hace unos cuantos años, y lo cierto es que mas que informar, parece que todos los periodistas del mundo se han puesto de acuerdo en una cosa. Poner las cosas feas a la nueva cibercultura, o dicho de otra manera, dar una imagen nada apreciable de los Hackers, piratas informáticos y demás índole.

Este libro no es un pretexto para defenderlos, pero tampoco pretende culparles de nada. Simplemente, esta obra se ha creado con el fin de informar a todo aquel que lo desee, que son, que hacen y como actúan los Hackers y los nuevos clanes de la ReD. Para ello, he tenido que revelar algunas cosas en este libro y quizas mas de uno piense que yo sea uno de ellos, todo lo contrario, pero he de admitir que algunas cosas he aprendido mientras los he estado investigando de cerca.

Pero ello no quiere decir que desee fomentar ciertas actuaciones, prueba de ello son mis ultimas investigaciones en el campo de la protección del Software y sistemas de comunicación, en favor de las principales multinacionales. Ademas, el conocimiento en este terreno, me permite escribir un buen puñado de reportajes y unos cuantos libros.

El presente libro, podría decirse, que contiene de todo un poco. Digamos que es algo así como un manual para algunos y un libro de lectura para otros. Creo que he tocado todos los términos de la nueva cibersociedad, pero en futuras revisiones incluiré nuevos contenidos que ahora están en borrador.

También he de decir, que la presente obra es algo así como un experimento, o mejor aun, una experiencia personal nueva, “ no en el ambito de escribir, claro esta “ una experiencia que quiero llevar mas allá de mi ordenador personal. Una experiencia que pretende recoger todas las ideas, sugerencias, opiniones y criticas de todos vosotros, con el fin de poder gestar una obra mas completa, mas amena y por supuesto, mas interesante.

Finalmente, solo me queda decir, que espero que disfrute con la lectura de este libro y que aprenda mucho de el, pero que todo lo que aprenda lo emplee para su bienestar personal, para su protección y para saciar la sed de la sabiduría.

Otro dato para terminar, la presente obra recoge contenidos de dos de mis libros y otro tanto, en reportajes.

**Claudio Hernández**
**Noviembre de 1999**

# Prologo

**...Dadme 10 Hackers y dominare el mundo en 24 horas...**

**Están en tu disco duro. Están en tu módem. Están en tu teclado. Están en todas partes y su reino es la gran telaraña de Internet y los bits que viajan por la ReD.**

Así es como empieza el nuevo documental, que en la actualidad, estoy escribiendo para varios canales de televisión de diversos países. He querido incluir una pequeña parte del guión en el prologo y en su primera parte, como adelanto de lo que será sin lugar a dudas, la principal fuente de información sobre este contenido, llevado al formato de las imágenes. Este es, con toda probabilidad el mejor prologo para esta obra. Así el texto es el que sigue.

Hackers, sinónimo de delincuentes informáticos para algunos, y genios de las nuevas tecnologías para otros, lo cierto es que la palabra Hackers ha revestido diversos significados a través del tiempo y los medios de información. Si retrocedemos un poco en el pasado, daremos cuenta que así se les llamaban a los técnicos de telefonía por la forma en que solían reparar los teléfonos. Con un golpe seco como habitualmente ponían de nuevo en marcha el teléfono, pronto este modo de operar, ostento el titulo de " Hack " que traducido literalmente significaba Hachazo y que a su vez resumía, el arreglo del aparato tras un golpe certero. Así a los técnicos que empleaban esta técnica se les llamaban cariñosamente " Hackers ".

Años mas tarde un grupo de estudiantes del MIT arrebataron el titulo de " Hackers " a estos técnicos, por las soluciones que adoptaron los mismos por hacerse un hueco delante de la única computadora de la universidad, sin necesidad de penetrar físicamente en la habitación, donde traqueteaba incesante la gran mole de cables y transistores ante las ordenes de unos dedos que no estaban allí. Desde la espesura de las paredes y entre las sombras de la noche, el grupo de estudiantes noche tras noche, programaban a distancia sin saber exactamente que ellos mismos comenzarían, en sus sesiones nocturnas, la que seria sin duda la era de los Hackers.

Esta es su historia.

**Voz en OFF**

Mucho a llovido desde que este grupo de estudiantes marcaran apenas sin darse cuenta, una definición para este tipo de actos " en la rebeldía " de hacerse con unas horas delante del computador, todo un hito a seguir. Desde entonces las técnicas denominadas del Hacking y la propia tecnología han cambiado mucho. También es cierto que los hackers ya no están solos y que en sus caminos se cruzan los clanes de la ReD, toda una estirpe de genios y locos de las computadoras y las tecnologías que han propiciado buena cantidad de libros, reportajes y películas, pero sobre todo han sembrado el terror ante los internautas de la ReD y los usuarios de los ordenadores y las nuevas tecnologías.

**Un hombre obeso con bigote es entrevistado**

...si, se lo que es un virus ! los virus te fastidian el ordenador y cuando lo hace te muestra un mensaje absurdo, es obra de locos!...

**Una mujer de poca edad es entrevistada**

...Hackers ?...son esos tipos que se pasan el día y la noche delante del ordenador...y que...lo saben todo a través de el...

**Un niño entrevistado**

...si, son personas muy inteligentes que lo saben todo acerca de los ordenadores y odian a Bill Gates. Son genios...yo quiero ser uno de ellos cuando sea mayor !

**Un anciano entrevistado**

...Un jaaa...que ? que es eso ?

**Voz en OFF**

La prensa los describe como delincuentes informáticos. Algunos como el chico entrevistado quiere ser igual que ellos cuando sea mayor y los cataloga de genios. Otros simplemente ven en ellos el lado malo de la tecnología. Pero sea cual sea la definición que se hace acerca de ellos, lo cierto es que son una parte importante de la ReD de Internet.

**Entrevista a un experto sobre Hackers**

...Los Hackers son una parte fundamental de la ReD y de los ordenadores, quizás porque están siempre ahí, detrás de todo cuanto sucede en la ReD. De hecho son los únicos que conocen perfectamente todos los entramados de la ReD. Y hoy por hoy el mito de la ReD no esta en la capacidad de información de esta, si no en la forma en como se mueven estos genios de la informática. Siempre ocultos, buscando nuevos bugs en los sistemas remotos con el fin de poner a prueba sus altos conocimientos. Solo de esta forma, pueden sentirse seguros en una ReD plagada de nuevos clanes aun mas terroríficos que los Hackers...

**Voz en OFF**

Esta es la definición de un Hacker según algunos expertos, pero cual es la definición real de todos los que en nombre de los Hackers, realizan sus fechorías ? La respuesta puede ser adversa y representarse de muy variadas formas. La prensa y la televisión siempre se refiere a piratas informáticos, cuando se refiere a todos ellos. Pero es que existe alguien mas, además del Hacker ?. Según los expertos los Hackers no están solos.

**Entrevista a un experto sobre Hackers**

...No están solos. Detrás de ellos existe toda una legión de acrónimos que engordan cada vez mas la lista, pero los mas inmediatos son los Crackers que curiosamente también se ven divididos según su propia especialidad. Pero puedo adelantar que los Crackers en su puro estado, son aquellos que penetran en un ordenador remoto y vulnera las defensas, para extraer del ordenador u ordenadores remotos, información importante, cuando esto sucede el Cracker suele dejar su tarjeta de visita en forma de virus en el peor de los casos o en forma de Troyano, si su intención es volver a entrar en el. Este es el primer grupo. El segundo grupo, también denominado Warezman, esta especializado en Crackear Software, esto es, desproteger un Software en versión Trial o de prueba y conseguir que este no presente caducidad. Esto lo consiguen escribiendo un pequeño programa que parcheara el ejecutable del programa afectado y de ahí surge el nombre de Crack. Un Warezman también puede definirse en dos grupos, los que ya he comentado y los que ofrecen Software crackeado a través de Internet. Si esta ultima operación se realiza desde el CD, esto es, que el Warezman duplica Software en CD, entonces se define como pirata informático...

**Voz en OFF**

También denominado Ingeniería Inversa, el cracker domina esta técnica que consiste en dar la vuelta a las cosas. O lo que es lo mismo, invertir el proceso de una función. En criptografía se trata de obtener la clave para recuperar el mensaje. En televisión de pago, se trata de obtener la secuencia del embrollado de la imagen. Y en el terreno de las tarjetas electrónicas se trata de obtener el algoritmo que las protege.

Hasta aquí, un poquito del guión, el resto deberán tener paciencia y ver el reportaje en televisión...

# Capitulo 1

# Introducción

La necesidad de escribir un libro como este era evidente. La actividad del Hacking fuera del ordenador y de la red de Internet, a cobrado fuerza y es quizas aun mas peligrosa que tal como la conocemos a través de los medios de información. Sin embargo, vamos a abordar en este libro todos los grados del hacktivismo, dentro y fuera del ordenador personal, dentro y fuera del espionaje industrial y en definitiva en todos sus aspectos mas conocidos y los menos conocidos. Así, la clandestinidad impera por todas partes, pero no es ese el tono que elegiremos en el presente libro.

El Hacking es una realidad y queremos exponer sus fundamentos. Escrito desde España, el libro quiere demostrar como el Hacking también ha hecho furor en nuestro País. Al contrario de lo que se creía, en nuestro país, el grado de piratería es superior al resto de los países. Sin embargo hay que saber diferenciar lo que es la piratería y lo que es el verdadero rol del Hacking.

Cualquiera de nosotros, cuando intentamos copiar una película de video, esta atentando con la piratería. Eso no es un Hacking. Si no un grado de clandestinidad y un acto de violación de los derechos de autor. El Hacking rivalida este hecho con otra intromisión. El Hacking simplemente nació como un estado de diversión y satisfacción personal y durante muchos años a revestido diversos significados. Obviamente todos los comentarios acerca del Hacking han resultado siempre acusadores y negativos. Pero la culpa no esta en el hecho de hacer Hacking, sino en el uso que se hace de el.

Hacker es una palabra prácticamente intraducible que ha revestido, a lo largo de los años, diversos significados como ya se ha dicho. Pero parece ser que este acrónimo se vincula muy especialmente a los llamados Hacks o dicho de otra manera, así se llaman 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 mas que probable que quienes lo hacían se denominaban Hackers. De cualquier forma nunca sabremos 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 trastadas 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 Hacking, pero permítame que le diga que estamos entrando en otros terrenos que van mas 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 de las paginas de este libro. De cualquier forma ante unas leyes nacidas por el bien de unos pocos, la mayoría de nosotros somos unos verdaderos delincuentes.

Pero quiero dejar bien claro el tratamiento que se le puede dar a este pequeño grupo de ***« sabios «*** antes de continuar explorando los inicios de esta nueva generación. Un 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 Hackes también fisgonean sistemas fuera de una CPU. Solo tenemos que echar una ojeada a nuestro alrededor para saber cuantas cosas mas atentan contra la curiosidad.

Hacer una llamada de telefono supone un reto muy importante para alguien que no tiene dinero, pero no es esa la intención. Sin embargo si lo que se desea es conocer bien los sistemas de conmutación de una red de telefonía inteligente, que mejor que dejarse atrapar por ella para beber de sus consecuencias. Ya en la segunda Guerra mundial se cifraban los mensajes y las comunicaciones y hoy por hoy todas las comunicaciones de los Satélites están encriptadas. 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.

Sin embargo la gula se lo come todo. El hambre no se sacia y se culmina con una proeza delictiva. Violar los secretos de una comunicación convierten a uno en un Cracker, algo mas devastador que un simple fisgoneo de Hacker. Como una extensión mas, surge el Carding, otro fenómeno capaz de clonar las tarjetas de credito 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.

Solo en España el uso fraudulento de estos conocimientos ha conocido un ascenso espectacular. Y en Estados Unidos el pasado año se dejaron de percibir mas de 63.000 millones de pesetas por estos conceptos. Por otro lado se estima que cada día nacen o se crean entre tres y cuatro nuevos virus informáticos y uno de cada dos estudiantes de informática entra en el ordenador de su compañero robándole el pasword. Todo esto es lamentable, porque la tendencia a desaprovechar las energías positivas va en aumento. Un buen conocimiento debe ser empleado para mejorar los sistemas en los que se trabaja, pero es mas fácil hincharse de satisfacción con un rictus en los labios demostrando que acabas de joder un ordenador o un telefono.

Estas son las decisiones mal intencionadas y las que mas perjudican al verdadero Hacker. Una imagen borrosa sobre este personaje puede echar por la borda todo el buensaber de estas entes. Otro caso negro para el Hacking son los 15.000 millones de pesetas que se dejaron de percibir en Europa por el uso fraudulento de tarjetas de acceso inteligentes clonadas de los canales de televisión de pago Europeas. Un Buen Hacker no habría puesto en circulación estas tarjetas, pero si hubiera enseñado a los demás, dentro de su pequeño foro disciplinario, como funcionan este tipo de tarjetas por el mero hecho de decir lo se

todo sobre ella y creo que posee un fallo...

Un bus, una codificación mediocre, son las fuentes de interés para un Hacker para mejorarlo. Una complejidad en los mecanismos de seguridad de cualquier sistema informático o electrónico despiertan en el un interés creativo. Después toma notas...las notifica y alguien hace mal uso de ellas.

Es el lado oscuro de Hacking.

Nadie es de fiar allí dentro y fuera se dan los conocimientos que se quieren por un puñado de periodistas inexpertos en el tema. Después todo hace explosión en un cóctel sin sabor y todo el mundo te señala como alguien realmente malo.

Pero hay que tener en cuenta ciertas cosas interesantes para mejorar la seguridad de los sistemas de nuestro complejo mundo. Un sistema de seguridad de por si no tiene mucha consistencia si no es atacado por alguien de fuera. En este proceso se demuestra la fuerza del sistema. Si el intruso entra es porque existe un error en el diseño. Así, si no es por el intruso los creadores del sistema de seguridad nunca sabrían que existe un agujero negro en su sistema. Después el intruso es sometido a un estudio y se le pide colaboración ya que normalmente siempre tendrá mas conocimientos que el propio creador y esto es porque se preocupa realmente de la seguridad del sistema. Es un reto demostrar todo lo contrario y lo consigue.

Y al contrario de lo que se pretendía, no se castiga al intruso, sino que se le contrata en la gran empresa. Esta es la política que persigue un buen Hacker. Sin embargo buenos, lo que se dicen buenos los hay bien pocos.

El mal uso de los conocimientos y el poder casi infinito que uno puede tener con ellos, en un mundo dominado por el conocimiento y la tecnología, ponen en tela de juicio cualquier intento de Hacking. Ya que hoy por hoy cualquier modificación en un fichero informático o una conmutación en un descodificador de señales de televisión, es un acto de consistente violación de los derechos de copyright.

Por ello la dominación de la tecnología es absoluta.

Hasta aquí he replanteado la posibilidad de que no todo el Hacking es malo y de que no solo los Hackers habitan en los ordenadores. Aunque es cierto que los ordenadores han popularizado enormemente a los hackers en los últimos años, no es cierto que solo habitan en ese submundo, ni tampoco es cierto que se emplean bien los conocimientos con fines científicos y no lucrativos. Por desgracia el hacking se ha convertido en el índice de un gran libro de insolencias e intromisiones peligrosas. Por lo que definir correctamente el Hacking se hace especialmente complicado.

Que aunque existen desde hace muchísimo tiempo, es ahora cuando conocen su propio acrónimo en el argot técnico y es ahora cuando la tecnología brinda la oportunidad de serllo con mas fuerza, ya que hay que reconocer que la proliferación de ordenadores personales, la red de Internet y los miles de comunicaciones encriptadas, son un gran caramelo sin saborear. Las tecnologías evolucionan y con ella los Hackers se ven forzados al limite de sus actuaciones. Fisgonear un ordenador o tratar de descodificar un canal de pago es siempre un acto delictivo, por lo que por mucho que hablemos, siempre estaremos catalogados como delincuentes informáticos y tratar de quitarse esa mascara es tarea imposible.

Hoy por hoy todo cuanto se crea, reposa sobre la base de los códigos y las encriptaciones para sacar el mayor rendimiento de la tecnología y el producto. Los programas de ordenadores son un buen ejemplo de ello. Las televisiones se han convertido en canales de pago temáticas y a la carta que requieren de sistemas

complejos de encriptacion y control para asegurarse una rentabilidad del canal. Los nuevos soportes de grabación ya son digitales para todos los sistemas ya sean de video, audio o datos y poseen códigos de protección contra copias piratas. A su vez todos estos soportes digitales, tales como un simple CD, DVD o Minidisc pueden estar encriptados y reducidos a un puñado de códigos que hacen de ellos una forma de pago por visión. Esto es, pagas y ves.

Ante este panomara se hace obvio que siempre habrá cierta curiosidad por « estudiar « estos códigos y estas propias tecnologías. Vivimos en un mundo de códigos, encriptaciones y rupturas de sistemas. Sin embargo como creo haber dicho ya, este fenómeno se remonta mucho tiempo atrás, desde que se emplearan las palomas como mensajeras. En cierta época los mensajes eran cifrados y convertidos a un puñado de palabras indescifrables y ya existían quienes descifraban el mensaje del enemigo. Por aquel entonces no se conocían como Hackers y ni tan siquiera estaban penalizados. Solo la llegada del ordenador ha revolucionado este sector y solo desde los ordenadores se ha hablado mucho sobre los Hackers.

Desde aquí queda poco mas que decir. Podría estar contando batallitas de Hackers hasta perder el pulso de la pluma, sin embargo creo que eso seria oportuno para otra ocasión. En esta introducción me conformo con definir por encima lo que es un Hacker y especular superficialmente sobre ellos. Defenderlos o acusarlos seria caer en un grave error. Según por donde se mire se actuaria de una u otra forma. Criticar los hechos podría ser nefasto y entraríamos en denuncias continuas que no son precisamente la ideología de este libro. Defenderlos hasta la muerte podría ser también otro error, ya que podríamos pecar de egocentrismo. De modo que solo queda exponer los hechos, o mejor dicho de otra manera, solo queda opinar y exponer mis criterios. Sentar las bases de lo que es el Hacking y explicar o mostrar los conocimientos adquiridos en un terreno complejo y difícil como es el mundo de las nuevas tecnologías, tecnología que agrupa la informática, las comunicaciones y los sistemas de pago por televisión.

Si, ha leído bien, los sistemas de pago por televisión también son el objetivo de la mayoría de los Hackers, de sobras es sabido de la existencia de Software para descodificar canales de pago. La criptografía también esta presente en esta área de las nuevas tecnologías y los nuevos Hackers se especializan, cada vez mas, en el tratamiento de algoritmos y sistemas de cifrado, que tan empleados están siendo en la televisión y en la informática.

Finalmente, me queda añadir una serie de opiniones o manifiestos de algunos Hackers a los que he conocido personalmente y con los que he charlado largamente, hasta descubrir algunas de sus necesidades. En las siguientes lineas encontrara todo tipo de declaraciones, esto es debido a que los Hackers que entreviste pertenecían a diversos campos de acción, lease televisión de pago o informática.

**Carta de un Hacker a una editorial:**

**Hola, soy Cybor. Probablemente no me conozcan. Tampoco pretendo salir en la prensa. Eso no me importa, sin embargo si hay otras cosas que me interesan mas que mi identidad. Por ejemplo, me interesan las aperturas de sistemas cifrados. Pero eso es algo que nadie te enseña. Eso tienes que aprenderlo por ti mismo. También me interesa que todos sepáis quienes somos y que no estamos solos en este peculiar mundo. Me interesa que sepan que no todos los Hackers somos iguales. También me interesa saber que la palabra Hacker tiene un significado muy curioso.**

**En un articulo reciente se publicó que se nos conocían como piratas informáticos. es probable, pero creo que están tremendamente equivocados. Quiero reivindicar mi posición. Pero lo cierto es que cada vez que hablan de nosotros es para decir que hemos reventado el ordenador de tal multinacional con grandes perdidas o que hemos robado cierta información. estas cosas suceden, y particularmente tengo que decir que estas cosas están al alcance de otros personajes mas peligrosos que nosotros. En nuestro mundo habitan los crackers y los phreackers. También están los snickers y cada uno de ellos tiene su cometido, pero para la mayoría todos somos iguales y todos somos piratas informáticos.**

**Pero quiero ir por pasos. ¿ que te parece saber de donde procede la palabra Hacker ?. En el origen de esta palabra esta el término Hack - algo así como golpear con un hacha en ingles-, que se usaba como forma familiar para describir como los técnicos telefonicos arreglaban las cajas defectuosas, asestándoles un golpe seco. También mucha gente arregla el televisor dándole una palmada seca en el lateral. Quien hacia esto era un hacker. Otra historia relata como los primeros ordenadores grandes y defectuosos, se bloqueaban continuamente y fallaban. Los que las manejaban se devanaban los sesos creando rutas para aumentar la velocidad y cosas parecidas. Estas cosas se denominaban Hacks y a los que lo hacían se les llamaban Hackers.**

**Otra denominación se le hacia a aquel experto en cualquier campo que disfrutaba modificando el orden de funcionamiento del aparato. De esta forma siempre superaba las limitaciones y esto le producía una alta satisfacción. A estas personas también se les llamaban Hackers. Pero pronto surgieron otros acrónimos como Crackers. este acrónimo surgió allá por el año 1985, y fue inventado por los propios Hackers para diferenciar a aquel que fisgaba en un ordenador con aquel que creaba un virus dañino o copiaba un software. Así, frente a un ordenador ajeno un Hacker y un Cracker no son la misma cosa.**

**Por otro lado en algunas ocasiones un Hacker es muy útil porque siempre detecta un agujero en cualquier programa nuevo. Esto es bueno para ponerlo en conocimiento de la empresa que ha creado el programa. El Cracker aprovecharía este error para entrar en el programa y copiarlo.**

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

**Pero, volviendo a los Hackers. ¿ Como son ? ¿ Que aspecto tienen ?. Cuando alguien oye mencionar la palabra Hacker rápidamente se le viene a la cabeza un adolescente ojeroso, con los ojos inyectados en sangre que ha pasado las ultimas 24 horas delante del ordenador. esta imagen esta estereotipada. No es así. Un Hacker puede ser cualquier estudiante de informática o electrónica, que sale con los amigos y que tiene novia. Un Hacker es una persona normal como tu.**

**Los Hackers son casi siempre gente joven. Quizas somos los que mas nos interesamos por la tecnología. Un Hacker normalmente despierta el gusanillo a temprana edad. Y no se hace de la noche a la mañana. Cuando logra serlo después de realizar un Hack, se busca un apodo y no da la cara por cuestión de seguridad. La gente todavía no confía en nosotros y nos ven con ojos**

**malos.**

**Normalmente al final de todo somos contratados por empresas importantes para ayudarles en su trabajo. y otra cosa que hacemos es contar como funciona la tecnología que se nos oculta. Este método se llama enseñar y creo que no es nada malo.**

**De modo que si un Hacker escribe un libro es porque tiene algo que enseñar y nada mas. Bueno, creo que ya he escrito bastante. son las doce y media de la noche y mis padres ya se han acostado. Mañana tengo que madrugar. Y sobre todo quiero que quede buena constancia de lo que somos.**

**Cybor, Bangor Diciembre del 96 Maine**

Me han invitado a realizar el prologo de esta obra y por supuesto he aceptado. Solo diré que me llamo Stivo. Por supuesto me considero un buen Hacker y tengo algo que decir. Tengo muchos colegas que piensan como yo y actúan como yo. Por el cual quiero exponer mi particular punto de visión ante todo este embrollo. Quiero definir en pocas palabras lo que es el verdadero rol de los Hackers. Y quiero diferenciar una intromisión de un acto delictivo. Y aunque el autor de esta obra ya habrá expuesto su particular punto de visión sobre este concepto yo quiero aportar mi grano de arena.

***Los Hackers responden a perfiles psíquicos de carácter huraño y desconfianza continua, si decides caminar por el « lado salvaje de la red «, actúa con prudencia, porque allí nadie es de fiar.***

Probablemente este es el perfil con el que se trata de definir a todos aquellos que algo tienen que ver con la practica de la piratería o el Hacking. Otra declaración de hechos es lo que sigue;

***« la primera vez que conseguí engañar al ordenador remoto, todo mi cuerpo se estremeció de regocijo...»***

Dos aspectos muy diferentes, pero basicos, mitificados por unos y descalificados por otros y realmente desconocidos por la mayoría de nuestra sociedad, estos dos puntos de vista aparecen como dos aspectos basicos a tener en cuenta a la hora de definir la imagen perfecta de un Hacker.

Ambos extremos son puntos deseados por todo aquel que se inicia o quiere reinventar una génesis ya hiperextendia por todo el planeta, así la desconfianza de un Hacker se entenderá mas adelante y la introversia es el grado de satisfacción personal.

Después de estas dos intromisiones, se formulan muy a menudo otras preguntas tan miticas como ***¿Que es un Hacker? ¿Que es necesario para convertirse en Hacker? ¿Que persiguen? ¿Quienes son?...***La primera pregunta tiene como contrapartida los dos primeros puntos anunciados anteriormente. Las siguientes, son las insistentes preguntas de todo aquel que se sienta delante de un ordenador o de una imagen grisáceo en el televisor.

A menudo alguien que esta sentado delante del ordenador se siente tentado a juguetear con el, con la

intención de descubrir algo oculto en su propio ordenador, que le permita quizas hacer algo mas que escribir. Esto es un acto instintivo. También es instintivo abrir el descodificador de Canal Plus y ver sus entrañas con ojos desencajados. Inmediatamente nuestro corazón empieza a bombear con mas fuerza de la habitual bajo nuestro pecho y desistimos la tentación de hincarle un destornillador al descodificador abierto.

Sin embargo existe otro grupo, quizas con un espíritu mas rebelde y aventurero, que comienza a rumiar alrededor del aparato. Las cejas enarcadas y las manos cruzadas detrás de la espalda mientras se pasea por la habitación, están fraguando lo que será un futuro Hacker.

Esta actitud es instintiva también, pero esta fraguando un futuro rompedor de códigos que mas de un quebradero de cabeza ocasionara a mas de uno sin la menor intención de joder al vecino.

***Entonces que es un Hacker?.***

Si hacemos esta pregunta a alguien de la calle, probablemente conteste con un insulto. En nuestro país este fenómeno no es bien conocido muy bien todavía. Los medios de comunicación se han hecho eco de ello en los últimos meses y podemos ver en las revistas de informática mas prestigiosas como algunas columnas detallando alguna fechoría de un Hacker, reposa en la intimidad de la parte derecha de la pagina. Algunos se dan de bruces con la noticia para leerla bajo un tic nervioso, les entusiasma, otros, simplemente pasan la pagina.

Es desalentador.

Pero lo cierto es que el Hacking se esta convirtiendo casi en una profesión. Y a ellos les han salidos rivales. Estos son los Phreackers y los Crackers.

Así, a las primeras preguntas se añaden otras. ***¿ Quienes son estos individuos ? ¿ Que persiguen cada uno de ellos ? ¿ Y porque tantos acrónimos ?.*** Lógicamente aquí no podremos definir todo esto de un solo golpe, de modo que iremos desentrañando uno a uno las incógnitas de este poderoso mundo de genios rebeldes.

He dicho genio rebelde?.

Si es así, quizas sea esta una definición de primer acercamiento de lo que es un Hacker. Otra definición, podría ser la que sigue; ***« El hacker es aquel individuo solitario que entiende de ordenadores y se dedica a piratear sistemas informáticos y obtener información de lugares no autorizados.***

Otra definición seria el que sigue; ***« La falta de recursos economicos para mantener el telefono o el canal de pago, ayuda a buscar el lado oscuro del fraude.***

Ambas definiciones son quizas las mas correctas, pero estamos seguros de que existe algo mas. A veces el espíritu introvertido como el que poseen los gatos, hace que muchos individuos quieran saber que sucede detrás de la tecnología. Así un canal encriptado es una tentación increíble para un experto de electrónica. Saber que hay detrás de la imagen grisáceo o desordenada es todo un reto significativo.

A partir de hay, es cuando se define un Hacker.

Pero un buen Hacker es aquel que logra su objetivo.

Un Hacker conseguirá serlo, si consigue introducirse en otro ordenador y leer o modificar sus ficheros. También se es un Hacker cuando se descubre el orden en que el canal de pago transmite las lineas de video.

Después de esto un buen Hacker se las arreglara para desarrollar sus propios programas desencriptadores

de códigos o sus propios descifradores de señales de video, audio o datos. Estas herramientas a menudo serán utilizadas en sus incursiones en otros ordenadores y siempre que se localice un enlace de televisión codificado, ya sea de noticias, futbol u otros eventos. La curiosidad de un Hacker es insaciable, como el apetito voraz de un tiburón. Sin embargo todo quedara hay.

Un buen Hacker solo buscara información. Un buen Hacker solo se interesara por el virus de Ebola, los ovnis o las técnicas de codificación de las grandes multinacionales. Un buen Hacker quiere ver aquello que un telespectador normal no puede ver en su televisor.

También se busca el ahorro propio. Pero es aquí cuando se entra en otro terreno, quizas mas peligroso. Se ha de tener en cuenta, también, el reto que supone para un Hacker poder acceder a cualquier sistema seguro o abriendo el canal de pago que se anuncia como algo seguro.

La satisfacción personal de lograr el objetivo deseado es como una bomba de éxtasis. Pero no se busca nada mas. Comentar o difundir como lo ha hecho, solo ayuda a descubrirlo como un « ***delincuente electrónico*** «, ademas alguien podría hacer mal uso de su información y de sus conocimientos.

Así nacen los Crackers.

Este nuevo grupo ademas de coincidir en el grado de satisfacción al entrar en un sistema seguro, tienen como objetivo comercializar sus ***« piraterías»,*** con el fin de hacerse ricos. También pueden tener represión y contraatacar con virus dañinos a los sistemas informáticos. Sin embargo la habilidad de crear virus informáticos puede ser algo que este al alcance de un Hacker también. De modo que no esta bien definido quien es realmente quien introduce estos virus informáticos. A menudo se crean por error y otras para comprender mejor los sistemas de seguridad informáticas.

Pero sea cual sea la realidad, lo cierto es que los virus informáticos presentan una grave amenaza para nuestra sociedad. De igual modo el Cracking es también una amenaza para los fabricantes de programas y para las cadenas de televisión. Los Crackers crean Warez, ***( programas informáticos piratas )*** revientan programas y tiran abajo todo lo que se mueve por Internet. El olfato destructivo de un Cracker crece a medida que las multinacionales lanzan nuevos productos. Cuanta mas seguridad exista, mayor es la tecnología empleada por un Cracker. En el ambito de la televisión de pago, abrir un canal encriptado y reventar sus códigos le permite al Cracker poner en jaque al grupo emisor mientras se enriquece rápidamente. También hay que recordar que el Hacker tiene la habilidad de abrir el canal de pago, pero no lo negocia con nadie, por lo que ambos términos son fácilmente confundibles.

Sin embargo este no es tampoco un grupo aislado, como ellos, están los Phreakers. A menudo se les confunden descaradamente entre ellos, pero lo cierto es que, aunque todos satisfacen sus deseos, cada uno de ellos se especializa en su propio juego. Así como los Crackers centran su atención en las passwords del softaware mas caro del mercado, los Phreackers tienen como objetivo en esta década, el uso gratuito de los teléfonos. Ya sean estos fijos o móviles.

Cada grupo posee sus propias técnicas. Y cada técnica resulta interesente, pero no menos fácil. De modo que un individuo solo podrá optar por ejercer una de las funciones deseadas. Esto es, no se podrá ser Cracker y Phreacker al mismo tiempo. sin embargo puede existir la posibilidad de que alguien se especialice en varios temas.

El Cracker conoce los ordenadores como una extensión mas de su cerebro. El Phreacker conoce los sistemas multitonos de los teléfonos como si fueran sus propios pulsos cardiacos. Ambos son genios y

ambos desean romper la barrera de lo imposible.

Y el Hacker especializado conoce a fondo los ordenadores, los teléfonos o los descodificadores como si fueran una creación propia. Aquí no hemos definido a una persona que cubre todos los campos. Solo hemos dicho que esta especializado en uno u otro tema. Aunque normalmente un Hacker siempre estará ligado a todo aquello que este relacionado con la tecnología y los códigos.

Cuando un Hacker sacia su red dentro de la red informática, busca nuevas fuentes en el exterior. Normalmente dejan de lado una simple avería del monitor del ordenador, pero no pasan de largo una señal de video que esta invertida en polarización. Esto les atrae. Ver un montón de colores esparramados en la pantalla del televisor despierta su interés. Ademas cuando observa que el amigo posee un descodificador con una tarjeta de acceso inteligente introducido en una ranura del aparato, acrecienta mas su interés por la nueva tecnología.

El buen Hacker se hará de uno de esos descodificadores y lo destripara. Mas adelante se pondrá como reto el poder hacer un clorico del descodificador que funcione de igual forma.

El grado de satisfacción es tal que la adrenalina fluye por sus venas como un chorro de agua ardiendo. Si el individuo sabe parar a tiempo. Se habrá convertido en un autentico Hacker que solo quería saber. No difundirá la información ni hablara de ello.

El hecho de que los Hackers se pasen información a través de la red, no quiere decir que así actúen los Hackers. Los verdaderos Hackers nunca comentan nada de sus trabajos y si lo hacen, suelen utilizar apodos para no ser descubiertos. Si es un principiante, solo deseara recopilar información y lo copiara. Estos individuos se llaman LAMER y son rápidamente expulsados de los heroicos guerreros de la red.

Porque un verdadero Hacker es un fisgón y un curioso con ansias de conocimiento, no un charlatán y un loco. Otro grupo destacado después de estos, son los llamados bucaneros. Estos tipos no saben nada del Hacking, pero se las arreglan para contactar con ellos. Son tipos con bastante dinero en busca de negocio. Ven en los Hackers una fuente de ingresos y se dedican continuamente en ir detrás de ellos. A menudo contratan a los Copy-Hackers, para que les faciliten la faena y ademas estos poseen conocimientos técnicos informáticos o electrónicos. Individuos con conocimientos elevados y habilidad Psiquica. Estos tipos mas acercados a espías, pueden poner en peligro a los Hackers. Son individuos sin escrúpulos y se dedican a cazar a los buenos Hackers para rápidamente, hacerse muy buen amigo de el y prometerle buenas cosas a cambio de información.

Después estos Copy-Hackers ponen en practica todo lo que han podido adivinar y logran poner en marcha el trabajo verdadero del primer Hacker. Cuando lo consiguen ofrecen el sistema y sus servicios a los bucaneros, quienes les pagaran una buena suma de dinero a cambio de lo que quieren. Este proceso es hábilmente seguido en el mundo de la codificación de la televisión vía Satélite. De esta forma pueden moverse por toda Europa en busca de talentos.

Por que un buen Hacker nunca saldrá de su habitación y jamas hablara de su logro.

Después el bucanero comercializara deliberadamente el producto de forma masiva a través de distribuidores. El nunca dará la cara. Y cuando surga un nuevo producto para copiar o desproteger, volverá a las andadas detrás del Hacker.

Sin embargo hay que saber diferenciar bien, quienes son los que realmente producen perdidas enormes en las redes o en las multinacionales. Es cierto que existen Hackers en América que han falseado números

de tarjeta de credito por un valor de 62.500 millones de pesetas solo en el año 1996. Por los que les convierten en Crackers. Y aquí una vez mas existe una controversia. El Hacker necesita mantenerse vivo y una de las maneras de hacerlo es mediante el apoyo economico para crecer en tecnología. Esto les obliga a tomar ***« prestados «*** unos cuantos dolares. Hay que tener en cuenta que Internet no es mas que un conglomerado de empresas, individuos, instituciones y todo tipo de organizaciones, que solo han puesto por el medio una red de comunicación para sus transacciones y mensajes. Esto es parte de un gran caramelo que incita al Hacker a fisgonear y buscar dinero fácil. Todo esto puede estar cifrado, como ya se hace con el correo electrónico. Pero los métodos empleados dejan mucho que desear y estos genios electrónicos o informáticos se las ingenian para descubrir la clave correcta. Para ello existen varias técnicas. Una de ellas es hacer una llamada de telefono y fingir ser otra persona que se ha olvidado la cartera en casa y necesita saber con urgencia ciertos datos. Esta técnica bien empleada durante mucho tiempo ya esta obsoleta. Hoy día nadie es de fiar y ademas ya te piden la clave que estas buscando. Si no esa otra para identificarte correctamente.

Otra técnica es introducir un ***« caballo de troya «*** en un programa. Esto es un comando o instrucción añadida al programa original, que descubrirá la clave cuando el usuario la introduzca en su ordenador, y la facilitara posteriormente cuando el Hacker acceda a su trampa.

De esta forma se pueden acceder a los archivos que se quiera desde una unidad remota. Sin embargo los Hackers encargados de abrir sistemas de codificación de señales de televisión, no lo tienen tan fácil. Aquí la intuición es un factor a tener en cuenta. Si no intuyes lo que realmente pasa detrás de la señal codificada, no sabrás nada.

Estos genios normalmente responden a perfiles de edad mas adulta que los Hackers tradicionales de la informática, que suelen ser adolescentes de familias modestas, en esta ocasión se trata de hombres de mediana edad con muchos años de experiencia en la electrónica y que están hartos de reparar viejos y desvaídos televisores. Sacian primero su sed de curiosidad y ven luego la posibilidad de ganarse un dinero extra con sus conocimientos. A menudo se presentan con su ***« cacharro «*** debajo del brazo en las oficinas de la productora de televisión con la intención de pedir trabajo. Muestra su logro y queda la posibilidad de que sea contratado, ya que todavía no existe ley para penalizar esta acción. sin embargo no siempre sucede así, y son acosados por los Copy-Hackers.

Este es el momento de despedirme, quizas haya quedado bien claro ciertos conceptos de este peculiar universo. Pero también es cierto que hay muchas mas cosas que explicar. La revolución tecnológica a la que estamos asistiendo esta creando nuevos grupos de expertos con otras autodenominaciones. Uno de los últimos grupos que han surgido son los Snickers, expertos en sistemas de codificación y aptos para esta obra. Siempre han estado allí, pero se les ha definido como Hackers hasta ahora y es que todo el mundo te cataloga por igual hagas lo que hagas. Menos mal que entre nosotros las cosas son bien distintas.

Hasta aquí lo dicho y espero que disfrute con el libro

**Stivo**

**California Septiembre 1997**

Estas ha sido, a resumidas cuentas, unas cuantas declaraciones de principios. Ha quedado bien claro el concepto Hacker a través de sus propios ojos, ahora queda seguir investigando y definir correctamente su interpretación, según vayamos avanzando en la lectura de este libro. Y es que el término acuñado por los nuevos genios de la informática, trae cola.

**Claudio Hernández**
**Aguilas Noviembre 1999**

# Capitulo 2

# Internet y su funcionamiento

Imagino, que la mayoría de vosotros sabrá a estas alturas, que es Internet y como funciona, dado que ha sido ampliamente tratado en las diferentes publicaciones del sector. Pero me gusta reincidir a mi modo, quizás por aquello de creer que solo si lo veis desde mi punto de vista comprenderéis todo lo que sigue en adelante.

Mostrare como funciona la gran Red de una forma muy superficial, solo lo Justo como para comprender porque se pueden hacer tantas cosas desde la Red y sobre todo porque existen tantas amenazas que pueden afectar a nuestro ordenador.

Principalmente la red de Internet no nació como tal, si no que su base sólida esta en ARPANET, una pequeña red analógica que conectaba los principales ordenadores de ciertas instituciones, que bajo, unos protocolos de comunicaciones, permitían leer e intercambiar información entre ordenadores remotos.

Después de un tiempo, relativamente corto por supuesto a alguien se le ocurrió inventar el correo electrónico y mas adelante las siglas W.W.W y ciertos protocolos que dejaban a un lado los sistemas operativos unix , para dejar paso a toda una legión de ordenadores dominados por sistemas operativos Windows capaces de navegar por la Red, ya extendida como una extensa telaraña.

Pero a ciertos " personajes " no se le escapo detalle de esta nueva forma de comunicación electrónica y ampliando conocimientos, descubrieron que se podía hacer mas cosas que visitar una pagina WEB.

Ahora Internet es un conglomerado de nodos de conexión y códigos viajando de un lugar a otro hasta saturar el ancho de banda de cada servidor. Son ya muchos los internautas que se han sumado a la Red y pocos, los que conocen quienes están detrás de ella y que hay, hay fuera.

## 2.1 Internet en detalles

La idea básica, estriba en que mas de dos ordenadores puedan mantener una comunicación entre ellos. Para ello, además de los citados ordenadores hace falta un soporte físico para enviar la información. En la actualidad Internet se apoya en el par telefónico o hilo extendido, dado que las compañías telefónicas son

las únicas que poseen nodos o conexiones a nivel mundial.

Actualmente existen una serie de proyectos vía satélite que sustituyen el cable de forma elegante, ya que integran mayor seguridad en las comunicaciones y sobre todo, velocidad.

Pero el soporte físico no lo es todo, para que dos o mas ordenadores puedan comunicarse o " entenderse " entre si hace falta un lenguaje o un protocolo de comunicación que siga unas pautas en el envío y recibo de datos. Este protocolo de comunicaciones, denominado TCP/IP " el mas extendido entiéndase " permite que todos los ordenadores del mundo mantengan comunicaciones y se " entiendan " entre si.

Por otro lado es de suponer que el cable que sale de tu casa no va directamente con estados unidos o Francia, por ello el servicio de conmutaciones a estas zonas geográficas las permiten hacer los servidores. Esto es, grandes CPU al servicio de una cartera de clientes a los cuales se les sirven direcciones electrónicas para correo o un espacio para nuestra WEB, además de los servicios FTP o CHAT por ejemplo.

Después de los servidores, están los nodos de conexión o enrutadores que facilitan los "saltos " a efectuar hasta llegar a destino. Estos enrutadores son sistemas que guían nuestros datos hacia una dirección predeterminada. Como sucede con los números de teléfono, por ejemplo cada pagina WEB tiene una asignación numérica como dirección electrónica.

Para alcanzar cada dirección, un robot se encarga de rastrear los nodos de conexión necesarios hasta llegar al destino. Este destino es una dirección IP y Host nuestro servidor que actúa de " operador ".

Las paginas son procesadas, esto es, leídas, gracias a un navegador instalado en nuestro ordenador. Un navegador es un programa capaz de marcar la dirección IP, capaz de soportar el protocolo TCP/IP y un programa capaz de interpretar las respuestas del lugar IP.

Entre estas respuestas, se encuentran textos y gráficos estáticos o animados, como JPEG y GIF89 respectivamente.

El navegador puede a su vez guardar cada parte de esta pagina descargada, modificarla o procesarla. También se soportan en la red trasvases FTP, esto es, envío y recibo de ficheros bajo programas específicos.

## 2.2 Conectando...

Para que un ordenador se conecte a la Red, se precisan de una serie de elementos esenciales, que sin ellos nada se podría hacer. En principio el ordenador debe tener instalado un módem o una tarjeta de comunicaciones interna y después un navegador para acceder a las paginas WEB. Lo mismo que se requiere de un gestionador de correo electrónico para el mismo.

Después de todo este software, existe un Hardware especifico que completa la instalación, siendo lo mas común un módem para trabajar con la Red externa y unas tarjetas de Red para interconexiones internas, estas conexiones " o redes privadas " se denominan redes LAN.

Cuando se realiza la conexión normalmente esto se hace introduciendo en primer lugar nuestra contraseña y nombre de usuario. Estos dos datos deben comprobarse debidamente por nuestro servidor, para validar nuestra conexión y acceso. Por un lado por motivos de " control " de la propia conexión a la red

telefónica, por otro, para dar vía libre al internauta registrado en el propio servidor, lo que le da derecho a otras operaciones mas que la simple navegación por Internet.

Tras introducir estos datos se pulsa OK, tras esto el ordenador chequea el módem emitiendo un código, tras el cual el módem devuelve una respuesta, no sin antes comprobar, este, si existe línea libre.

El protocolo TCP/IP se encarga del resto, en el caso para acceder a una pagina WEB, primero es necesario abrir el navegador, programa que chequeara si el módem esta listo antes de activarse. Si esto es así, normalmente el navegador marcara una dirección predeterminada en formato numérico como por ejemplo 195.456.456.908. si la dirección es localizada el Host, enviara un código de respuesta a nuestro ordenador y este nos indicara WEB ENCONTRADA, tras esto se prevé la descarga de la pagina.

Cuando esto sucede, además de los textos y gráficos de la pagina, existen unos cookies, esto es, microprogramas que permiten identificar la visita y albergar otras instrucciones en la WEB visitada y en nuestro ordenador. " Estos cookies a veces son la cuna de los Virus o los caballos de Troya " por lo que a menudo son eliminados del sistema, como medida de seguridad.

Tras esta simple explicación, supongo que habrá adivinado que el protocolo de comunicaciones TCP/IP se basa en una comunicación bidireccional, solo de esta forma se pueden sincronizar dos ordenadores remotos.

Para que cualquier equipo pueda ser interactivo con otro es necesario que la comunicación sea bidireccional con peticiones y respuestas que sincronizaran los paquetes de datos recibidos. Por cada paquete de datos recibido de una extensión determinada, se envía un OK y se prosigue la descarga.

Los datos viajan así, de una lado a otro con cierta facilidad.

## 2.3 Algo mas que navegar

Si los datos pueden viajar de una lado a otro de forma ordenada y permitir descargas de " datos " a cualquier ordenador por medio de una previa petición de otro ordenador. También es posible mantener otro tipo de relaciones entre ordenadores, entre ellos el intercambio de ficheros del disco duro.

Esto se consigue mediante FTP, que entre otras cosas no es mas que un estándar de comunicaciones, mas perfeccionado quizás, que permite " leer " el disco duro de otro ordenador remoto y bajarse algo o todo de el, por supuesto con previa autorización.

Por otro lado, con FTP podemos también enviar cualquier fichero de nuestro disco duro hacia otro disco duro remoto. Y es aquí donde pueden surgir " las puertas oscuras " de un sistema, ya que a través de ellas se obtienen penetraciones al sistema y paswords de acceso.

POP3, las siglas mas comunes del correo electrónico, es algo mas de lo mismo. Son protocolos estandarizados que permiten realizar envíos y recepciones de datos de un formato u otro.

## 2.4 Entre tanto cable

Entre cable y cable los datos podrían perderse, pero esto no sucede gracias a nodos de conexión y estaciones BBS intermedias " que en realidad monitorizan todo lo que se cuece en la red y se almacena en memorias temporales " estos pasos intermedios, procuran guiar cada paquete hacia y a donde , su destino sin cometer errores.

Por otro lado las estaciones BBS, " filtran " la información " mala " para la Red. Los nodos de conexión encaminan los datos y los enrutadores los distribuyen, pero en realidad todo esta complementado por otros " sistemas " que controlan todo lo que circula en la Red, como los sniffers y en el peor de los casos vienen las grandes caídas del ancho de banda por culpa de algún " Worm ".

De estas cosas hablaremos mas adelante.

# Capitulo 3

# Seguridad en Internet

Hablar de seguridad en Internet es como hablar de si nuestro coche esta seguro en la calle con las llaves puestas en la cerradura. Evidentemente no. Por ello, podemos decir encarecidamente que no existe ningún tipo de seguridad en la gran red de redes. Esto es debido a que quizás, o bien pensaron en una estructura simple " cuando se creo Arpanet " o que quizás hay demasiado listillo suelto por hay.

De cualquier forma, Internet es un lugar donde puedes hacer de todo y paralelamente recibir de todo. Desde descargar un programa de evaluación con éxito a " cogerte " un virus que con un poco de suerte, te dejara fuera de combate por un tiempo.

También es cierto que internet ha sabido coger muy buena fama para recibir todo tipo de amenazas para tu ordenador, pero no siempre es así, si no te metes con ellos…

## 3.1 Quienes son ellos ?

Ellos en un principio son muchos y muy variados. Son los nuevos personajes de una nueva sociedad underground o ciberdelincuentes en la mayoría de los casos. Pero es evidente que no podemos echarle la culpa a todos, de lo que pasa en la red.

En Internet existen, principalmente internautas que se pasan largas horas delante del ordenador buscando atractivas imágenes de mujeres desnudas, otros simplemente buscan algún tiempo de información para terminar un trabajo, otros buscan la sinopsis de la ultima película de Spielberg, pero una pequeña minoría se pasa largas horas entrando en sistemas con el fin de lograr sus objetivos basados en satisfacciones personales. Entrar en un lugar supuestamente " seguro ", los que lo consiguen simplemente se sazonan de alegría, una diminuta minoría se queda en el lugar y fastidia todo lo que ve a su paso.

Dentro de esta galería de personajes podemos nombrar a los sencillos internautas, los Hackers, Crackers o los Lamers entre una devastadora familia de intelectuales expertos en temas informaticos. Hablaremos de cada uno de ellos, con detenimiento en el próximo capitulo de este libro y ahora nos centraremos a los peligros que obran en Internet.

## 3.2 Pesadilla en la ReD

Podemos enumerar una gran lista de amenazas que pondrían los pelos de punta a mas de uno, pero no se trata de eso. Mi obligación como escritor es informar y dar detalles de las diferentes amenazas que han surgido en la Red en los últimos años, no sin ello desalentar al futuro o actual internauta a engancharse a la red.

Todo lo que quiero explicar es, para que el internauta adquiera la conciencia de la existencia de ciertos peligros y los suficientes conocimientos, como para estar preparado frente a lo que se puede encontrar y donde encontrarlos. Es algo así, como formar un experto a distancia, para prever que le fastidien su ordenador o recibir una sorpresa, que lo único que aporta es un buen cabreo.

En Internet es posible navegar a través de paginas WEB denominadas World wide Web. Otra opción es la del correo electrónico, el cual nos facilita la comunicación entres las personas a través de texto, pero las ultimas tendencias permiten enviar vídeo además de texto, así como audio, por lo que las comunicaciones a través de internet nos ofrecen claras ventajas a los tradicionales métodos de comunicación como el teléfono, por ejemplo.

Otro de los objetivos de internet " el principal " es que cualquier ordenador también pueda conectarse o comunicarse con otro cualquiera desde cualquier punto del planeta. Por ello en un principio, ese era el principio de la idea imponible y como los ordenadores conectados en red " en aquel momento " eran principalmente los de las principales instituciones de estudios e investigación, se tomo pocas precauciones de seguridad, salvo los pasword de acceso.

El problema vino después, cuando la red de Arpanet se convirtió en una red mas grande llamada Internet, que permitía el acceso a cualquier internauta para consultar unas simples paginas de una sede. Después llegaron otras opciones, como correo electrónico, y servicios FTP entre otras. Pero estos servicios no fueron la causa del nacimiento de los primeros Hackers o sociedad ciberpunk.

El problema vino después, cuando a alguien se le " escapo " literalmente un programa a través de la red, que poseía la opción de autoreplicado de si mismo. El cual causo un embotellamiento de las comunicaciones de esta red, ya que el programa se autoreplicaba con tal velocidad que colapsaba las comunicaciones como si miles de nuevos internautas se sumaran a la red al mismo tiempo.

Para eliminar el problema, hubo de crearse otro programa que contrarrestara las funciones de dicho programa autoreplicante. A este incidente se le denomino " gusano " y a la solución al problema " vacuna ".

Así nació el primer virus y el primer antivirus.

## 3.3 Los virus informaticos

Los virus son la principal amenaza en la Red. Estos programas de extensión relativamente pequeña, son

programas capaces de autoreplicarse o dicho de otra manera, son capaces de hacer copias de si mismo en otro archivo al que ocupa. Este método bloquea y llena el disco duro de un PC.

Otros virus además poseen funciones de modificaciones en los principales ficheros del sistema operativo de nuestro ordenador. Pero los hay también benignos que solo muestran mensajes en la pantalla. Nos detendremos a estudiar los diferentes tipos de virus y analizaremos algunos de ellos, como los a tener en cuenta.

Los virus poseen unas particularidades que los hacen perfectamente reconocibles por la forma en que trabajan, los virus poseen un proceso de creación, incubación y reproducción.

## 3.4 La vida de un virus

El virus se crea o nace, esta claro en el ordenador del creador como subprograma o microprograma ejecutable. Después este se " suelta " en la red o se copia " inserta " dentro de un programa comercial de gran difusión, para asegurar un contagio rápido y masivo.

Después de esta primera fase de creación, vienen las mas importantes a cumplir de forma automática e independiente del control de creador del virus, " principalmente creado por un enfadado empleado recientemente despedido de la empresa en la que trabajaba y que guardaba esta carta bajo la manga " este proceso consta de contagio, incubación, replicacion y ataque.

## 3.5 el contagio

El contagio es quizás la fase mas fácil de todo este arduo proceso. Solo hay que tener en cuenta que el virus debe introducirse o " soltarse " en la red. El virus debe ir incrustado en un archivo de instalación o en una simple pagina WEB a través de los cookies.

Las vías de infección son también principalmente los disquetes, programas copiados, Internet o el propio correo electrónico.

## 3.6 La incuvacion

Normalmente los virus se crean de formas especificas que atienden a una serie de instrucciones programadas como el " esconderse " y " reproducirse " mientras se cumplen unas determinadas opciones predeterminadas por el creador del virus.

Así, el virus permanece escondido reproduciéndose en espera de activarse cuando se cumplan las condiciones determinadas por el creador. Este proceso puede ser muy rápido en algunos casos y bastante largo en otros, según el tipo de virus.

## 3.7 La replicacion

La replicacion consiste en la producción del propio virus de una copia de si mismo, que se situara en otro archivo distinto al que ocupa. De esta forma el virus se contagia en otros archivos y otros programas, asegurándose de que el proceso de multiplicación esta asegurado.

Además, el virus asegura su extensión a otros ordenadores y debe hacerlo de la forma mas discreta y rápida posible. En este momento el virus no se manifiesta, ya que solo se instala en cuantos mas lugares mejor.

Solo de esta forma, mas posibilidades tendrá de dañar un mayor numero de ordenadores.

## 3.8 El ataque

Cuando se cumplen las condiciones, efectuadas por el creador del virus, este entra en actividad destructora. Aquí es donde formatea el disco duro o borra archivos con extensión COM o EXE por citar algunos ejemplos.

El ataque es el escalón final del trabajo del virus. Cuando se llega a este punto el trabajo ha culminado. El ordenador se encuentra infectado y si no se dispone de un programa que elimine el virus, jamas se podrá recuperar los archivos. Podemos instalar de nuevo el software, pero de nuevo tendremos la destrucción de nuestra unidad nada mas se cumplan los acontecimientos antes citados.

Estos programas capaces de destruir el virus, se denominan vacunas antivirus.

## 3.9 Pero, son todos lo virus iguales

Indudablemente no.

Estamos ante unos programas bastantes inteligentes y obviamente creados por diversas personas con ideas y fines distintos. Los virus, son denominados así, para conocimiento común, pero no todos ellos reciben este nombre. Entre la extensa familia de virus que existen con diferentes manifestaciones, hay que destacar otra extensa galería de subprogramas inteligentes que pueden actuar como virus con fines diferentes al de fastidiar únicamente el disco duro del ordenador.

Por ejemplo tenemos programas que únicamente se encargan de robar los pasword de nuestro ordenador, otros simplemente llenan el disco duro y otros tantos se dedican a mostrarnos multitud de publicidad en nuestro correo electrónico hasta saturarlo. Todos ellos serán mencionados en este libro y trataremos de explicar que son y que hacen cada uno de ellos.

Entonces entra la sugestiva pregunta de si todo lo que se sale de lo normal en la red son virus, como

respuesta diremos que no, ya que además de estos virus, podemos citar los Caballos de Troya, las bombas lógicas o los Spam por ejemplo.

## 3.10 Los caballos de Troya

Son programas que normalmente ocupan poco espacio y se " cuelan " a voluntad en el interior de un ejecutable. Este subprograma se coloca en un lugar seguro de la maquina para no ser detectado y no modifica nada de los archivos comunes del ordenador y cuando se cumplen unas especificaciones determinadas el subprograma muestra unos mensajes que sugieren o piden la contraseña al usuario de la maquina.

En otros casos simplemente lee el pasword cuando nos conectamos a la red, tras copiar el pasword, este se encripta y se envía por correo electrónico adjunto. El Hacker lo que debe de hacer ahora es " capturar " ese mensaje y descifrar su propio código.

El mensaje es fácilmente capturado, mediante un sniffer, esto es, un programa de monitorizado de la red, pero los mas expertos emplean caballos de Troya mas inteligentes, que lo que hacen es reenviar o " desviar " el mensaje a una dirección del Hacker sin que el usuario se de cuenta.

## 3.11 Las bombas logicas

Son una de las buenas bazas del Cracker " malicioso " al igual que un virus las bombas lógicas están especialmente diseñadas para hacer daño. Existen dos definiciones del mismo acronimo o programa asociado. Una es la de crear un subprograma que se active después de un tiempo llenando la memoria del ordenador y otra es la de colapsar nuestro correo electrónico.

De cualquier forma ambas son dañinas, pero actúan de forma diferente. En la primera referencia, este se instala en nuestro ordenador después de ser bajado junto a un mensaje de E-Mail. Se incuba sin crear ninguna copia de si mismo a la espera de reunir las condiciones oportunas, tras ese periodo de espera el programa se activa y se autoreplica como un virus hasta dañar nuestro sistema. En el caso segundo, alguien nos envía una bomba lógica por E-Mail que no es sino que un mismo mensaje enviado miles de veces hasta colapsar nuestra maquina. Los programas antivirus no están preparados para detectar estos tipos de bombas lógicas, pero existen programas que pueden filtrar la información repetida. De modo que la única opción de fastidiar es hacer " colar " una bomba lógica que se active frente a determinadas circunstancias externas.

## 3.12 Los gusano " Worm "

Son programas que tienen como única misión la de colapsar cualquier sistema, ya que son programas

que se copian en archivos distintos en cadena hasta crear miles de replicas de si mismo. Así un “ gusano “ de 866 Kbyts, puede convertirse en una cadena de ficheros de miles de Megas, que a su vez puede destruir información, ya que sustituye estados lógicos por otros no idénticos.

Los gusanos o “ Worms “ suelen habitar en la red a veces como respuesta de grupos de “ Hackers “ que pretenden obtener algo. La existencia de uno de estos gusanos se hace notar, cuando la red se ralentiza considerablemente, ya que normalmente el proceso de autoreplicado llena normalmente el ancho de banda de trabajo de un servidor en particular.

## 3.13 Los Spam

No se trata de un código dañino, pero si bastante molestoso. Se trata de un simple programa que ejecuta una orden repetidas veces. Normalmente en correo electrónico. Así un mensaje puede ser enviado varias cientos de veces a una misma dirección.

En cualquier caso existen programas, antispam, ya que los spam son empleados normalmente por empresas de publicidad directa.

## 3.14 Volviendo a los virus informaticos

Internet aporta, lo que se podría decir una vía rápida de infección de este tipo de programas dañinos. Antes, la distribución o infección de los virus, era algo mas que una tarea lenta y ardua, ya que solo se contagiaban a través de disquetes. Por ello, la Red bien podría llamarse el gran nido.

Después de explicar las distintas fases, desde la creación de un virus, tenemos que enumerar al menos que distintos tipos de Virus coexisten actualmente en la Red. No sin antes dejar comentado, que tal como están puestas las cosas hoy por hoy, surgen cada dia unos 100 nuevos “ bichos “ en la red. De seguir así, para el año 2.000 podríamos tener unos diez millones de estos “ bichos “ en la Red dispuestos a destrozar nuestro disco duro.

A esto hay que añadir la metamorfosis de los nuevos virus cada vez mas inteligentes y a las tres vías de propagación mas ampliamente conocidas, como son por un attach de correo electrónico, un trasvase FTP o un dowload desde una pagina WEB.

Con todas estas circunstancias, podríamos atrevernos a decir que la red estará gobernada por millones de formas capaces de bloquear cualquier sistema, dado además, por los varios tipos de virus que existen.

## 3.15 Tipos de Virus

Existen al menos cinco tipos de Virus conocidos hasta ahora, esto no quiere decir que están todos, seguramente mientras escribo estas líneas habrá surgido algún que otro engendro mas sofisticado. Pero

básicamente son estos :

*** Virus de arranque o Virus de Boot.**

*** Virus de Macro.**

*** Virus de ficheros.**

*** Virus polimorficos.**

*** Virus multiparte.**

A la presente lista podemos añadir los Virus Hoaxes que no son realmente lo que representan ser, hablaremos mas adelante de ellos.

Los Virus de boot o de arranque eran hasta los 90 los típicos virus que infectaban el sector de arranque del disco y estos eran introducidos al ordenador a través de disquetes. El modo de funcionamiento es básico, al arrancar la computadora, el virus se instalaba en la memoria RAM antes que los ficheros del sistema INI, de esta forma podían " fastidiar " a su antojo lo que querían.
Para no ser detectados, estos virus de Boot, se copiaban a si mismos en otro lugar del disco duro, con el fin de no ser descubiertos.

Los virus de Macro están mas elaborados y son virus escritos a partir del macrolenguaje de una aplicación determinada. Por ejemplo podemos citar el Word, procesador de textos. Estos virus, son realmente dañinos, porque son capaces de borrar un texto, dado que los bloques macro son diminutos programas del propio Word, por ejemplo, que permite ejecutar varias funciones seguidas o a la vez con solo activar la casilla.
Por ello un Macro programado con la instrucción deshacer o borrar, resultara " hermosamente " dañino. Otros sin embargo, podrán resultar inofensivos, dado que son programados con funciones de copiar y pegar por ejemplo, no perdemos datos, pero si resulta algo bastante molesto.
En el caso de Acces, esto se complica, ya que este programa permite además de códigos Macro, programar Scripts. Los scripts son invocados según unas determinadas funciones, por ejemplo la tecla A pulsada tres veces ocasiona la ejecución de un Macro.
Por otro lado, eliminar los virus o scripts malintencionados puede resultar una tarea bastante compleja, ya que reemplazar o desactivar no solo los comandos Macros si no también los scripts, puede causar que algunas funciones básicas del programa dejen de funcionar.

Los Virus de Fichero son conocidos también como " parásitos " y suelen operar desde la memoria tras haber tomado control de los ficheros o archivos ejecutables, como las extensiones COM ,EXE, DLL o SYS.
Se activan solo cuando se ejecuta algunos de estos ficheros, permanecen ocultos y estallan después de unas determinadas funciones programadas.

Los virus polimorficos son aquellos que son capaces de cambiar de estado o la propia cadena de datos. De esta forma el mismo Virus puede verse dividido en varias secciones repartidas en varios ficheros, pero a causas naturales actúa como tal. Estos Virus son difícilmente localizables y solo en excepciones, los método heurísticos podrían detectarlos en el caso de que algún fichero crezca demasiado de tamaño.

Estos virus pueden estar encriptados y muy bien repartidos por decenas de ficheros, con lo cual se convierten en los virus mas peligrosos, dado que pueden ser programas largos.

Los virus multiparte, están conformados a base de Virus tipo boot que operan desde la memoria y virus de Fichero, que infectan extensiones ejecutables. Estos Virus también pueden burlar los modernos métodos heurísticos de búsqueda de los programas de antivirus.

## 3.16 Otras amenazas

Dejando a un lado los temibles Virus y los caballos de Troya, existen otras amenazas en la red prediseñados para monitorizar el trasvase de datos en la línea y de hay tomar prestados algunos paswords o números de tarjeta de crédito.

Estos programas capaces de monitorizar a alguien en particular o todo aquello que se mueve en la red, recibe el nombre de sniffer y como su nombre indica, son programas capaces de interpretar todos los datos de la red, copiarlos y modificarlos.

Otras amenazas son los buscadores de puertos libres IRQ, con estos programas se pueden localizar puertos libres o abiertos y entrar por ellos a otros sistemas. A veces estos puertos contienen Bugs, “ fallos “ y los Hackers las emplean para penetrar en los sistemas.

# Capitulo 4

# La nueva Cibersociedad

Quizás con el transcurso del tiempo los hombres o mujeres que indagaban en otros sistemas, sean físicos o no, han pasado de denominarse espías a Hackers. Pero en realidad esta definicion no converge demasiado. En realidad no es bueno confundirlos. Sin embargo si hay que aceptar que algo tienen de parecido los espías y los Hackers, y es la ingeniería social y la tecnología empleada por cada uno de ellos, para descubrir lo que quieren.

Un buen espía se hará pasar por alguien en quien confiar, un buen Hacker convencerá a otra persona para que le de el numero del modem. Esto es ingeniería social. Kevin Mintnik era un buen ingeniero social. Sabía arreglárselas para que la gente confiara y creyera en el.

Después esta la tecnología, los espías emplean sofisticadas maquinas para introducirse en sistemas remotos, o potentisimos radioescuchas para detectar las conversaciones deseadas. El Hacker también se rodea de estos equipos, y en cierta forma emplea los mismos métodos que el espía.

Por otro lado tenemos que espías y Hackers tienen demasiada similitud, porque en ambos bandos existen defraudadores. Esto es, personas que finjen ser lo que realmente no son o no son capaces de ser. Por esta razón hay veces en que armas tan poderosas en manos tan débiles, puede tirar abajo todo un arduo trabajo.

Pero en la nueva cibersociedad de hoy, la gente es joven y tiene ganas de divertirse y parece que esto es lo que menos importa. Por ello, quizas, han surgido tantos acrónimos o derivados del verdadero Hacker. Esta nueva cibersociedad esta corrompiendo lo que hasta ahora era un arte. Un conocimiento superior y un control absoluto.

En la actualidad, ni la prensa, ni los que están en la nueva era ciberpunk saben exactamente quienes son cada uno de ellos.

Pero no obstante, tampoco es muy difícil adivinar quien es el impostor o el malo en esta nueva urbe de cerebros desbocados. Vamos a dar un repaso al verdadero perfil del Hacker y de paso descubriremos, que mutaciones han surgido en los últimos años.

## 4.1 El perfil del Hacker

Un perfil idóneo prácticamente no existe, pero si un acercamiento. El Hacker es alguien compulsivo y obsesivo por acumular conocimientos. Es extrovertido e investiga todo lo relacionado con la electrónica y la informática. Es el tipo de personas que suelen abrir todos los aparatos de consumo de casa o lee los ficheros de su ordenador hasta modificarlos para ver que sucede.

Un buen Hacker prueba y modifica las cosas que tiene entre sus manos y se pasa largas horas pensando en ello. Existen dos tipos de Hackers, los Hackers en si y los Hardware Hackers. El primero de ellos practica con los ordenadores, el segundo con la electrónica.

Pero ambos conocen bastante ambos extremos, ya que le son útiles tener conocimientos electrónicos e informáticos.

Un Hacker no es el tipico personaje con gafas y pelo engominado o graso. Ni es un tipo delgado con la cara cubierta de granos. Tampoco es un despistado ni muestra una calavera en la parte posterior de la camisa.

Un Hacker no conduce un civik sacando el dedo corazón a la gente, ni es el tipico consumidor de coca-cola y pizzas. Es posible que le guste algo de todo esto, como es posible que lleve gafas de monturas de hueso perfectamente ajustadas, pero no tiene que ser así de serie.

Hacker es quien se interesa por la tecnología, sea delgado o no, alguien que posee ansias de tener conocimientos sobre algo, al margen de si lleva vaqueros o si va en calzoncillos. El Hacker, es alguien normal, con sus miedos y sus dudas, pero que posee una fuerte voluntad para pasarse horas delante del ordenador probando cosas. Le encanta descubrir como funcionan los programas o por lo menos para que sirve cada cosa.

Cuando ha adquirido bastantes conocimientos, el Hacker es capaz de desproteger un programa o copiar una tarjeta electrónica. Y hay esta la confusión. Un buen Hacker se apunta lo aprendido y no lo difunde con una sonrisa de oreja a oreja, como un idiota. Se calla. Es mejor para poder proseguir.

Si es cierto que al Hacker, le entusiasma todo lo que rodea la tecnología, la telefonía celular, los ordenadores, las tarjetas de credito electrónicas o los Satélites. Normalmente lee demasiadas revistas y estudia pesados libros de técnica.

El Hacker, es entonces una persona normal, con amplios conocimientos acumulados a fuerza de " puro huevo " y que normalmente suele sorprender con su forma de ver la vida. Pero ahora es cuando nace la nueva sociedad underground**.**

## 4.2 Los Crackers

En realidad son Hackers, pero con unas intenciones que van mas allá de experimentar en casa. Por cualquier motivo su Crack puede extenderse como la pólvora.

Un Cracker se dedica unica y exclusivamente a " reventar " sistemas, ya sean estos electrónicos o

informáticos. Alcanza el éxtasis de satisfacción cuando logra “ reventar “ un sistema y esto se convierte en una obsesiva compulsión. Nunca tiene bastante y aprovecha la oportunidad para demostrar al mundo que sabe mas que nadie.

Y esto no es malo, porque cada cual puede tener los conocimientos suficientes como para quebrantar cualquier sistema protegido. Pero no difundirlo. Pero algunos Crackers si lo hacen, se mofan difundiendo su logro o en cualquier caso ofrece por Internet su ultimo programa capaz de reventar los programas Shareware.

Por esa razón se les denomina Crackers, ya que quebrantan los sistemas de seguridad y la filosofía del propio Hacker.

## 4.3 Los gurus

Son los maestros y enseñan a los futuros Hackers. Normalmente se trata se personas adultas, me refiero adultas , porque la mayoría de Hackers son personas jóvenes, que tienen amplia experiencia sobre los sistemas informáticos o electrónicos y están de alguna forma hay, para enseñar a o sacar de cualquier duda al joven iniciatico al tema.

Es como una especie de profesor que tiene a sus espaldas unas cuantas medallitas que lo identifican como el mejor de su serie. El guru no esta activo, pero absorve conocimientos ya que sigue practicando, pero para conocimientos propios y solo enseña las técnicas mas basicas.

## 4.4 Los lamers

Estos si que son peligrosos, no saben nada y creen tener el mundo en sus manos. Si cae en sus manos un programa generador de Virus, este, lo suelta en la red y muestra una sonrisa estúpida al tiempo que dice. ¿ Has visto de lo que soy capaz de hacer ?. En realidad resulta patético.

Un lamer rastrea en la basura cibernética de la red, se baja todos los programas y los prueba todos. Es el tipico tipo que se pasa la vida “ jodiendo “ a los demás, enviando bombas lógicas o Virus por la Red, y lo peor de todo es que se cree saber algo.

Hoy día cualquier persona es capaz de manejar un programa determinado con pocas enseñanzas de informática. Después de diez minutos sabe que si pincha sobre el icono deseado el programa se ejecutara. Esto es lo que hace el lamer, ejecutar programas creados por otros.

Después se cree un todopoderoso, pero en realidad no vale nada.

## 4.5 Los copyhackers

Son otra nueva generación de falsificadores. Obtienen lo que les interesa y se lo venden a alguien sin

escrúpulos que comercializara el sistema posteriormente. Estas personas quieren vivir del cuento y son personas obsesivas que mas que ingeniería social, poseen obsesión compulsiva.

Suelen leer todo lo que hay en la Red y las revistas técnicas en busca de alguien que sabe algo. Después se pone en contacto con ella y trata de sacarle la idea. Cuando lo consigue, no tiene escrúpulos en copiarlo, llevarlo a cabo y vendérselo al bucanero.

## 4.6 Los bucaneros

En realidad se trata de comerciantes. Los bucaneros venden los productos crackeados como tarjetas de control de acceso de canales de pago. Por ello, los bucaneros no existen en la Red. Solo se dedican a explotar este tipo de tarjetas para canales de pago que los Hardware Crackers, crean.

Los bucaneros suelen ser personas sin ningún tipo de conocimientos ni de electrónica ni de informática, pero si de negocios. El bucanero compra al CopyHacker y revende el producto bajo un nombre comercial.

En realidad es un empresario con mucha afección a ganar dinero rápido y de forma sucia.

## 4.7 El Newbie

Traducción literal de novato. Es alguien que empieza a partir de una WEB basada en Hacking. Inicialmente es un novato, no hace nada y aprende lentamente. 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 pagina WEB para seguir las instrucciones de nuevo.

Es el tipico tipo, simple y nada peligroso. Esta apartado en un rincón y no es considerado.

## 4.8 El Wannaber

Es el tipo que quiere ser Hacker, pero su “ sesera “ no da para mucho. No consigue aprender nada y se exprime al máximo. Y al final nunca logra nada, sin embargo, posee paciencia y actitud positiva. De lo contrario se sumergiría en una grave depresión.

Un caso olvidado.

## 4.9 Piratas informáticos

A menudo confundidos con Hackers, los piratas informáticos son aquellos que simplemente pinchan sobre el icono copiar disco. El programa y la grabadora hacen el resto del trabajo.

Una vez copiado el programa lo vende. Este es quizas el mas peligroso de todos en cuanto a derechos de copyright, ya que estafa y crea copias ilegales de soportes audiovisuales.

## 4.10 Phreakers

Son tipos con unos conocimientos de telefonía insuperables. Conocen a fondo los sistemas telefonicos incluso mas que los propios técnicos de las compañías telefónicas.

Estos tipos han sabido crear todo tipo de cajas de colores con una función determinada. Por ejemplo la caja azul permite realizar llamadas gratuitas, ya que emula el tono de 2600 Hz para desactivar el contador de la centralita.

Actualmente se preocupan mas de las tarjetas prepago, que de estas cajas, ya que suelen operar desde cabinas telefónicas o móviles. Un sistema de retos, es capaz de captar los números de abonado en el aire. De esta forma es posible crear clones de tarjetas telefónicas a distancia.

## 4.11 El Underground final

Se ha descrito brevemente cada grupo y supongo que habrá quedado claro quienes son cada uno de ellos y que papel interpretan en la nueva cibersociedad.

Son cada vez mas los jóvenes que se autodenominan Hackers y lo unico que hacen es soltar Virus y probar programas de Hacking. Esto confunde a la sociedad y este tipo de personas si son algo violentas y abolecen lo material. Disfrutan " jodiendo " al vecino y muestra una cara de idiota brillando bajo la luz de la bombilla, cuando suelta uno de esos fatídicos Virus o gusanos en la Red.

Los buenos Hackers, no son nunca descubiertos y apenas aparecen en la prensa, a menos que sean descubiertos por una penetración en un sistema demasiado seguro. Entonces la han fastidiado.

Pero volviendo a la consideración de si son una nueva sociedad difícil de comprender, debo decir que así es, y también debo aceptar, al igual que todos vosotros que el verdadero Hacker posee el control del mundo.

Por ello alguien muy importante en los Estados Unidos dijo alguna vez, dadme diez Hackers y dominare el mundo.

# Capitulo 5
# 32 preguntas y respuestas sobre Hackers

Es difícil catalogar lo que a continuación va a leer, no por su contenido, ya que es obvio que voy a tratar sobre el tema del Hacking, sus conceptos y sus atributos, como he venido haciendo desde el principio de este libro. La diferencia de este capitulo con el resto de los capítulos del libro, es que no sigue un orden cronológico y ni mucho menos aporta nada nuevo al tema. Sin embargo se hace inevitable el reincidir de nuevo aquí, en el concepto Hacker y los clanes de la ReD.

Publicado inicialmente como un articulo para una revista de prestigio de tirada nacional, he querido incluir aquí el borrador de lo que fue, finalmente el articulo. Con esto quiero decir que en las siguientes lineas, se escribe o mejor dicho, encontrara mas datos de los que realmente apareció en la publicación de dicho articulo.

Así, y justificándome una vez mas, he de decir que reincidiendo en el concepto anteriormente tratado en el capitulo anterior, tiene aquí de nuevo un nuevo escrito que de una vez por todas despejara todas sus dudas sobre los Hackers. Así y valga la redundancia, tiene en adelante a su disposición la trascripción de uno de los mejores artículos de Hackers publicado hasta ahora.

## 5.1 Trascripción del borrador del articulo completo

### HACKERS, LA NUEVA GENERACIÓN

**CRÓNICA DE UN HACKER ANUNCIADO EN 32 PREGUNTAS Y RESPUESTAS**

**MITIFICADOS POR UNOS Y ODIADOS POR OTROS, LA NUEVA GENERACIÓN DE HACKERS PARECE DISPUESTA A DOMINAR LA TECNOLOGÍA ACTUAL Y FUTURA. PERO TAMBIÉN ES CIERTO QUE EXISTE MUCHA CONFUSIÓN SOBRE ELLOS. DESDE AQUÍ EXPLORAREMOS SU MUNDO Y QUIENES SON EN REALIDAD. HACKER, DE HACK, SIEMPRE SE REFIRIÓ A ELLOS COMO EL TÉCNICO DE TELÉFONOS QUE ARREGLABA ESTOS APARATOS ASESTÁNDOLES UN GOLPE SECO. OTRO BANDO DE ESCRITORES DENOMINA LOS PRIMEROS HACKERS A UN PEQUEÑO GRUPO**

**DE ESTUDIANTES DEL MIT QUE HACE UNA VEINTENA DE AÑOS PROTAGONIZARON UNA SERIE DE INCURSIONES A UN GRAN ORDENADOR, PERO CUAL ES EL VERDADERO PERFIL DEL HACKER ?. POR OTRO LADO, CONTAREMOS EN UN SEGUNDO BLOQUE, UN RELATO CRUDO QUE DESCRIBA LO QUE MAS DESEAMOS SABER TODOS, LA CRÓNICA DE UN « HACKER « EN UN DÍA CUALQUIERA.**

La prensa esta plagada de espectaculares noticias sobre estos individuos y otros que a menudo son confundidos con ellos. Nos estamos refiriendo a las grandes columnas que narran los hechos de un grupo de estudiantes que ha extendido una red de difusión de copias de programas informáticos. A estos individuos se les denominan de forma acertada, piratas informáticos, pero otras plumas se adelantan al describirlos como Hackers. Nada mas lejos de la realidad.

En el presente articulo trataremos de separar cada uno de los componentes que forman la nueva sociedad Underground con el fin de identificarlos correctamente y conocerlos a fondo. Es posible crear un perfil de cada uno de ellos y conocer cuales son sus intenciones a partir de las experiencias adquiridas en este sector. **También trataremos de acercarnos mas al verdadero mundo del Hacking y que sucede en realidad en este terreno, por ello relataremos una crónica del Hacker, esto es, un día cualquiera de alguien que irrumpe la red con ganas de divertirse.**

También es cierto que la nueva cibersociedad surge a partir de la era de la informática llevada al hogar, esto es así ya que la posibilidad de manejar un ordenador ha aumentado de forma considerable al ser altamente asequibles estos equipos. Por otro lado Internet ofrece con mucho, grandes posibilidades de exploración de mundos desconocidos y el encuentro con Software especifico, véase Sniffers o unabombers por ejemplo.

El acercamiento para cualquiera de la tecnología de los bits y las comunicaciones, ha despertado el interés de muchos talentos que son capaces de hacer algo mas que escribir un texto. Un ordenador presumiblemente podrá hacer un renderizado complejo de una imagen 3D, pero también es cierto que si conocemos el lenguaje a fondo, podemos hacer mas cosas que escribir o dibujar. Por otro lado hay que añadir, que cualquier programa de comunicación, como un navegador o un gestor de correo, siempre tendrá ***« una puerta trasera «*** por la que realizar otras operaciones que las permitidas. A esto se les denominan Bugs, pero nos preguntamos si acaso están hay de forma intencionada, ya que es difícil creer que una cosa así, pase inadvertido por cientos de ojos, ya que un núcleo o programa normalmente no lo realiza una sola persona.

Sea cual sea la razón, lo cierto es que estos bugs han permitido un aumento considerable de ***« cerebros fugados «*** capaces de detectarlos y hacer uso de ellos, algunos de ellos de forma indebida. Y estos ***« cerebros «*** han encontrado también una buena fuente de inspiración en la Red de Internet, ya que a través de ella se realizan los grandes Hacks y comprometen la seguridad del internauta aislado.

## DE VERDAD, QUE ES UN HACKER

### El perfil de un Hacker...

Un Hacker es a todas luces, alguien con profundos conocimientos sobre una tecnología. Esta puede ser la informática, electrónica o comunicaciones. El Hacker normalmente conoce todos los terrenos en los que reposa la actual tecnología.

Así pues, el verdadero Hacker es alguien que tiene ansias por saberlo todo, le gusta la investigación y sobre todo lo que resulta mas difícil de descifrar. Nos estamos refiriendo a sistemas de cifrado o sistemas de codificación. En la actualidad los sistemas de cifrado y codificación están al orden del día, tomemos como ejemplo los canales de televisión de pago o cualquier soporte de grabación de datos como el CD o DVD.

Cada uno de estos dispositivos se basa en un estándar de codificación de datos, al igual que sucede con el protocolo de comunicaciones de Internet TCP/IP. En la actualidad y mas en el futuro, la tecnología se basa en protocolos y datos correlacionados en cadena. El entendimiento de estas cadenas de datos nos darán una superioridad de control sobre cualquier tecnología. Este entendimiento nos permitirá entre otras cosas, modificar la información, un reto para todo Hacker.

Así un Hacker busca, primero el entendimiento del sistema tanto de Hardware como de Software y sobre todo descubrir el modo de codificación de las ordenes. En segundo lugar, busca el poder modificar esta información para usos propios y de investigación del funcionamiento total del sistema.

El perfil del Hacker no es el típico chalado de los ordenadores que vive solo y para los ordenadores, aunque si es cierto que pasa largas horas delante de el. Ya que sin trabajo no hay resultados. Los conocimientos que adquiere el Hacker son difundidos por el, para que otros sepan como funciona realmente la tecnología.

Otros datos erróneos sobre la descripción del Hacker, es aquella que los presenta como adolescentes de gafas negras de montura de hueso y extendido acné sobre su cara, en la mayoría estudiantes de informática de cuerpos endebles que siempre consumen cocacola y pizzas. Esto es totalmente incierto, si bien podría coincidir en alguna ocasión, el Hacker normalmente es una persona normal con aspecto físico variado, estudiante de informática o no, al que le guste la cocacola o no. El Hacker puede ser adolescente o adulto, lo único que los caracteriza a todos por igual, son las ansias de conocimientos.

Tampoco es cierto que el Hacker surge a raíz de la nueva era de la informática, ya que Hacker es aquel que trata de averiguar cosas y esto se puede aplicar en las comunicaciones que existieron mucho antes que los ordenadores. De modo que se desmiente que los HACKERS tengan una edad temprana. Ya en la segunda guerra mundial se trataba de descifrar los mensajes del enemigo.

Sin embargo, también es cierto que es ahora, cuando mas proliferación de Hackers existe, dado la importancia que cobra la informática y la Red de Internet hoy día. Por otro lado en la actualidad existe mas información al respecto a través de la prensa y WEBs en la red.

Los verdaderos Hackers aprenden y trabajan solos y nunca se forman a partir de las ideas de otros, aunque es cierto que las comparten, si estas son interesantes.

## LA NUEVA CIBERSOCIEDAD

A raíz de la introducción de la informática en los hogares y los avances tecnológicos que esta aporta, a

surgido toda una generación de personajes mas o menos peligrosos que difunden el miedo en la Red y la prensa.

Catalogados todos ellos como ***« piratas informáticos «*** la nueva generación de ***« rebeldes «*** de la tecnología aportan, unos sabiduría y enseñanza y difunden, otros destrucción y desolación. Hay que saber bien quien es cada uno de ellos y catalogarlos según sus actos de rebeldía en la mayoría de los casos.

Hasta la fecha esta nueva cibersociedad, ha sido dividida en una decena de grandes áreas fundamentales en las que reposan con fuerza, la filosofía de cada uno de ellos. Todos y cada uno de los grupos aporta, en gran medida algo bueno en un mundo dominado por la tecnología, pero esto, no siempre sucede así. Algunos grupos rebeldes toman estas iniciativas como partida de sus actos rebeldes.

Los hackers son el principio y el nivel mas alto de toda esta nueva sociedad. Estos poseen mayores conocimientos que el resto de grupos, pero emplean metodología poco agresivas para mostrar sus conocimientos. Los crackers son probablemente el siguiente escalón y los que son capaces de Crackear sistemas y romper su seguridad, extendiendo el terror entre fabricantes y programadores de Software. Los Lamers, auténticos curiosos aprendices de brujo, poseen mayor influencia en la red a través de WEBs espectaculares, pero vayamos por partes y tratemos cada grupo por separado.

***Hackers : El primer eslabón 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 para lograr comprender sistemas tan complejas como la comunicación móvil. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. Les encanta entrar en ordenadores remotos, con el fin de decir aquello de « 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.***

***El perfil del Hacker idóneo es aquel que se interesa por la tecnología, al margen de si lleva gafas, es delgado o lleva incansablemente encima un teléfono celular de grandes proporciones. emplea muchas horas delante del ordenador, pero para nada debe ser un obsesivo de estas maquinas. No obstante puede darse el caso.***

***Este grupo es el mas experto y menos ofensivo, ya que no pretenden serlo, a pesar de que poseen conocimientos de programación, lo que implica el conocimiento de la creación de Virus o Crack de un software o sistema informático.***

***Crackers : Es el siguiente eslabón y por tanto el primero de una familia rebelde. Cracker es aquel Hacker fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas.***

***Para los grandes fabricantes de sistemas y la prensa este grupo es el mas rebelde de todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica hay, si no en que esta rotura es difundida normalmente a través de la Red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers.***

*En la actualidad es habitual ver como se muestran los Cracks de la mayoría de Software de forma gratuita a través de Internet. El motivo de que estos Cracks formen parte de la red es por ser estos difundidos de forma impune por otro grupo que será detallado mas adelante.*

*Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware. 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. Mas adelante hablaremos de los Cracks mas famosos y difundidos en la red.*

*Lamers : Este grupo es quizás el que mas numero de miembros posee y quizás son los que mayor presencia tienen en la red. Normalmente son individuos con ganas de hacer Hacking, pero que carecen de cualquier conocimiento. Habitualmente son individuos que apenas si saben lo que es un ordenador, pero el uso de este y las grandes oportunidades que brinda Internet, convierten al nuevo internauta en un obsesivo ser que rebusca y relee toda la información que le fascina y que se puede encontrar en Internet. Normalmente la posibilidad de entrar en otro sistema remoto o la posibilidad de girar un gráfico en la pantalla de otro ordenador, le fascinan enormemente.*

*Este es quizás el grupo que mas peligro acontece en la red ya que ponen en practica todo el Software de Hackeo que encuentran en la red. Así 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 autodenominandose Hacker.*

*También emplean de forma habitual programas sniffers para controlar la Red, interceptan tu contraseña y correo electrónico y después te envían varios mensajes, con dirección falsa amenazando tu sistema, pero en realidad no pueden hacer nada mas que cometer el error de que poseen el control completo de tu disco duro, aun cuando el ordenador esta apagado.*

*Toda una negligencia en un terreno tan delicado.*

*Copyhackers : Es una nueva raza solo conocida en el terreno del crackeo de Hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de televisión de pago. Este mercado mueve al año mas de 25.000 millones de pesetas solo en Europa.*

*En el año 1994 los Copyhackers vendieron tarjetas por valor de 16.000 millones de pesetas en pleno auge de canales de pago como el grupo SKY y Canal+ plus- Estos personajes emplean la ingeniería social para convencer y entablar amistad con los verdaderos Hackers, les copian los métodos de ruptura y después se los venden a los « bucaneros « personajes que serán detallados mas adelante.*

*Los Copyhackers divagan entre la sombra del verdadero Hacker y el Lamer. Estos personajes poseen conocimientos de la tecnología y son dominados por la obsesión de ser superiores, pero 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.*

***Bucaneros : Son peores que los Lamers, ya que no aprenden nada ni conocen la tecnología. Comparados con los piratas informáticos, los bucaneros solo buscan el comercio negro de los productos entregados por los Copyhackers. Los bucaneros solo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos « Crackeados « pasan a denominarse « piratas informáticos « así puestas las cosas, el bucanero es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de Cracking a nivel masivo.***

***Phreaker : Este grupo es bien conocido en la Red por sus conocimientos en telefonía. Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente.***

***Sin embargo es, en estos últimos tiempos, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta y/o emplean la informática para su procesado de datos.***

***Newbie : Es un novato o mas particularmente es aquel que navega por Internet, tropieza con una pagina de Hacking y descubre que existe un área de descarga de buenos programas de Hackeo. Después se baja todo lo que puede y empieza a trabajar con los programas.***

***Al contrario que los Lamers, los Newbies aprenden el Hacking siguiendo todos los cautos pasos para lograrlo y no se mofa de su logro, sino que aprende.***

## CRÓNICA DE UN HACKER

En el encabezado de este articulo desvelábamos un segundo bloque bajo la denominación crónica de un Hacker en 32 preguntas. Esto es debido a que el término Hacker, aunque es ampliamente utilizado, pocos son los que hacen buen uso de su nombre. El resto, Crackers o simples Lamers, son la verdadera crónica del día. Ahora, prosigamos.

Para comprender mejor el concepto Hacker, además de saber o conocer que miembros rodean o enturbian a este grupo, es obvio que tenemos que saber que herramientas emplean y que se puede hacer con ellas.

A menudo leemos el correo electrónico ignorando por completo que un troyano acaba de instalarse en nuestro ordenador. Esto es fácil hoy día, ya que existen muchísimos programas Freeware para desempeñar esta función. Por ello, hoy por hoy, el verdadero Hacker quizás no existe o esta en peligro de extinción.

Esto lo demuestra el Chat « o chateo « una opción de Internet que te permite comunicarte con los demás, pero en la que encuentras como casi todo el mundo esta en guerra en el canal. En esta crónica explicaremos de que se trata.

## INICIO DE LA CRÓNICA

...el día que empece con todo esto, no tenia ni la mas remota idea de lo que acabaría haciendo con solo un teclado y unos cuantos golpes de ratón. Toda esa historia de Hackers y de que los demás podían saber lo que estabas haciendo con tu ordenador me parecía mas que un cuento de fábula. Pero no es así. Al contrario de lo que nadie pueda creer, en la red se pueden hacer cosas espectaculares. Todas las respuestas las encontrara en 32 preguntas.

### *1- QUE ES UN HACKER ?*

Ha quedado bien claro en la primera parte de este articulo lo que es un Hacker, pero es obvio que vamos a reincidir en dejar claro lo que es un Hacker, por aquello de quien ha pasado directamente a esta sección.

La palabra Hacker definía, en una primera versión « después de la traducción de Hack « a los entusiastas de los ordenadores que permanecían largas horas de delante de ellos. En la actualidad se definen como expertos en programación y conocimientos elevados sobre informática y electrónica.

Por otro lado, la ley e incluso los medios escritos, aluden a esta nueva generación como aquellos que lindan con lo ilegal. En la actualidad, al fin, se describen a estos personajes como auténticos expertos en sistemas digitales que disfrutan explorando sistemas y probando sus capacidades en oposiciones los simples usuarios, que se conforman con redactar unas cuantas líneas en un procesador de texto.

### *2- ES SEGURO INTERNET ?*

De todos es sabido que no. Hoy por hoy, la red de redes contiene mas virus, exploits, comandos javas « especiales « y otras especias que paginas WEB existen. Es una paradoja, pero lo cierto es que tienes que andar con cuidado en la red. Los canales IRC suelen estar infectados de « aprendices « que emplean todo tipo de « armamento « IRC para fastidiar a cuantos chatean en el canal.

El correo electrónico también se ve perjudicado ya que puedes encontrarte un mensaje sin sentido que lo único que ha hecho es colocarte un « troyano « en tu ordenador o quizás un Virus. Para los usuarios que se decantan por el tema de Hacking, navegar sin precauciones por estas paginas, puede resultar peligroso, ya que a veces cuando se hace una descarga de algún programa, este contiene un virus o un troyano.

El pago electrónico a través de la red también esta en peligro, ya que existen programas específicos para interceptar las transiciones o en el peor de los casos emplean tu numero de tarjeta para futuras compras ajenas.

También existen utilidades que permiten escanear los puertos de cualquier ordenador conectado a la red y utilidades que controlan todos los paquetes que viajan por la red, sin embargo también es cierto que podrás navegar, a menudo, por la red sin tener problemas.

### *3- ESTA BIEN VISTO SER HACKER ?*

Para la sociedad no. Y de esto tiene la culpa en parte la prensa escrita, ya que a menudo se confunden los hackers con piratas informáticos. Por otro lado solo aparecen publicados las fechorías mas sonadas de la actualidad, como la penetración de piratas informáticos en el pentágono o la NASA.

O quizás han sido unos Hackers...lo cierto es que solo publican el daño que han hecho, además en la actualidad se esta poniendo de moda el ciberterrorismo en la red, donde cuelgan severas protestas en las WEBs mas importantes.

Por otro lado la palabra Hacker parece estar ligada siempre a alguien que ha perpetrado un robo a un banco desde un ordenador o alguien que hace daño a cualquier internauta u empresa. La poca o mala información sobre el tema, y la expansión de nuevos « especímenes « en la nueva cibersociedad, infundan confusión.

### *4- EXISTEN SOLO LOS HACKERS O HAY ALGUIEN MAS EN LA RED ?*

Por supuesto que existe alguien mas, por ello la causa de la confusión del verdadero rol de los Hackers. Después de estos, están los Crackers « Hackers de élite rebeldes « que emplean sus conocimientos para difundirlos en la red en forma de Software que otros utilizaran indebidamente. Los Crackers revientan sistemas y roban la información del ordenador ajeno.

También están los Lamers o Newbies, esto es, novatos que se bajan de las paginas de otros « aficionados « programas Sniffers, escaneadores o virus para luego ser empleados a uso de ratón, ya que hoy por hoy no hace falta ser un experto programador para dirigir el puntero del ratón sobre cada pestaña del programa descargado.

Pero el grupo que mejor merecido tiene, son aquellos que no se denominan Hackers, como cuartango, en este caso son expertos en seguridad que detectan fallos o bugs en los sistemas y lo hacen publico, para que las empresas de dicho software « dañado « ponga remedio. Un ejemplo de ello, es el agujero de Cuartango, un bug o puerta trasera del conocido navegador EXPLORER que permite mediante una simple opción, coger información del disco duro de un ordenador remoto.

### *5- QUE ES UN MAILBONBING*

Es el envío masivo de correo electrónico comúnmente conocido como bombardeo en el entorno del Hacking. Los MAILBONBING son programas que permiten enviar miles de veces un mismo mensaje a una determinada dirección de correo electrónico.

A veces el mailbombing, también permite el envío de correo fantasma, esto es, correo falso sin dejar rastro para quien lo envía, esto le permite pasar inadvertido. A esto se le llama correo anónimo.

### *6- QUE ES UN CRACKER*

El tema Cracker también ha quedado suficientemente claro, pero podemos recordar de nuevo que se trata de un Experto Hacker en cuanto conocimientos profundos de programación y dominio de la tecnología.

El Cracker diseña y fabrica programas de guerra y hardware para reventar software y comunicaciones como el teléfono, el correo electrónico o el control de otros ordenadores remotos. Muchos Crackers « cuelgan « paginas WEB por diversión o envían a la red su ultima creación de virus polimorfico.

También existen Crackers que se dedican a crear Cracks para Software importante y negocia con ellos, existen cracks para tarjetas, Shareware y sistemas electrónicos como el DVD o las consolas Playstation entre otros.

### *7- QUE ES IRC*

Comúnmente conocido como canal de chateo o « forma de intercomunicarse con otros usuarios en tiempo real a través de texto y ahora 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 paginas de Hackeo y utilidades WAR o de guerra, es una moda ir fastidiando por este canal.

### *8- QUE ES UN LAMER*

Es un aficionado en el tema. Es aquel que ha visitado varias paginas WEB sobre Hacking y se ha bajado unos cuantos programas fascinados. Después hace uso de ellos indebidamente y sin conocimientos, lo mismo se destruye su propio ordenador como otros de la red y cuando esto sucede se siente alguien superior a los demás.

Este tipo de personajes es quien emplea los Bac Orifice, Netbus o virus con el fin de fastidiar y sin tener conocimientos de lo que esta haciendo realmente. Son el ultimo escalón de la nueva cibersociedad.

### *9- SON SEGURAS LAS PAGINAS WEB SOBRE HACKING*

Algunas de ellas pueden resultar peligrosas e inseguras, pero no todas. Es cierto que las paginas sobre Hacking, pueden resultar una muy buena fuente de información para los « novatos «, pero existen algunas paginas, creadas por personas con vagas intenciones, que colocan en ellas utilidades dañinas como Virus o cookies « malos «.

Un ejemplo esta en lo que me sucedió el otro día. No recuerdo que pagina era, pero si que aparecía tras una búsqueda en el buscador METABUSCA. En ella aparecía una pagina que llamaba la atención por su aspecto gráfico. Cuando trataba de bajar un archivo de no mas de 30 Kbytes y justo cuando estaba al 95 % de la descarga, la utilidad de Antivirus de Panda Software detecto un virus solicitando abortar o desinfectar. Seleccione desinfectar y la sorpresa fue cuando un nuevo cuadro de dialogo me indico que era imposible desinfectar el fichero. La única solución era pulsar escape, pero ya era demasiado tarde, el nuevo virus con nombre desconocido VxD y unos cuantos números aleatorios, había resultado ser un programa autoejecutable, que terminó por bloquear el ordenador.

Lo curioso del caso es que después de resetear el ordenador este no detectaba el fichero principal del Antivirus panda. Tras arrancar Windows, Panda había dejado de funcionar porqué el fichero EXE había

sido borrado del sistema. Pero lo que mas me impacto fue cuando trate de instalar de nuevo el Antivirus. Este ya no se podía instalar de nuevo, abortándose el proceso de instalación.

### *10- QUE ES UN TROYANO*

Un troyano posee diversos significados y acometidos. Atrás, un troyano era un programa oculto que proporcionaba un cuadro de dialogo falso que debías aceptar, tras lo cual, el troyano se « quedaba « con lo que tecleabas después, en este caso la clave. Después el troyano encriptaba la clave nuestra y se enviaba de forma automática a un correo electrónico especifico, cuando empleábamos el correo electrónico, sea cual sea la dirección.

Ahora un Troyano recibe el nombre de Back Orífice, Netbus o Deep Troaht. 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.

Estos, son los troyanos que han hecho « flaquear « la seguridad de Windows 95 o 98.

### *11- QUE ES UNA BOMBA LÓGICA*

Es lo mas parecido a un virus. Una bomba lógica es un programa autoejecutable que espera un determinado tiempo o actividad sobre el teclado para explotar, o dicho de otra manera, infectar el ordenador, modificando textos, mostrando gráficos o borrando parte del disco duro.

### *12- ES SEGURO EL CORREO ELECTRÓNICO*

En absoluto, el correo electrónico no es nada seguro. A través de el se pueden recibir ficheros « pegados « indeseables. Además el correo electrónico puede ser interceptado y leído por los Lamers, que emplean Sniffers, programas capaces de interceptar correo electrónico entre otros.

### *13- QUE ES UN FIREWALL*

Un Firewall es una utilidad o herramienta de seguridad, que impide que ciertos comandos o paquetes de datos « anormales « penetren en nuestro sistema. Comúnmente son traducidos como barreras de fuego, que detectan ataques o entradas forzadas en los puertos de nuestro sistema. Denominados también Nuke.

### *14- SON SEGUROS LOS DOWLOADS DESDE INTERNET*

Ni mucho menos, entre ellos puedes descargar un virus « insertado « en el programa o un troyano renombrado. Las descargas mas peligrosas son las extensiones ZIP y EXE. El servidor de Back Orífice, puede renombrarse fácilmente y hacernos creer que estamos bajando otro fichero.

### *15- ES SEGURO WINDOWS 95 O 98*

Con la presentación en sociedad de Back Orífice por « Cult of The dead « Windows ha dejado de ser un sistema operativo aislado y seguro por sus limitaciones de comunicaciones en redes, excepto el explorador.

En la actualidad se han encontrado bugs en el navegador que permiten a alguien husmear nuestro disco duro o robar ficheros de nuestro ordenador. Es el denominado agujero de cuartango, el bug mas peligroso de todos.

Los cookies de las paginas WEB son otra amenaza para Windows, pero como mucho nos cuelan algún tipo de virus. Sin embargo lo mas peligroso es el fichero servidor.EXE de Back el que hace tambalear Windows, dada la moda reciente de « controles remotos «.

### *16- QUE ES BACK ORÍFICE*

Back Orífice es un programa de control remoto de ordenadores que funciona bajo un servidor y un cliente. si colocamos el servidor a otro ordenador remoto, es posible desde el cliente, gobernar cualquier función del ordenador remoto, entre los que destaca abrir y cerrar programas, controlar el CD, leer y escribir ficheros o borrar parte del disco duro.

Para ello el servidor se autoejecuta y se borra cada vez que el ordenador ajeno se enciende, nuestro cliente escanea el puerto elegido y cuando este esta abierto, actúa a través de el desde un menú cliente repleto de pestañas y opciones de control remoto.

El sistema es bueno para controlar un ordenador o ordenadores en una red LAN interna y a pesar de lo que se diga, podría ser menos nocivo que un virus, aunque dejar esta puerta abierta para Windows es todo una amenaza.

### *17- QUE ES UN PIRATA INFORMÁTICO*

Comúnmente confundido con un Hacker, un pirata informático es quien hace copias de Software en CD y comercializa con ellos. No posee conocimientos, mas que para duplicar discos y este es el grupo que mas mancha a la nueva sociedad de hackers, después de los Lamers.

### *18- QUE ES NETBUS*

Se trata de un troyano anterior a Back Orífice y funciona bajo los mismos principios que este, en la actualidad esta siendo de moda el empleo de Netbus o Back Orífice por cualquier usuario de ordenador.

### *19- EXISTE UN MANUAL DEL HACKER*

Existen varios y todos ellos se encuentran en Internet. El manual del Hacker indica los diez puntos mas importantes que todo buen Hacker busca en su progreso hacia la cumbre. Los manuales están en ingles,

pero existen versiones reducidas en español, bajo el nombre de « novicio «, estos manuales normalmente cubren situaciones dirigidas hacia los « nuevos « en esta cibersociedad y por supuesto no indican el modo de hacer funcionar programas peligrosos.

### *20- QUE HERRAMIENTAS SON IMPRESCINDIBLES PARA EL « HACKER «*

El Hacker necesita herramientas que le faciliten el trabajo en la red. Entre estas herramientas destacan los sniffers, escaneadores y programadores de tarjetas inteligentes. También se recomienda poseer algún Mailbombing y Nukenabber para enfrentarse a aquellos que solo actúan por fastidiar.

Para entrar en sistemas ajenos, « aunque sea solo para ver dentro de el y salir después « el Hacker debe echar mano a un buen diccionario para obtener la clave de acceso. Actualmente también es necesario disponer de utilidades de guerra IRC y WAR, para enfrentarse a otros enemigos. Un buen Virus bajo la manga nos apartara al indeseado que nos moleste.

Pero lo mas importante es la motivación y la intuición, sin ellas nada se puede hacer.

### *21- QUE ES PGP*

PGP, de Pretty Good Prívate es el programa de cifrado por excelencia para la mayoría de usuarios que pretenden proteger su correo electrónico o 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 Diffie fue prohibido para su exportación, pero a alguien se le ocurrió publicarlo en Internet en forma de texto, y alguien lo compilo de nuevo en Europa. Así fue como PGP llego a Europa. Actualmente esta por la versión 6.0 e incluso se conoce una versión en castellano de este programa de cifrado altamente seguro.

También los hackers deben disponer de esta herramienta.

### *22- QUE ES WAREZ*

Warez es en realidad software « conocido « que lleva incluido un Crack para ser instalado sin numero de serie o en varias maquinas sin pagar por el. En Internet se encuentran infinidad de Warez y números de serie para los programas mas conocidos.

Los Warez son una forma de Crackear software y linda con el lado del delito entrando de lleno en el, ya que se violan los derechos de autor.

### *23- QUE SON LOS ESCANEADORES*

El mas conocido es el Scanerport y como su nombre indica, se trata de programas que permiten rastrear la red en busca de puertos abiertos por el cual acceder y manipular un sistema o introducir un troyano o virus.

PortScan es otra utilidad ampliamente conocida por los Hackers y con este programa nadie esta a salvo.

### *24- QUE ES UN CRACK DE SOFTWARE*

El Crack de un software, que convierte al mismo en un Warez, es la inclusión de un código o varias líneas de códigos en los ficheros de registro del Software que impide que se caduque tal programa.

Todas las versiones de evaluación o Shareware poseen caducidad. Los datos que permiten esto, normalmente están 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 estos datos u otros de forma que el programa no reconozca la fecha de caducidad.

Por otro lado, el Crack es también la localización del numero de serie del programa. Este numero de serie es localizado gracias a un generador de números de serie o Generator, una utilidad muy ampliada por los Crackers para obtener logins o números de serie.

### *25- ES SEGURO EL PROTOCOLO TCP/IP*

El protocolo de comunicaciones de Internet TCP/IP es quizás, el protocolo menos seguro de cuantos existen, pero este es el estándar y por ello los Hackers desarrollan continuamente herramientas capaces de monitorizar la secuencia de datos y paquetes TCP/IP.

SSL pretende ser un nivel de seguridad para transacciones electrónicas de dinero, pero también ha sido objeto de conocimiento de los Hackers y por tanto un sistema inseguro. Los sniffers pueden monitorizar estos comandos, al igual que el VOYAGER monitoriza los comandos de las tarjetas ISO 7816.

Un protocolo seguro seria aquel que contenga protocolos variables y encriptados, así como estructura de paquetes variables.

### *26- QUE ES 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 este puerto.

Nukenabber es una utilidad muy útil para un Hacker.

### *27- QUE ES EL PRHEAKING*

El Prheaking es una extensión del Hacking y el Cracking. Los Phreakers son expertos en sistemas de telefonía fija o inalámbrica. Conocen a fondo los sistemas de tonos, enrulados, tarjetas inteligentes y el sistema GSM.

Tron era un buen ejemplo de Phreaker, ya que había logrado clonar una tarjeta GSM. Los Phreakers emplean sus conocimientos para realizar llamadas gratis y a veces es empleado por Hackers para mantener sus actividades en la red.

### *28- QUE ES UN SNIFFER*

Un sniffer es una utilidad que permite la monitorizacion 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, son empleados como Sniffers, esto es, monitorizacion de la red y la unidad central.

Una navegación lenta en Internet nos puede indicar que hay un sniffer en línea.

### *29- QUE ES CARDING*

El Carding es una extensión mas de esta nueva cibersociedad y sus constantes búsquedas por controlar todos los sistemas informaticos y electrónicos de la sociedad actual. Hoy por hoy la implantación de las tarjetas de crédito, es masiva y esta presente en casi todos los sectores tales como operaciones bancarias, acceso a televisiones de pago, sistemas de pago electrónico y acceso controlado.

El Carding es el estudio de tarjetas chip, magnéticas u ópticas y comprende la lectura de estos y la duplicación de la información vital. actualmente se ha conseguido clonar las tarjetas GSM, tarjetas de canales de pago y Visa por este procedimiento.

### *30- EMPLEAN LA CRIPTOGRAFÍA LOS HACKERS*

Mas que nadie, los hackers o crackers se ven obligados a emplear sistemas criptograficos para su correspondencia electrónica. Normalmente emplean el conocido PGP, pero también es habitual otros métodos de cifrado, siempre de claves publicas.

También es cierto que los Gurus emplean métodos criptograficos desarrollados por ellos mismos, además del empleo de la esteganografia, método que permite encriptar datos en una imagen o gráfico.

### *31- QUE SON LOS DICCIONARIOS*

Existen dos tipos de diccionarios entre la comunidad Hacker y ambos son imprescindibles dado su contenido. El diccionario básico del Hacker es aquel que detalla la extensión de los nuevos acrónimos habitualmente empleados entre esta sociedad. Así se describen acrónimos como spoofin, Nuk, Zombie o 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 sobre el Hacking, Cracking, Phreaking y otros servidores.

El otro gran diccionario y verdadera utilidad de los Crackers mas que de los Hackers, es el diccionario de palabras. cuando se emplea la fuerza bruta para obtener los Paswords o contraseñas de un programa, pagina 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

esto se le denomina fuerza bruta ya que se compraran miles de palabras en menos de un segundo.

### *32- QUE ES LA INGENIERÍA SOCIAL*

La ingeniería social es quizás la base de un Hacker, para obtener los datos o lo que le interesa por medio de una conversación y de personas. Es la forma de engañar al otro, camelarlo y hacerle creer que eres alguien bueno, el técnico de la compañía de teléfonos quizás.

Una buena muestra de ello, es el timo de telefónica, en el que te llaman haciéndose pasar por un técnico de la compañía y te solicitan que teclees un numero después de colgar. Este comando llamado ATT, le permite al ingeniero social, realizar llamadas a través de tu teléfono.

Y en la actualidad esta sucediendo en nuestro país, así que cuidado.

# Capitulo 6

# El manual del Hacker

***....No existe una Biblia al respecto, que indique paso a paso como introducirse en un sistema o " desproteger" la BOOT de un disco de Playstation. Mostrar todas las técnicas y Cracks seria una tarea demasiado ardua y larga, por ello aquí debo enunciar los pasos básicos del verdadero Hacker.***

***El primer manual del Hacker es aprender las cosas por si solo. El segundo paso es tener en cuenta este libro, el que tiene entre sus manos y que le muestra muchas cosas interesantes. El tercer paso es ser cauto con lo que se hace. Y para finalizar, un buen aspirante a Hacker debe documentarse hasta la saciedad.***

***Para que ello sea así, he rebuscado por Internet y he descubierto una muy buena colección de libros que serán del agrado para el nuevo Hacker. En ellos se describen verdaderas historias de Hackers y se revelan algunas tácticas de como se han efectuado ciertos Hacks o Cracks....***

Esta seria a resumidas cuentas las palabras que podrías encontrar en cualquier pagina de Hacking en la ReD, mi objetivo desde aquí, no es fomentar el Hacktivismo, pero si el de informar de todos los conceptos que los rodean. Lo que a continuación voy a describir, es la existencia de una serie de libros " los mejores " que tratan sobre Hackers e historias sobre los mismos. Son libros de obligada lectura, siempre con fines educativos y para nada se deben emplear los conocimientos adquiridos con ellos.

## 6.1 Los nuevos manuales

Uno de los mejores libros podría ser Approaching Zero de Bryan Clough y Paul Mungo. Dos expertos escritores sobre temas de Hackers. En España este libro ha sido editado por la editorial Ediciones B, bajo el titulo Los piratas del CHIP. Es un libro muy recomendable y practico.

**Approaching Zero Bryan Clough, Paul Mungo**
**1992. ISBN : 0571168132**

**1992. ISBN : 8440631529 España**
**242 paginas**

Es tal vez el mejor relato sobre los phreakers (Hackers telefónicos), y uno de los pocos libros que ofrece versiones completas sobre casos como el del robo del QuickDraw de Apple por parte de los Crackers, los primeros virus informáticas con nombres propios y la historia del Chaos Computer Club. El título hace referencia al posible borrado global de toda la información de los ordenadores del planeta por culpa de los ataques de los piratas, una de las catastróficas perspectivas que plantea el libro.

**Secrets of a Super Hacker The nightmare**
**1994. ISBN :1559501065**
**204 paginas**

Este libro es, sencillamente, un manual de Hackers. Escrito por un anónimo experto, explica todos los métodos clásicos de los Hackers, con un texto muy sencillo y fácil de comprender (incluso infantil, en algunos momentos). Entre las técnicas que se explican están los ataques por fuerza bruta a archivos de contraseñas, la ingeniería social, la interceptación de correo y contraseñas, el acceso a cuentas privilegiadas y otros cuantos trucos más. Incluye incluso una pequeña historia del Hacking y algunas técnicas básicas relacionadas con BBS, Unix y algunas listas de contraseñas comunes

**The New Hacker´s Dictionary Eric. S.Raymond**
**1994. ISBN : 0262680920**
**506 paginas**

Esta segunda edición del Diccionario del Hacker es sin duda referencia obligada para todos los Hackers como para los quiero-y-no-puedo (una de las definiciones del diccionario). Es una edición de lujo del famoso archivo JARGON (jerga) de Internet, en el que durante décadas se ha ido incorporando información sobre la jerga de los Hackers, y usos y costumbres del lenguaje informática. Muchos de los términos y chistes proceden de las oscuras épocas de los orígenes de los Hackers, pero no dejan de tener su gracia. Incluye capítulos sobre costumbres gramaticales de los Hackers, el folklore relacionado, un retrato del prototipo del Hacker y bibliografía adicional. Al Macintosh se le califica en la jerga como Macintoy (considerado como juguete) o Macintrash (por los Hackers que realmente no aprecian separarse de los verdaderos ordenadores por una interfaz bonita). Un Hacker es, cómo no, una persona que disfruta con la exploración de los detalles de los sistemas programables y cómo aprovechar toda su capacidad, frente a la mayoría de los usuarios que prefieren aprender sólo el mínimo necesario.

**Hackers Steven Levy " La revolución de los héroes de las computadoras "**
**1994 ISBN : 0385312105**
**454 paginas**

Si alguien captó y plasmó la realidad de los Hackers desde los años 50 (oh, sí, desde entonces) ese ha sido Steven Levy. Con un gran trabajo de investigación y una atractiva narrativa, Levy recorre los primeros tiempos de los Hackers del MIT y el Tech Model Railroad Club (donde comenzó a usarse la palabra «Hackers») hasta terminar en la época gloriosa de los videojuegos para los ordenadores familiares. En el recorrido se diferencian en tres partes los «auténticos Hackers» del MIT, los Hackers del hardware, incluyendo a la gente del Homebew Computer Club (Wozniak, Steve Jobs, Bill Gates) y los hackers de los videojuegos, centrándose en la gente de Sierra y la evolución de los juegos de ordenador. La «ética del Hacker», su forma de vida y su filosofía quedan plasmados en este libro mejor que en ninguno. Un documento histórico y absolutamente obligatorio

**Underground Suelette Dreyfus**
**1997 ISBN . 1863305955**
**476 paginas**

Esta novela, basada en hechos reales, cuenta las andanzas de un grupo de hackers australianos y sus aventuras en las redes. Al igual que otras novelas sobre hackers, Underground acerca al lector al «lado oscuro» de la Red describiendo varias historias de forma entretenida y explicando, de forma sencilla y elegante, los métodos utilizados y el entorno de cada aventura. Narra varios casos diferentes, situados en el tiempo a partir de 1989, sobre hackers que se introdujeron en la red de la NASA (e introdujeron el «gusano WANK»), la conexión australiana con hackers americanos, los BBS dedicados al lado oculto de la Red, utilizados por hackers y phreakers («piratas telefónicos») y muchas pequeñas historias de casos que tuvieron algo de publicidad en los medios de comunicación. Entre las más llamativas se encuentra el caso del «asalto» a la red de Citybank en Australia, donde los intrusos intentaron hacerse con más de medio millón de dólares. El libro no se dedica sólo a las aventuras divertidas: también indaga en las personalidades de los hackers, su comportamiento habitualmente antisocial, sus problemas familiares y a veces con las drogas, así como la (inevitable) captura por parte de las autoridades, posterior juicio y estancia en prisión de la mayoría de ellos. La descripción de las detenciones, registros y procesos legales es especialmente interesante. El libro tiene como fuentes a varios grupos de hackers australianos y todas las sentencias de los casos de asaltos informáticos de esa época.

**The CucKoo´s Egg Clifford Stoll**
**1989 ISBN : 0671726889**
**394 paginas**

Narrada en forma de novela, el «huevo del cuco» cuenta la historia de Clifford Stoll, un astrónomo e informático que, comprobando sus sistemas, descubre una diferencia de 75 centavos en la contabilidad. Este pequeño detalle le lleva a darse cuenta de que los ordenadores de su red están siendo atacados por Crackers del extranjero, y con ello comienza su particular carrera de persecución hasta dar con ellos. Escrito de forma entretenida y amena, describe la forma en que los Crackers se introducen en los ordenadores y la forma en que pueden ser detectados. Interesante como documento histórico, es uno de los

clásicos sobre el mundo del Hacking y el Cracking.

**Cyberpunk Katie Hafner, Jhon Markoff**
**1991 ISBN : 068418620**
**370 paginas**

Los cyberpunks son los forajidos y hackers de la frontera informática. Este clásico ensayo sobre phreakers (hackers telefónicos) y crackers (piratas informáticos destructivos) narra las aventuras de tres hackers bien diferentes: Kevin Mitnick, uno de los más conocidos hackers telefónicos; Pengo, el Hacker que flirteó con los espías de más allá del telón de acero y RTM (Robert T. Morris), quien creó el famoso gusano de Internet y puso de rodillas a toda la red mundial. Muy informativo y entretenido por su narrativa.

**The Hacker Crackdown Bruce Sterling**
**1992 ISBN : 055356370X**
**316 paginas**

Otro de los clásicos, se trata de un excelente acercamiento periodístico a la historia del phreaking telefónico y el Hacking. Comenzando, literalmente, por la historia del teléfono, recorre los años 70, 80 y 90 contando las historias de los phreakers y hackers más conocidos (Fry Guy, Acid Phreak, Phiber Optik), las historias de los primeros BBS, las incursiones de los pioneros, las persecuciones policiales y del FBI y el famoso caso de los documentos E911 que dejó totalmente en ridículo a la justicia americana ante los hackers. Es un libro muy completo que describe la personalidad de muchos hackers, grupos y entidades del mundillo informático, como los círculos del boletín 2600, el WELL de San Francisco y la EFF (Electronic Frontier Foundation).

**Masters of Deception michelle Slatalla, Joshua Quitter, Harper Collins**
**1995 ISBN : 0060926945**
**226 paginas**

En este libro sobre los crackers (piratas informáticos destructivos) y los phreakers (hackers telefónicos) se describen las andanzas por las redes de bandas como los MoD (Masters of Deception), la LoD (Legión of Doom) y las personalidades y técnicas empleadas por muchos de sus componentes, incluyendo algunos tan populares como Acid Phreak y Phiber Optik. Narra una auténtica batalla entre bandas rivales, las reiteradas detenciones de muchos de sus miembros y la persecución por todo el ciberespacio por parte de los agentes del FBI, para terminar con la detención de los componentes de los grupos y su comparecencia ante la justicia.

**Takedown Tsutomu Shimomura, John Markoff**
**1997 ISBN : 8403595980 versión español**

**464 paginas**

El libro tiene un buen encabezado y dice así; Persecución y captura de Kevin Mitnick, el forajido informatico mas buscado de Norteamérica. Una crónica escrita por el hombre que lo capturo. Narrada con gran maestría, en este libro Tsutomu detalla, con la inestimable pluma de John Markoff, por supuesto, todo lo que sucedió en la noche de Navidad mas larga de su vida. Tsutomu estaba fuera de su casa, pero sus tres ordenadores estaban encendidos y alguien trabajaba con ellos...a distancia. Kevin Mitnick había conseguido penetrar en el sistema de Tsutomu, el hombre mas experto en seguridad informática, pero había algo en sus ordenadores que a Kevin le interesaba. Se trataba del Software de un teléfono móvil OKI. Y quizás esa obsesión por este Software marco el principio del fin del Hacker mas perseguido de toda Norteamérica. En la actualidad, lejos de los teclados, Kevin cumple condena en la cárcel, pero esta siendo apoyado por docenas de WEBs que reivindican sus derechos y su libertad, hasta el punto que varios Hackers amenazan con colapsar la Red con " Gusanos " si no lo sueltan pronto. Por otro lado, como curiosidad cabe decir que Kevin tiene acceso al exterior a través de Internet, ¿ Como lo hará ?. Un libro muy recomendable.

**Enigma Robert Harris**
**1995 ISBN : 8401326672 español**
**388 paginas**

Esta novela de intriga tiene como protagonistas a los expertos británicos que deben descifrar los códigos secretos de la máquina alemana Enigma mientras decenas de submarinos se dirigen hacia los convoyes aliados de las aguas del Atlántico Norte. Los personajes de la historia son ficticeos, pero las máquinas, señales y mensajes alemanes son las originales de los textos históricos.

**Codebreakers F.H:Hinsley. Alan Stripp**
**1993 ISBN : 019285304X**
**320 paginas**

Este libro narra, en primera persona, la historia de Bletchley Park, el lugar en que se rompieron e interpretaron las transmisiones alemanas, italianas y japonesas durante la Segunda Guerra Mundial. Los protagonistas responsables de Ultra, el nombre en clave que los británicos dieron a todas las transmisiones de inteligencia de los enemigos del bando Aliado, cuentan cuál fue su importancia y cómo se descifraron sistemas criptográficos como los empleados en la máquina Enigma alemana y el tráfico Fish (no-morse). El libro es una recopilación de relatos de los trabajadores de Bletchley Park, algunos bien conocidos en el mundo de la criptología, otros, héroes anónimos. Bletchley Park llegó a romper la criptografía de 4.000 mensajes alemanes al día y desarrollar las «bombas» lógicas, Mark y Colossus, precursores de los actuales ordenadores, con el único objetivo de romper códigos secretos. Como vino a decir Churchill, Bletchley

Park y su gente fueron el arma secreta aliada que permitió ganar la guerra. En este libro queda narrada esta historia en primera persona.

**The codebreakers David Khan**
**1996 ISBN : 0684831309**
**1184 paginas**

The Codebrakers es un libro obligado de referencia histórica para cualquier interesado en la criptotología y sus orígenes. Cubre de forma extensa toda la historia de la criptología y sus protagonistas, desde el principio de los tiempos hasta la actualidad. La primera edición de The Codebreakers data de 1967, y la actual (1996) ha sido ligeramente revisada para incluir algo sobre informática, criptografía de clave pública e Internet. [En realidad no hay demasiados cambios sobre la edición original, unas 16 páginas nada más... digamos que se queda en 1967 aproximadamente. Sobre la criptografía moderna pueden encontrarse otros libros más completos]. Comenzando por los jeroglíficos del año 3.000 antes de Cristo, Kahn describe con una narrativa agradable y cuidada los pasos históricos por la criptografía, el criptoanálisis y todas las etapas de su utilización en tiempos de guerra y paz. La mayor parte del libro se centra en los siglos XIX y XX, y en la utilización de la criptología en las guerras mundiales. En su estudio de la criptografía el autor aprovecha para explicar todos los códigos y sistemas de cifrado clásicos, quiénes fueron sus inventores, cómo se descubrieron los sistemas de criptoanálisis y cómo se utilizaban. Todo ello, aderezado con breves biografías de los más importantes criptógrafos. La explicación de los métodos criptográficos está al alcance de cualquiera, y se incluyen abundantes ejemplos, referencias, imágenes y fotografías. Episodios clásicos como el Telegrama Zimmermann (probablemente el criptoanálisis más trascendente de la historia, en la I Guerra Mundial) o el funcionamiento y descifrado de las máquinas Enigma de los alemanes durante la II Guerra Mundial son tratados en profundidad y con todo lujo de explicaciones. El libro completa la visión histórica con explicaciones puntuales sobre la importancia de la criptografía en la sociedad, y está aderezado con varios apéndices sobre la anatomía y patología de la criptología, la criptografía aplicada a la comunicación con seres extraterrestres y una amplísima bibliografía.

**Firewalls and Internet Security Willian R.Cheswick, Steven M.Bellovin**
**1994 ISBN : 0201633574**
**308 paginas**

Describiendo como «cortafuegos» (firewall) un conjunto de componentes diversos, entre los que están los filtros y las pasarelas (gateways), este manual es más una recopilación de consejos prácticos sobre seguridad que una guía paso a paso sobre cortafuegos o productos concretos. Comienza explicando la necesidad de la seguridad y la base de todo: el TCP/IP. La segunda parte explica la filosofía de los cortafuegos y las funciones de sus componentes, de forma más detallada, parándose en todos los servicios de Internet, indicando sus debilidades y dando ideas prácticas. La tercera parte es la más divulgativa, y describe lo que muchos administradores suelen pasar por alto: las más rebuscadas formas de robar contraseñas, la ingeniería social, los fallos y bugs de sistemas y protocolos, las puertas traseras y algunas

formas concretas de ataque a servidores. La última parte está dedicada a las consideraciones legales (monitorización, pruebas) y, de forma destacada, a las comunicaciones seguras sobre redes inseguras. La introducción a la criptografía es muy interesante (y teórica), y se explican algunos sistemas como Kerberos (autenticación) y varios sistemas de cifrado a nivel de aplicaciones y transporte de red. Termina con una lista de software gratuito útil para los administradores de redes y seguridad, algunas recomendaciones generales (para fabricantes de sistemas) y una bibliografía extensa, donde se pueden encontrar muchos ejemplos teóricos y prácticos de ataques. Lo más interesante del libro: una serie de iconos de «alto peligro» (más de 40) que alertan en cada sección de los problemas más graves que suelen encontrarse en las redes.

**PGP, Pretty Good Privacy Sims Garfinkel. O´Reilly**
**1995 ISBN : 1565920988**
**394 paginas**

Este libro es un manual de referencia sobre PGP realmente completo y bien escrito, que cubre todas las variantes de la versión 2.6.2. Contiene todo lo que se puede necesitar saber sobre las primeras versiones de PGP y su utilización: todas las opciones, modos, uso de las claves públicas e instrucciones paso a paso para la generación de claves, gestión de los anillos de claves y uso de las firmas digitales. Además de esta parte práctica, el libro cuenta con varias secciones de interés general. En la primera, las bases de la criptografía, explica todos los términos y teoría de la criptografía clásica y moderna. Un par de capítulos están dedicados a la criptografía antes de PGP (historia y política) y otro al desarrollo de PGP en sí, incluyendos datos difíciles de encontrar en otros libros, como la historia detallada y pormenorizada de PGP desde las primeras ideas hasta la versión 1.0. Otro capítulo está dedicado a las implicaciones políticas de la «criptografía fuerte», y la inmiscusión de las «agencias de tres letras» en este terreno. Los apéndices del libro incluyen información detallada para instalar PGP (versión 2.6) en PC, Unix y un Macintosh.

**Applied Cryptography Bruce Schneider. John wiley**
**1995 ISBN : 0471117099**
**784 paginas**

Este es el libro de referencia obligatorio para cualquiera que quiera programar algoritmos y protocolos criptográficos en su ordenador, o aprender cómo funcionan y cuáles son sus bases. Applied Cryptograpy está dividido en cuatro partes: Protocolos, técnicas, algoritmos y «el mundo real». La parte de procolos explica los sistemas básicos y avanzados de intercambio de claves, autentificación, firmas, etc. La parte de técnicas describe sistemas de gestión de claves, cifrados de bloques y de flujo, funciones hash y el uso del cifrado en sistemas convencionales. La tercera parte, más técnica, describe los algoritmos criptográficos, su base matemática y algunas implementaciones. Entre los algoritmos más destacados están el DES y sus variantes, Diffie-Hellman, RSA, RC2 y RC4, IDEA, Skipjack (Clipper) y funciones hash como MD2-MD5 y SHA. La parte del «mundo real» explica algunas implementaciones clásicas, como Kerberos,

PEM, MSP, PGP, Clippper y Capstone. También hay algo sobre criptografía y política en uno de los capítulos finales, incluyendo referencias a páginas WEB, boletines, asociaciones y grupos de noticias de Usenet. La parte final del libro incluye listados del código fuente en C de muchos de los algoritmos explicados en la tercera parte del libro: Enigma, DES, NEWDES, IDA, MD5 y otros.

**The Book of prime number records Paulo Ribenboim. Springer-Verlag**
**1988 ISBN : 0387965734**
**478 paginas**

Este curioso libro presenta, como su título indica, los récords relativos a los números primos. Pero contiene mucho más: todas las preguntas frecuentes, respuestas y demostraciones de teoremas relativos a los números primos. Comenzando por «cuántos números primos hay» explica en lenguaje matemático (de alto nivel) un gran número de formas de comprobar si un número es primo (importante en criptografía), explica los diferentes tipos de primos y su distribución e incluye diversos apéndices con problemas, conclusiones y tablas.

**Protect youMacintosh Bruce Schneier**
**1994 ISBN : 1566091012**
**316 paginas**

Libro de referencia para los usuarios de Macintosh y responsables de sistemas interesados por los temas de seguridad. Describe técnicas de encriptación de archivos, protección ante virus informáticos, copias de seguridad, seguridad física y seguridad en red. Incluye muchos consejos y referencias a software y hardware comercial, con ejemplos, descripciones y precios.

**Codes, Ciphers and secret writing Martin Gardner**
**1972 ISBN : 0486247619**
**98 paginas**

Pequeño libro de Martin Gardner (autor durante muchos años de la columna «Recreaciones Matemáticas» de Investigación y ciencia) en el que en forma de juegos explica los códigos y sistemas de cifrado más sencillos. Contiene muchas ilustraciones y problemas sencillos de resolver. Aunque antiguo, resulta entretenido y muy recomendable para principiantes. Es tal vez la forma más amena de comprender y jugar con los sistemas de cifrado clásicos. Podría considerarse un The Codebreakers simplificado, porque el recorrido que hace por la criptografía sigue también la línea histórica. Para los amantes de los sescretos, también se incluyen un buen número de sistemas «alternativos» de envíos de mensajes, especialmente de steganografía.

**Hackers Piratas Tecnológicos Claudio Hernandez**
**1997 ISBN :**

**417 paginas**

Un libro indispensable para los futuros Hardware Crackers y además uno de los muy pocos libros editados en Español sobre el tema de Hacking y el primero que revela aspectos técnicos de los Cracks. El libro repasa sobremanera a una buena cantidad de Hardware Crackers y sus logros. También se exponen circuitos y tácticas para descodificar casi todos los canales de televisión de pago. Se da un repaso a las tarjetas electrónicas de pago y se trata con delicadeza las técnicas de Hackeo.

## 6.2 Agradecimientos

En primer lugar le debo un especial agradecimiento a todos aquellos, que con tesón y voluntad, han escrito estupendos libros y manuales que nos son de mucha ayuda. Otros libros, que simplemente repasan la historia de los Hackers, son también una fuente de inspiración.

Todos los libros aquí expuestos son asequibles desde la pagina criptopublicaciones de Alvaro, ex-director de la revista Iworld y buen amigo, o al menos nos comunicamos por E-Mail y le regale uno de mis libros...con la incursión de estos títulos, en cierta manera fomento y ayudo al mismo tiempo, a que se divulgue la cultura Hacker y todos, cada día un poquito mas, sepamos de que estamos hablando.

Pero el mayor de los agradecimientos es para la ReD de Internet, porque encuentras todo lo que necesitas. Existen muchos libros mas, como el diccionario del Hacker, así como versiones electrónicas de algunos de estos libros citados aquí. Pero nómbralos todos, seria una tarea ardua y no cabrían en este libro. Así que te animo a que investigues por tu cuenta, algo que forma parte del buen ivestigador de los temas de la nueva cibercultura .

# Capitulo 7

# El Software del Hacker

Además de la parte divulgativa y teórica, este libro pretende dar a conocer también que Software emplean los Hackers para el quehacer diario. El software presentado a continuación esta " capturado " de la Red y en ningún momento se pretende comercializar desde aquí. Simplemente citarlos y explicar algunas simples funciones de ellos.

Todo buen Hacker tiene unas herramientas o Software que le permite " trabajar " a sus anchas por la gran Red. Estas herramientas o software están divididos en seis grandes bloques, claramente identificados, según la acción que deseemos realizar. Dentro de estos bloques existe el riesgo de cometer delitos y entrar en Cracking. En este punto, el uso que de ellos se deriva corre bajo la responsabilidad del " actuador " en ese momento. Pero desde aquí tenemos la obligación de informar cuales son y que hacen, dado que se encuentran en la Red y merecen también un apartado para ellos.

## 7.1 Los seis bloques

Divididos en seis bloques diferenciaremos cada una de las herramientas que todo Hacker o aprendiz de Hacker, parece tener guardado en su disco duro y en copias Backup.

*** Hacking y Cracking.**

Se trata de Software que permite controlar la Red o por otro lado, " reventar " Software extraído de la Red. Los programas que se pueden adquirir dentro de este bloque, permiten entre lo dicho, " capturar " paswords, controlar FTP o puertos IRC. También se pueden encontrar " manuales " de Hackeo y Diccionarios para desencriptar claves.

*** Clonacion de tarjetas de crédito.**

Se trata de Software capaz de crear números aleatorios de tarjetas de crédito, que pueden coincidir o no con la realidad. También en este bloque se emplean programas capaces de interceptar números de tarjetas de crédito que circulan por la Red sin estar encriptadas.

*** Encriptacion.**

Se emplean por los Hackers y Crackers como medio para esconder su información o los propios Virus. Es indispensable tener software de este tipo para que no sepan nunca de que hablas en la red.
Los sistemas de encriptacion pueden ser de encriptacion de simple correo electrónico, o cifradores de imágenes o ficheros ejecutables.

*** Virus.**

Son empleados para fastidiar al enemigo y siempre se tiene uno de ellos a mano en momentos precisados. El tema de los Virus ha sido bien detallado por lo que sobran las palabras.

*** Telefonía.**

Aquí esta el Phreaking, todo Hacker o Cracker tiene algún programa que le permite realizar llamadas gratuitas o escanear los números de los teléfonos de la Red. En la actualidad también existe software para controlar los teléfonos celulares, así encontramos Software capaz de chequear números de tarjetas a través de retos, o programas que generan números para tarjetas AT&AT.

*** La guerra de puertos IRC o penetraciones en equipos remotos.**

Es la máxima aspiración del Hacker o Cracker, el poder entrar en ordenadores remotas, para ello debemos escanear los puertos o buscar las direcciones IP de los Host. Aquí también se crean Software para " inutilizar " a la maquina del enemigo.

# Capitulo 8

# Historias de Hackers y Crackers

Tomemos un momento de descanso y repasemos historia. También es bueno analizar que han hecho algunos Hackers y Crackers, con el fin de inspirarnos un poco o impresionarnos otro tanto.

En las siguientes líneas explicare algunos sucesos, los cuales mas me han impactado, pero estoy seguro que existen mas penetraciones de sistemas, Craks y toda una extensión de fechorías que no cabrían en este libro.

Me tomare también la libertad de cambiar nombres y lugares de los hechos, por aquello de no " relatar " la intimidad si así no se desea, pero claro esta si un buen día se escribió sobre ellos, a modo de titulo les gustaba salir en la prensa, pero siempre había una pequeña nota, bajo el articulo que decía :

Los nombres y lugares de los hechos son ficticios, pero los hechos, son por el contrario, reales a todas vistas.

Ahora la prensa se entera de si tu perro se mea en el sofá. Pero, por mi parte y con mucho respeto no diré si el perro de un buen Hacker se mea en el sofá, ni tampoco revelare su nombre. Aunque ahora que digo esto...quizás si revele uno, solo uno, y será al final de este capitulo.

## 8.1 El caso del Phreaker ciego

Es quizás, y con toda probabilidad la historia que mas me ha impresionado de alguna manera. Se trata de Tim Rosenbaum, un chico que a la temprana edad de 10 años, acometió, lo que hasta la fecha será la mayor estrategia lograda.

El buen chico nació ciego, pero dios le dio un excelente sentido, el oído, con una sensibilidad superior a los demás seres mortales. Sus blandas yemas de los dedos también poseían un tacto inverosímil, capaz de almacenar el tacto suave o áspero de las cosas y reconocerlas por ellas después.

Y también tenia algo que fascinaba a todos los chicos de Dollan, un pequeño pueblo costero al este de Maine, y esto eran sus silbidos. Era capaz de imitar a los pájaros de todas las clases y sobre todo podía controlar el tono del silbido hasta alcanzar notas musicales, hasta que un buen día le sucedió algo realmente importante.

A Tim le encantaban los teléfonos y sobre todo le encantaba escuchar la voz del otro lado del hilo cuando alguien llamaba a casa. Cada vez que podía marcaba un numero cualquiera de teléfono y se sentaba a escuchar la cálida voz que decía ; Este numero esta fuera de servicio.

Hasta que un buen día Tim silbó al tiempo que la voz decía la frase y callo de golpe. Esto asombro a Tim. Volvió a marcar otro numero de teléfono, silbó y sucedió lo mismo. Años mas tarde descubría que era capaz de generar silbidos a una frecuencia perfecta de 2.600 ciclos, el tono que indica que el teléfono esta colgado.

De esta forma Tim fue catalogado como uno de los primeros Phreakers de la historia. Tras este descubrimiento algunos ingenieros electrónicos probaron diversas frecuencias y descubrieron que se podían activar y desactivar los contadores de las centralitas y realizar llamadas de larga distancia de forma gratuita.

Basándose en la generación de tonos, con osciladores estables, se creo la primera cajita azul, que fue rápidamente extendida por su buen funcionamiento, y sobre todo porque se podía llamar gratis con ella.

## 8.2 El robo del banco

Uno de los casos mas difundidos, quizás sea el que sigue; dos Hackers tenían como objetivo ganar dinero fácil y de forma rápida. El objetivo así, era una sucursal de Citibank, en nueva York.

Los dos Hackers descubrieron, mientras monitorizaban la Red, que esta sucursal realizaba las transferencias a través de una compañía telefónica, y el sistema empleado era una red X.25.

Descubierto esto los dos hackers decidieron que si podían monitorizar estas transacciones, también podían redirigirlas a otra cuenta. Claro que había que retirar el dinero antes de que se dieran cuenta. Haciendo manos a la obra, buscaron el prefijo de la sucursal. Probaron varios números en serie a partir de un par de prefijos que sabían de antemano, hasta que terminaron por conectarse con varias terminales VAX. Durante un fin de semana se dedicaron exclusivamente a penetrar en ellos.

Después de esto fueron deduciendo terminales hasta quedarse con cinco de ellos. Sabían que uno de ellos era el que controlaba las transacciones. De estas terminales, una , parecía interesante porque tenia un debug o puerta abierta. Les fue fácil entrar en ella, empleando la clave de acceso del fabricante, ya que se ve a nadie se le ocurrió cambiar esta clave.

El sistema al que accedieron contenía menús que los guiaban a través de cuentas bancarias. Después de varias horas de exploración, encontraron un paquete de herramientas que permitía crear directorios y programas. Los dos hackers crearon uno, que interceptaba todas las entradas y salidas del terminal. Después crearon un directorio .. y decidieron que este fichero seria el capturador de las transacciones.

Varios días mas tarde accedieron de nuevo a este terminal, e impresionados vieron como esta unidad

había echo multitud de transacciones en los días anteriores. Descubrieron a su vez que este terminal se conectaba a otra unidad parecida y tras una petición recibía una respuesta, entonces se iniciaba una larga serie de números y letras como pasword.

Los hackers grabaron estos datos y los emplearon días después, generando cientos de transacciones a una cuenta " ficticia " que ellos habían creado. Hasta aquí esto no era mas que una prueba de que sabían los datos de control de cada ordenador. De modo que se tomaron unos días de descanso y planearon el gran golpe.

Días mas tarde abrieron una cuenta en suiza y otras seis en Estados unidos, donde residían. Cada cuenta estaba registrada a un nombre diferente. Cada una de las cuentas tenia una pequeña cantidad de dinero y tras extinguirse la noche, los Hackers pusieron manos a la obra.

Durante largas horas, los dos hackers hicieron turno delante del terminal, respondiendo los acuse de recibo. Al mediodía tenían cerca de 200.000 dólares en su cuenta de suiza y al final de la semana, cada uno se llevo 100.000 dólares en efectivo a casa.

Esto hoy día, es mas difícil de realizar, pero no imposible, la historia parece haverse repetido en Hong Kong en los últimos meses, un Hacker japonés había robado las cuentas de mas de 200.000 clientes de un importante banco de ese país. Pero esta vez fue descubierto.

## 8.3 El primer virus

El primer Virus se le escapo a alguien o " lo soltó " deliberadamente en la Red, causando este un colapso en las comunicaciones. En realidad se trataba de un worn o gusano, como quiera llamarle. El creador se sorprendió de los efectos y tuvo que crear otro programa que anulara las funciones de este primero. Así nació, también el primer Antivirus.

Pero de todo esto se ha escrito mucho y según Paul Mungo y su colega Bryan Clough, el primer virus tuvo lugar el 22 de octubre de 1987. Este primer Virus infecto varios cientos de disquetes. Y en la prensa lo catalogaron como una catástrofe, hasta el punto que se llego a decir que se pedían 2.000 dólares para inmunizar o destruir este Virus.

Los investigadores pusieron manos a la obra y descubrieron el mensaje " oculto ", en realidad no se pedía dinero y como una forma de evadirse o justificarse, el creador del Virus mostraba un teléfono de contacto para poder solicitar lo que entonces se denominaba, " Vacuna ".

Este Virus se llamo Brain y en realidad tampoco era demasiado destructivo, " comparado con los actuales ". El Virus Brain se esconde en el sector de arranque del disco y espera a que el ordenador se ponga en marcha y lea las primeras pistas del disco. Entonces se carga a si mismo en la memoria RAM, como si este fuera un programa de arranque común o BOOT.

El virus Brain es excesivamente largo, comparado con los posteriores virus mas sofisticados, tenia una densidad de 2750 bytes, los cuales no cabian en el sector de arranque. Así, que el Virus hacia dos cosas ; colocar sus primeros 512 bytes en el sector de arranque y almacenar el resto de datos en otras seis pistas del resto del disco. De forma que siguiera una cadena.

Este Virus " conocido como el primero " podía resultar inofensivo a primera vista si el disco no estaba

demasiado lleno, pero a la sazón si este estaba completo, el Virus, que se autoreplicaba, podía borrar algunos datos importantes, cuando este se reescribia en otras pistas del disco.

El Brain también tenia un contador, y trataba de infectar un nuevo disquete cada cierto tiempo. Esto era lo que realmente hacia peligroso al Brain, en manos inexpertas.

La única misión que tenia este Virus era insertar la etiqueta de bienvenida, Brain y ejecutar un proceso automático de reescritura. Pero por aquel entonces los ingenieros le dedicaron mas de una semana, en estudio y para erradicarlo totalmente.

Y ese fue el principio de una nueva generación de micro-programas autoreplicantes que implantarían el terror en los siguientes años, hasta llegar a la actualidad, en la cual se les consideran el mayor " terror de la Red ".

## 8.4 Kevin Mitnick, el nuevo forajido

La historia de Kevin comienza a la temprana edad de 16 años. Corría el año 1980, cuando Kevin rompía la seguridad administrativa del sistema informatico del colegio donde estudiaba. En aquella ocasión, solo se limito a " mirar " los ficheros del sistema y no toco nada.

Al año siguiente. Kevin en compañía de unos amigos, penetro físicamente en las oficinas de COSMOS de Pacific Bell. Esta era una base de datos de control de llamadas, y Kevin y sus amigos robaron algunos manuales del sistema, las claves de seguridad, la combinación de las puertas de acceso al lugar y dañaron otros tantos archivos.

Por ello, después Kevin y sus amigos, " después de que la novia de uno de los amigos los delatara como autores de los hechos " eran condenados a tres meses en un centro de detención juvenil de los Ángeles y un año de libertad provisional.

Pero Kevin solo había hecho mas que empezar. En 1982 Kevin entro 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 mas 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.

Pero como siempre dicen, la leyenda nunca muere y en 1988 protagonizo otra de sus andanzas. Esta vez Kevin cumplió un año de prisión por robo de Software. Todo comenzó cuando durante varios meses, Kevin observo el correo electrónico del departamento de seguridad de MCI y Digital.

Con la ayuda de un amigo, Kevin penetro en el sistema y capturo 16 códigos de seguridad de ambas compañías. Pero del ordenador principal de Digital, Kevin se llevo consigo los ficheros de un nuevo prototipo de seguridad S.O, denominado VMS. Esto fue lo que alerto a los ingenieros de Digital, que rápidamente se pusieron en contacto con la FBI y así fue como comenzó el rastreo hasta dar con Kevin.

En 1992 Kevin salía a la calle y comenzaba a trabajar para una agencia de detectives, que en un principio vieron en el, el perfecto hombre que resolvería importantes " cambios ", pero pronto Kevin penetro en sistemas y mas sistemas y el FBI, determino que era Kevin quien estaba detrás de todo. Pero Kevin escapo esta vez.

Sin embargo es 1994, cuando Kevin conoce, lo que seria su caída mayor. Al estar " prófugo " de la justicia. Kevin no puede dar su identidad en ninguna parte, ya que esta, en busca y captura y como tiene que moverse, Kevin se hace de un portátil y un teléfono móvil, y es así como esquiva en cada ocasión a la policía y al propio FBI.

Como Phreaking, Kevin era un autentico especialista pero necesitaba algo mas. El sabia que existía el peligro inminente de ser detectado muy pronto. Eso lo sabia porque empleaba un teléfono móvil motorola y como todos, estos poseen un software, " oculto " que permite enviar una señal a la central para su localización, pero Kevin sabia que los teléfono OKI, permitían " puentear " esta opción y sabia donde podría encontrar el Software para ello.

Así, la noche del 25 de diciembre de 1994, Kevin había penetrado en el ordenador de Tsutomu Shimomura, el hombre que lo capturaría un año mas tarde, en busca del Software de OKI. Un Software que también era " pirata " ya que Tsutomu era Hacker antes que experto de seguridad.

Nueve minutos después de las dos de la tarde del 24 de diciembre de 1994 Kevin, iniciaba la ardua tarea de entrar en los sistemas de Tsutomu, que estaba ese día fuera de su domicilio. Los tres ordenadores de la casa de Tsutomu en San Diego, California, comenzaron a recibir una serie de instrucciones externas. Kevin trataba de averiguar que relación tenían entre si los tres ordenadores que estaban encendidos ese día y pronto averiguo cual de las maquinas era el centro de la pequeña red local.

Se trataba de una SPARC que había sido detectada en tan solo tres minutos. Después de una pausa, recibía una solicitud de conexión desde una dirección falsa de Internet. El ordenador SPAC contesto con la respuesta adecuada de conexión con la " dirección falsa ".

Kevin ya estaba cerca de su objetivo, pero no respondió a la maquina y en lugar de ello, envío otras 29 peticiones mas seguidas en tres segundos. Con lo que consiguió bloquear la maquina con una ráfaga de datos velozmente transmitidos.

Había conseguido su primer paso.

Después otra de las estaciones SPARC de Tsutomu que se empleaba como terminal, recibió otras 20 solicitudes en no mas de diez segundos. El terminal reconoció cada una de ellas, pero siempre recibió un mensaje de cancelación, con el fin de despistar esta segunda maquina conectada a la red.

Pero mas que despistar, Kevin lo que quería era " capturar " los datos obtenidos como respuesta de estas estaciones SPARC. Estudio cada una de estas respuestas y dedujo que debía añadir 128.000 unidades al numero de respuesta. De esta manera Kevin podía acceder al tercer terminal. Tras esto, Kevin añadió un fichero " oculto " que le permitiría entrar libremente cada vez que lo solicitara, sin tantas complicaciones como esta vez.

Kevin husmeo el disco duro y encontró algo que le interesaba. Era el software del OKI y otros tantos archivos de seguridad que Tsutomu había desarrollado. Y esto fue lo que realmente cabreo e incito al japonés afincado en Estados Unidos, a iniciar una persecución lenta y laboriosa que concluyo el 15 de Febrero de 1995, con la captura de Kevin y su nuevo " Teléfono fantasma ".

## 8.5 El caso del sistema de codificación de videocrypt y el profesor ZAP

El caso mas sonado es quizas el que le sucedió al grupo SKY y su sistema de codificación Videocrypt. Dicho sistema se anuncio como el mas seguro y se creo con la intención de frenar la actividad febril de los piratas, en una época en donde todo se codificaba por métodos analógicos y por tanto eran fácil de clonarse. Careciendo en todo momento de una seguridad absoluta o fuerte.

El nuevo sistema de Videocrypt aumentaba su seguridad ya que se basaba en tecnología digital para la codificación de video. Ademas presentaba una importante novedad,y es que el nuevo sistema de encriptacion se basaría en una tarjeta de acceso inteligente. Un punto fuerte según los ingenieros que lo inventaron. A partir de ahora se podría activar y desactivar cada descodificador a voluntad. Ademas el sistema digital de encriptacion permitía trabajar con algoritmos complejos y estos necesitaban de claves secretas que se albergaban en el interior de la tarjeta electrónica.

Sin embargo no tardarían en descubrir que la orden de activación se definía como una tensión de control sobre el descodificador. De modo que bastaba con cortar una pista de cobre del circuito o Hardware del descodificador para eliminar la función de activación y desactivación del sistema. Y por supuesto el sistema mas fuerte había caído repentinamente.

No obstante se tenia en cuenta dicha posibilidad y rápidamente entro en acción la segunda fase. A partir de ahora el sistema se complicaría aun mas. El algoritmo del embrollamiento se trataría en el interior de la tarjeta y la orden de activación y desactivación del equipo descodificador, ya no seria una simple tensión de control. A partir de ahora se convertiría en una palabra u octeto en forma de respuesta a partir de una palabra mas larga. Dos claves, una pública y otra secreta se encargarían de desentrañar la clave de acceso. Así la clave pública se desenmascaria en el interior del descodificador, mientras que la clave secreta se revelaría en el interior de la tarjeta de acceso.

De esta forma si se pretendía hacer un Hack sobre el sistema seria por vía software a partir de ahora y no por Hardware como había sucedido en un primer nivel de seguridad de este sistema.

Durante un tiempo los Hackers se vieron frenados y nada pudieron hacer. El algoritmo era complejo y utilizaba una palabra de control de varias decenas de bits. Y lo que era peor, estos códigos no eran repetitivos. Puesto que se sabía que las tarjetas de acceso se basaban en el estándar de comunicación ISO 7816, se podían leer las comunicaciones de dicha tarjeta con el descodificador a través de un interface programado. Pero los comandos que iban y venían , en una y otra dirección variaban de forma constante. Sin embargo se constataba que un sistema no podía trabajar con claves aleatorias. De hecho ningún sistema puede hacerlo así. Eso era una esperanza. Rider Shamir fue el encargado de crear el algoritmo nuevo que pondría en jaque a los piratas. El código se denominaba RSA y se creía mas seguro que el estándar americano DES, un algoritmo que se permutaba hasta 16 veces.

Durante un tiempo Murdow durmió tranquilo hasta que un buen día a un estudiante de informática se le ocurrió preguntar a su profesor como funcionaba el sistema de codificación del canal SKY. El profesor le respondió que no lo sabía exactamente, que sentía cierta curiosidad por el sistema y que le había llamado especialmente la atención el hecho de emplear una tarjeta inteligente.

El alumno se encogió de hombros y animo al profesor a que estudiara la forma de revelar el algoritmo del sistema. Entonces el profesor le pregunto cual era la razón para que le invitara a hacerlo. Si la complejidad del sistema u otra razón. Entusiasmado el alumno le contestó que le agradaría ver la serie de Star Trek que emitía dicho canal de pago. El profesor se encogió de hombros y le invito al alumno a que se sentase.

Durante un tiempo las palabras del alumno le rondaron por la cabeza como una obsesión incontrolada. El profesor había desarrollado un interfaz con un pequeño programa para estudiar y leer lo que se avenía entre la tarjeta y el descodificador con la intención de enseñar a sus alumnos como funcionaba el protocolo ISO 7816. Ademas de los códigos de control comunes de este protocolo habían otros códigos hexadecimales que variaban constantemente, pero pronto cayó en la cuenta que ciertos códigos se repetían esporádicamente y que si seguía con detenimiento la cadena de datos, estos se repetían asiduamente a lo largo de un periodo.

Un mes después dio con la clave y tuvo a punto la primera tarjeta electrónica basada en un micropocesador de Arizona Chip, un PIC 1654. El nivel de seguridad del sistema se denominaba nivel 6 y el profesor se sentía satisfecho de haber conseguido abrir el sistema con cierta facilidad.

Al día siguiente de crear la tarjeta se la regalo al alumno invitándole a que viera Star Trek y de paso sirvió como modelo de estudio para toda la clase. Y así fue como empezó una feroz batalla de códigos entre New Datacom, la creadora de códigos de SKY y los piratas.

Como era de esperar dicha tarjeta cayó en manos de otros piratas y pronto los códigos y tablas se difundieron con rapidez. Había quien había visto con buenos ojos un negocio fructífero y pronto miles de tarjetas cloticas invadieron Europa.

Semanas después New Datacom cambio el código 6 al código o nivel 7. Pero pocas eran las variaciones hechas en el sistema, ya que el profesor dio de nuevo con la clave una semana después. Y creo las tablas.

Estas tablas permitían cambiar el numero secreto de la tarjeta, por tanto un mismo algoritmo adoptaba formas diferentes en cualquier momento. Durante mas de un año New Datacom cambiaba esta clave, pero un cambio por esta tabla reiniciaba de nuevo las tarjetas piratas.

Y es que un algoritmo puede sufrir alteraciones con solo cambiar un octeto y eso es lo que hacían, pero el algoritmo era el mismo, solo se cambiaba un par de códigos y estos códigos estaban disponibles en una tabla ya preparada. Con ayuda de un reprogramador era posible activar de nuevo cada tarjeta después de cada cambio de código. Entonces fue cuando New Datacom introdujo una novedad en sus códigos. Cada tarjeta poseía un numero de identificación y se podía modificar dicho numero por vía aire y a través de Software. Ademas los PIC podían ser modificados externamente y pronto se supo que todos los PIC ya tenían un numero clave de serie. Los ingenieros de New Datacom adquirieron algunas de estas tarjetas piratas en el mercado negro y las estudiaron con detenimiento y pronto encontraron el fallo.

La respuesta fue modificar el Software de la tarjeta para que respondiera de otra forma. De esta forma los piratas tenían que modificar sus tarjetas si querían seguir vendiendo. una vez que se logro el proceso, se introducía la contramedida electrónica ECM, junto con los códigos secretos y se bloqueaban las tarjetas piratas con esta medida electrónica. paradójicamente cayeron todas las tarjetas y el código ECM se había convertido en una forma mas de anular estas tarjetas sin tener que cambiar los códigos de forma continuada.

Ya que había que tener en cuenta que las tarjetas oficiales tenían que seguir funcionando sin tener cortes en su funcionamiento. Pero el protocolo 7816 permitía ciertas modificaciones de Software y seguir

funcionando.

Paralelamente los piratas y como en todo cada uno tenia su misma versión de la misma idea. Abrir y engañar al sistema mas fuerte anunciado hasta el momento. Así otra de las formas de hacerlo era modificando el Software del programa que albergaba el microprocesador de control de comunicación con la tarjeta. Se escogía la instrucción que daba autoridad para habilitar otro chip especifico encargado del desembrollamiento de la señal de video y se anulaba o se simulaba independientemente de la respuesta de la tarjeta de acceso oficial. Para ello se cambiaba dicho microprocesador por otro que estaba trucado. A este método lo bautizaron con el nombre de Kentuky fried chip y duro mas o menos un año hasta que los ingenieros de New Datacom modificaron el programa de dicho chip, pero eso es algo que solo son rumores ya que se cree que todavía hoy funciona. Lo unico engorroso que tiene es que hace falta modificar el descodificador y no siempre es posible hacerlo, ya que un usuario puede estar a miles de kilómetros del taller.

Por ello se optaba mas libremente por la adquisición de una tarjeta clonica. Era menos complicado y ademas se podía enviar por correo. El unico inconveniente es que debía reprogramarse cada cierto tiempo.

Pero pronto pasaron a la versión 08 y 09 y fue cuando hubo un gran paron y surgieron nuevas ideas para hacer un Hack definitivo que nunca fue, del sistema mas emblemático de todos.

Así nació el Phoenix Hack.

El resurgir del ave, así se rebautizo la nueva promesa que se mantuvo en secreto durante al menos dos meses de constantes pruebas en un laboratorio a las afueras de Hannofer. La nueva tarjeta pirata funcionaba pero presentaba ciertos problemas cuando llevaba algún tiempo insertada en el descodificador. En un principio la existencia de esta tarjeta solo era un rumor, pero los medios de información ya se habían hecho eco de ello y publicaban extensos artículos rememorando la tarjeta pirata versión 07 que había sido presentada en una feria de Francfort en el año 94, por un grupo de ingenieros. Pero nada mas lejos de la realidad. La vieja tarjeta versión 07 denominada Hipercrypt en aquel momento se había presentado junto al Kentuky Fried chip.

Y volviendo a los nuevos Hacks de la versión 08 y 09 cabe destacar que se apuntaron al éxito numerosas empresas autorizándose el dominio del mismo, pero lo cierto es que estas tarjetas siempre han sido creadas por una misma persona, al contrario de lo que se pretende hacer creer en un mundo donde se falsean los datos.

El profesor de informática, cuyo apodo es Zap, tenía en jaque a todo un poderoso centro de investigación de seguridad como New Datacom. Su nueva tarjeta basada en dos poderosos chip PIC 1684 estaba lista para funcionar.

Paralelamente al Phoenix otras empresas seguían fabricando ***« cartones electrónicos «*** como se les denominaban en aquellos gloriosos días. Ya que no todos los canales que estaban codificados con el sistema de codificación de Videocrypt no trabajaban con el mismo código, todavía existían canales que funcionaban bajo el código 07 y el profesor ZAP vendió sus códigos con el nombre de SEASON 7 ***( este programa fue actualizándose hasta alcanzar la versión Season 13 ).*** El programa en un principio se pagaba como si se trataran de lingotes de oro y así fue como varias empresas fabricaban sus propias tarjetas piratas. Empresas tales como Megatek e Hi - Tech consiguieron colocar en el mercado miles de estas tarjetas con códigos 07.

Mas tarde cuando los códigos cambiaron a 08 y 09, estas empresas habían negociado con el profesor ZAP y tenían lista sus propias versiones. Pero el profesor ZAP era cauto y les advirtió que no lanzaran todavía el producto ya que según el todavía existía un fallo en los códigos a pesar de que funcionaba bien.

Las nuevas tarjetas se lanzaron al mercado y cayeron fulminadas unas dos semanas después. Por ello la confianza degenero en miedo y ya nadie compraba tarjetas piratas. New Datacom había pasado decididamente al código 09.

Mientras el código 09 maduraba en el laboratorio del profesor ZAP, otras empresas lanzaron otros Hacks basados en tarjetas oficiales. Esto inspiraría mas confianza al comprador. El sistema se basaba en bloquear los códigos ECM de borrado de tarjeta mediante un interface electrónico entre el descodificador y la tarjeta legal u oficial. A este circuito se le bautizo con el nombre de Bloquers y aunque surgieron varios de ellos, ***( El mas destacado fue la Sunbloquer de Hungría por ser la mas eficaz )*** uno de ellos recibió el nombre de Lázaro. Como una alevosía a la resucitación de los piratas.

Los bloquers permitían activar tarjetas caducadas y ademas impedían que estas se desactivaran desde el centro de control de abonados. El sistema funciono bien hasta que los ingenieros de New Datacom contraatacaron con nuevos códigos ECM ***« control de medida electrónica «*** para desactivar definitivamente las tarjetas legales. el sistema se basaba en una instrucción secreta que fundía el fusible de lectura de la tarjeta chip.

Y así fue como se impuso de nuevo la nueva tarjeta pirata versión 09, después del desastre de la desactivación de mas de 100.000 bloquers en un solo día.

La nueva versión 09 también poseía códigos variables y tablas. El algoritmo seguía basándose en la norma RSA y solo se había complicado en un octeto mas de instrucción. Ademas existían códigos que no actuaban sobre el encriptamiento o el algoritmo, pero estaban hay y servían para algo, pero no se sabía para que exactamente.

Mientras tanto el código 07 se servia en un servidor de Internet y uno podía fabricarse un interface que se conectaba al ordenador y el descodificador y podía ver aquellos canales de videocrypt que conservaban los códigos 07. Cuando había un cambio de claves, solo tenias que probar con varios números desde el ordenador y rápidamente se activaba la tarjeta.

Probablemente el sistema de Videocrypt haya sido el sistema mas pirateado del mundo y el que mas cambios ha conocido. y aun hoy a estas fechas en las que se escribe este libro sigue la dura lucha entre los piratas y New Datacom.

Durante varias semanas la nueva tarjeta del profesor ZAP funciono correctamente, pero eso solo era una maniobra de New Datacom que tenía preparada una coartada. La nueva tarjeta oficial tenía mucha mas memoria ROM interna y mucha mas memoria RAM. Lo cual en un principio desconcertó al profesor ZAP. Pero NEW les tenía preparado una sorpresa.

Como era habitual, los cambios de códigos se efectuaban siempre el día de navidad y la fecha estaba próxima. Cuando por fin llego el día todas las tarjetas piratas reaccionaron de forma extraña. Solo descodificaban por momentos y presentaban extraños mensajes en la pantalla del televisor. Ya que estas tarjetas no poseían fusibles internos que desactivar y eran inmunes a los ECM, NEW decidió que la nueva versión debía ser cuasi-aleatoria y que debía permitir modificar los códigos cada 48 horas.

Y eso fue lo que sucedió.

Las tarjetas piratas se volvieron locas y de nuevo la incertidumbre reino en este peculiar universo. Pero el profesor ZAP también tenía su coartada.

Una nueva tarjeta denominada Card Mate estaba en proceso de creación. Ahora se aumentaría la memoria interna y ademas esta nueva tarjeta seria reprogramable a través de un teclado al tacto. Y seria tan sencillo hacerlo como introducir un numero de telefono.

La nueva Card Mate estaba basada en un potente chip de Dallas DS 5002 y ademas estaba preparada para nuevos códigos futuros y así sucedió.

Un año después New Datacom decidió cambiar a la versión OA. Ridher Shamir cobro una importante suma por modificar su algoritmo RSA de seguridad, pero el capitán ZAP le estaba esperando.

Cuando hubo el cambio de la versión 09 a la versión OA, solo se hubo que reprogramar las tarjetas Card Mate. Y fue así como el capitán ZAP gano la batalla.

## 8.6 Otros casos de Hacking no menos importantes

Filmnet, un canal de cine las 24 horas, fue uno de los primeros canales de televisión vía Satélite que decidió codificar su señal allá por el año 1986. Concretamente el 1 de Septiembre, con un sistema de cifrado basado en tecnología analógica. Durante los siguientes cinco años conoció hasta 6 variaciones del sistema.

La primera versión era extremadamente sencilla y fácil de clonar, por lo que fue uno de los primeros sistemas en ser pirateado con éxito, después del sistema de codificación de SKY en ese mismo año. Ambos canales empleaban codificaciones similares basados en las mismas bases y fundamentos. Pero el OAK ORION que así se llamaba el sistema de codificación de SKY antes de adoptar el sistema de Videocrypt, no conoció modificación alguna a pesar de estar clonado con éxito.

El 23 de marzo de 1987, se decide cambiar algunas secuencias en la codificación del sistema de Filmnet, denominado SATPAC, con la esperanza de dejar fuera de servicio los descodificadores piratas. Sin embargo el intento fue en vano, ya que un simple modificación volvía a renacer el descodificador pirata.

El 24 de Diciembre de 1989 Filmnet cambia de nuevo sus códigos y es que parece que la fecha de navidad es siempre la propicia para estos cambios, como si de un regalo de navidad para los piratas se tratara. Pero de nuevo el intento era fallido, puesto que se volvieron a cambiar los códigos nuevamente el 11 de mayo de 1990, de nuevo en diciembre de 1990, en enero de 1991 y en marzo de ese mismo año.

Hi - Tech, con sede en Inglaterra, era la empresa encargada de fabricar masivamente los descodificadores piratas y algunos medios de publicaciones electrónicas, publicaron sus propios descodificadores.

Ese mismo año filmnet introdujo una codificación del audio digital y durante unos años los piratas vieron frenados sus deseos, pero la llegada de potentes chips en el sector de la electrónica de consumo, hicieron posible la apertura del sistema.

Pero quizas el caso mas sonado fue y será la masiva clonación del sistema adoptado por Canal Plus Francia y sus sistema de codificación DISCRET 1, que mas tarde se convertiría en la versión 12. De este sistema se fabricaron mas de un millón de descodificadores piratas y de nuevo la empresa inglesa Hi - Tech estaba detrás de todo esto.

Este sistema también fue objeto de estudio y publicado en las revistas de electrónica mas prestigiosas del

momento. El sistema de codificación analógica, también permitía variaciones de códigos, pero los Hackers siempre estaban atentos y ya habían predecido dichos cambios con anterioridad.

Finalmente Canal Plus adopto un sistema digital mas seguro, que puso fin a la piratería mas grande jamas conocida.

Un caso parecido sucedió con el sistema SAVE de la BBC, que se estaba empleando en un canal hardcore. En esta ocasión no se empleaban códigos y era fácil de clonar y es que durante un tiempo en el que solo, reinaban los sistemas de codificación analógicos, la polémica estaba servida.

Con todo esto quiero hacer especial hincapié en lo referente a seguridad. Es un factor muy importante, pero que no siempre se consigue. Volviendo a los códigos RC5, IC2 o el protocolo ISO 7816, cabe destacar que si estos códigos hubiesen sido absolutamente secretos en vez de públicos, probablemente hoy día estarían disponibles en algunas publicaciones y en algún servidor de Internet.

Con lo cual concluyo que estamos ante un factor importante pero que no siempre se logra el objetivo. Ya que por el momento sigue la batalla por el dominio y la seguridad.

# Capitulo 9

# Software gratis en Internet

Este es un capitulo critico, ya que da la impresión de querer mostrar el lado del Crackeo de Software, pero no es así. Por cruda que parezca la realidad, para conocer al Hacker y a todos sus clanes descendientes, debemos conocer sus trucos, sus hazañas y compartir todos sus conocimientos. Solo así comprenderemos mejor todo este rol. Usted pensara que aquí le revelaremos donde están los programas gratuitos en Internet, quizás sea esto lo que voy a hacer a continuación, aunque en realidad lo que voy a explicar es como convertirlos en " accesibles ", o mejor dicho como los convierten en accesibles.

Pero que quede bien claro que lo que voy a revelar esta basado en mis experiencias, para mejorar la protección del software, a partir de programas Shareware y de Evaluación. Esto forma parte de un proyecto personal para crear un sistema de registro y de antipirateria para el Software que esta siendo reventado impunemente.

Después de atajar los largos caminos que debe recorrer el Hacker hasta hacerse con el sistema para detectar intrusos, fallos o incluso códigos. Nos llega la hora de emplear nuestros conocimientos, que sin emplear herramientas para ello, podremos " romper " cualquier programa " caducable " de modo que poner en practica mi idea, podría estar entre el delito y la experimentación.

Por otro lado, me cuesta creer que a los programadores se les ha escapado las ideas mas simples, pero ahí esta.

## 9.1 Los programas de evaluación

Normalmente existen WEB " muy visitadas por cierto " que ofrecen programas Freeware y Shareware para sus evaluaciones. Los primeros estarán siempre disponibles en nuestro ordenador dado que el autor no ha introducido ningún método de protección en los principales ficheros de arranque, esto esta bien fundamentado ya que al autor lo que realmente le interesa es difundir su programa, que suele ser mas bien modesto y básico en cuanto a funciones.

Los Shareware, que son programas completos y mas complejos, sin embargo ya precisan de registro pasado un tiempo de evaluación que oscila entre los 15, 30 o 45 de prueba, tras los cuales el programa caduca y deja de funcionar. Esto es así por que dichos programas han sido creados para su comercialización,

pero para vender un producto, primero se dejara probar su funcionamiento y entorno.

Los métodos para hacer caducar estos programas Shareware son muy variados y depende de la empresa que los diseñe, el que posean mayores o menores medidas de seguridad. Así, para programas demasiado caros se limitan algunas funciones como la de “salvar “ o “ exportar “ por ejemplo. De esta forma se puede probar el funcionamiento del programa, pero no salvar nuestro trabajo, lo que despierta la furia por un lado y el interés de adquirir el producto por otro.

Pero algunos de estos programas son demasiado caros y hay que buscar otras formas de trabajar con ellos. Para ello hay que saltarse algunas reglas.

Otros Shareware están limitados al numero de usos, esto es, se descuenta un uso cada vez que se abre el programa. Estos dos últimos son los mas difíciles de Crackear, sin embargo como se suele decir, quien invento la ley, invento también la trampa.

## 9.2 Los primeros trucos

Hasta ahora si un programa caducaba a los treinta días, lo mas fácil era dar marcha atrás al reloj para alargar este tiempo. Solo de esta forma, desde el setup de arranque, al cambiar la fecha uno podía disponer del programa un tiempo invariable. Por ello surgieron otras medidas de seguridad, como la limitación de usos.

Algunos programas como el Winzip 6.2 se basan en escribir el numero de usos y los días en el fichero INI. Algo habitual hasta ahora. Si accedemos hasta este fichero y modificamos ambos datos, conseguimos que este programa siga funcionando indefinidamente.

Por ello, los Crackers en un principio buscan los ficheros INI, para modificarlos, algo que hasta la fecha era tan valido como atrasar el reloj. Pero los programadores se dieron cuenta del “ trueque “ y decidieron repartir estos datos de control entre los ficheros INI y REG. De esta forma los datos compartidos son mas difíciles de localizar y además pueden estar multiplexados o encriptados.

Pero, sigamos adelante con los trucos.

## 9.3 Cuando arranca un programa

Normalmente se hace pinchando sobre el icono del programa, si este esta en modo acceso directo desde el escritorio. Al hacer esto el Shareware busca primero los datos o lee la fecha de la memoria del ordenador, la compara con los datos de los ficheros INI, REG o DLL en algunos casos, y procede a añadir la nueva fecha a la entrada de registro.

Después de esto se proceden a cargar los módulos plugins, DLL y los necesarios para abrir el programa. Pero si la fecha es superior a la establecida en el fichero de tiempo, el programa no ejecutara la rutina de apertura.

Para que esto no suceda o bien se retrasa el reloj o bien se localiza la fecha tope y se cambia por otra

superior. Pero esto solo era valido hasta la fecha, ya que Macromedia y Adobe por ejemplo han creado un nuevo sistema Shareware DSS basado en técnicas de detección de manipulación de datos.

Tratar de cambiar cualquier dato en cualquiera de los ficheros de arranque, solo hará que el programa detecte el cambio y no ejecute nada. Si retrasamos el reloj, el programa detectara un cambio " no lógico " de fecha y bloqueara el contador Shareware invalidando el programa.

Por ello si tenemos por ejemplo el programa Fireworks Tryout y lo instalamos el día 10, este caducara 29 días después. Si modificamos el reloj adelantando tres días, el contador indicara que quedan 26 días, pero si retrocedemos 1 día, el contador se bloqueara y solicitara el numero de serie, para desbloquear la llave de bloqueo.

Este nuevo contador se esta implantando masivamente por las grandes multinacionales, para " parar " el truquillo del reloj.

## 9.4 Siguiendo con los trucos

El siguiente paso es registrarse y para ello debemos rellenar un formulario y comprar el programa, para que el autor de este nos remita la clave de desbloqueo. Generalmente estas claves son excesivamente largas, de hasta 24 cifras en el caso de Macromedia.

Los Crakers emplean " la fuerza bruta " para la creación de claves, pero el método mas sencillo es buscar un amigo que haya comprado el mismo programa y solicitarle el numero de serie. Este método es el mas empleado hasta ahora, pero no siempre se tiene ese amigo al lado que posee el ultimo programa de diseño.

Por ello, lo básico es acceder a una pagina Cracking y buscar el numero de serie, pero de forma decepcionante no siempre encontramos la que realmente necesitamos.

Sin embargo existe una posibilidad bastante empleada por los Crackers y es que al copiar un programa original, este se modifica ligeramente a través de otro " controlador " Crack que elimina las secciones de bloqueo y numero de serie encriptada. Por ello cuando instalamos un programa pirateado, a menudo solo es necesario introducir una clave cualquiera, esto es así, ya que el programa esta bien Crackeado.

Los programas que permiten estas operaciones están disponibles en paginas basadas en Hacking, pero las BBS están fulminando este tipo de paginas a una velocidad pasmosa, ya que quieren erradicar definitivamente el pirateo del software.

Otro truco es emplear métodos de " Carding " esto es utilizando un numero de tarjeta ajena para comprar el Software. Existen miles de números de tarjetas VISA interceptadas en la red cuando se han efectuado compras con estas. Que aunque este tipo de mensajes esta encriptado, existen Sniffers capaces de desencriptar estos números.

## 9.5 El truco de Simply

El truco de Simply es hasta la fecha el mas sencillo y el mas elegante hasta la fecha. Este truco se puede

hacer de forma manual o automática, esto es, a través de Software o Hardware.

Hasta la fecha en que se están escribiendo estas líneas, este truco ha conseguido burlar perfectamente cualquier tipo de contador DSS o similar, ya que se trata de " congelar " el tiempo del reloj fuera de los ficheros INI y no registrarlos.

Dicho de otra manera, antes de arrancar el sistema operativo hay que introducirse en la BIOS y modificar la fecha, guardando siempre relación. Esto quiere decir que si se bloquea el día 5, el ordenador siempre deberá registrar que esta en el día 5. Como se sabe, los contadores pueden detectar cambios inferiores de fecha, pero no igualdades, y como hasta la fecha no se controla la hora y los minutos, el truco esta servido.

Con este método han caído todos los últimos programas del mercado hasta la fecha, palabra.

**Nota : No se pretende promocionar el truco Simply ni ninguno de los expuestos en este capitulo, de modo que quien lo ejecute quedara a responsabilidad suya el " trequear " el Shareware y de nada responde el autor o autores de esta obra, el empleo de este truco u otros descritos. Al no existir copia ni animo de lucro, no existe piratería. Queda dicho.**

# Capitulo 10

# Criptografía

Desde tiempos inmemorables siempre se busco, la forma de cifrar o " ocultar " un mensaje mediante técnicas reversibles, pero que a su vez volvían los textos ininteligibles. Cifrar un texto o mensaje, conlleva a que si este es interceptado por alguien, el texto no pueda ser descifrado sin la clave correcta.

Los sistemas criptográficos se han extendido como la pólvora en la Red, buenos y malos emplean la criptografía para " esconder " sus mensajes. Los Crackers mas hábiles, por otro lado, tratan de demostrar que también los sistemas criptográficos mas modernos caen ante ellos.

Una buena muestra de ello es el Crack del código DES en 56 horas. De modo que la polémica esta servida. Pero por otro lado tenemos que...en su día se trataron sistemas de criptografía o cifrado, pero en señales de televisión, refiérase a Hackers, piratas tecnológicos. Donde se exponían los diferentes sistemas de cifrado reversibles.

Al igual que sucede con la televisión de pago, las comunicaciones, los programas y la propia Red de Internet, debe poseer una seguridad que proteja la intimidad de los datos.

Hasta ahora hemos comentado " se comento en el primer libro " que los canales de televisión se pueden proteger mediante modificaciones en la señal compuesta. Estos procesos de encriptacion de componentes son reversibles con el fin, naturalmente, de obtener la información en clara en el lado autorizado para tal fin.

Este mismo proceso debe seguir el campo de la informática, pero se detiene uno a pensar que aunque la palabra seguridad habita en todos los lugares, poco se parecen ambos métodos empleados, naturalmente por ser de diferentes naturalezas. Un canal de televisión esta compuesto por ciertas funciones analógicas y unos componentes indicativos de la señal. Todos estos componentes pueden ser sustituidos por otros elementos o transformados. A esto se le llama proceso de enmascaramiento o encriptacion.

En la informática, aunque no existan los mismos elementos de una señal de video, también es posible encriptar la información. A este proceso se le denomina criptologia.

Criptologia es el arte de transformar un mensaje claro en otro sin sentido alguno. Este mensaje debe ser reversible en el otro extremo igual que si no hubiera sucedido nada. Es mas fácil encriptar un texto que una señal de video, pero siempre resultara mas complicado desencriptar el texto que la señal de video. En una señal de video siempre puedes ver que sucede, pero en un texto normalmente no puedes adivinar nada, ademas los ficheros aparecerán encriptados y no podrán ser leídos por comandos estándares.

Pero la criptologia o los programas criptográficos no son toda la seguridad que se pretende crear. Existen a su vez diversos complementos que aumentan la seguridad de un terminal informático.

Un ordenador es un equipo sofisticado que procesa datos, y como los descodificadores puede tener palabras de acceso que pueden bloquear el sistema si no se conocen. En los descodificadores esto, se llama, bloqueo paterno, mientras que en los ordenadores es una clave de acceso para empezar a trabajar con el. En ambos equipos se debe introducir una clave o contraseña antes de iniciar la sesión. en los descodificadores suelen ser claves de cuatro dígitos por la baja seguridad que necesitan. Normalmente estas claves es para evitar que alguien ajeno a la familia manipule el descodificador o receptor. Pero en los ordenadores, como se guardan valiosos datos, la seguridad debe de ser mayor.

En estas circunstancias debemos saber que un terminal de ordenador posee dos puertas de acceso al corazón del sistema. Uno, es a través del teclado, que es la puerta de introducción de datos mas usual y la otra puerta, es el moden que comunica al ordenador con el mundo exterior gracias a Internet.

En el primer caso, se debe introducir una contraseña de mas de cuatro dígitos si se desea, para poder acceder al sistema operativo. Esta protección es valida, para que nadie pueda entrar en nuestro ordenador desde el teclado sin nuestra autorización. Este método es ciertamente seguro para nuestra intención.

Pero en la Red existen peligrosos Hackers capaces de hacer cosas impensables, por ello la puerta segunda, requiere un mayor grado de seguridad. Normalmente, en base el buen entendimiento entre dos ordenadores, dos terminales deben poseer un inicio y salutación para que dos terminales se identifiquen y puedan trabajar conjuntamente. Es algo así como un telefono, si este no marca un numero definido por el usuario, jamas nos pondríamos en contacto con la persona deseada.

En los ordenadores ocurre exactamente lo mismo.

Cada ordenador debe tener asignado un nombre de identificación y ademas debe ser capaz de dialogar con el otro terminal, en los extremos mas simples como enviar un saludo, acuse de recepción y otros detalles. Sin estos detalles un terminal no podría identificar nunca al del otro extremo, ni dejar constancia de ello. De esta manera se controla el trafico y se evitan nudos indeseables en las comunicaciones. Pero esta puerta hasta ahora no poseía mas seguridad que los números de identificación del terminal a la dirección que le corresponde.

Y estos números son fácilmente reconocibles como se conoce el numero de telefono de cada persona

gracias a la guía telefónica.

Los Firewalls o muros de fuego, son la solución para tapar el agujero de esta segunda puerta. Este programa puede identificar quien solicita el servicio de nuestro ordenador ademas e impedir que entren datos a nuestro ordenador. Por otra parte estos firewalls pueden reconocer comandos dañinos o peligrosos para nuestro terminal.

Sin embargo, eso no termina de cuestionar la seguridad total.

Podemos impedir que un intruso entre en nuestro sistema, pero que sucede cuando tenemos que enviar algo a otro punto de la red. Inevitablemente nuestro trabajo corre peligro de ser capturado por alguien externo a nuestro deseo. El programa PGP de Zinmerman es una solución muy buena a nuestro problema. Nuestro terminal ademas de velar por la seguridad de las dos puertas hacia el exterior, debe ser capaz de generar archivos ininteligibles por cualquier otro ordenador remoto que no tenga la autorización correspondiente.

Estos programas criptográficos son capaces de encriptar textos u otra información, gracias al empleo de algoritmos de encriptacion altamente seguros. Podemos encontrar varios sistemas empleados y los vamos a tratar a continuación.

## 10.1 Criptografía

Criptografía significa literalmente " *escritura secreta* ", es la ciencia que consiste en " transformar un mensaje inteligible " *en otro que no lo sea en absoluto* ", para después devolverlo a su forma original, sin que nadie que vea el mensaje cifrado sea capaz de entenderlo.

Esta es la definición mas correcta de la criptografía, ya hemos comentado porque debemos echar mano de ella, y ahora vamos a explicar que sistemas existen y de que forma se efectúan los mensajes criptográficos. Los Hackers los muy habilidosos para descifrar estos textos, pero lo cierto es que hace falta poseer un buen programa para poder descifrar incluso mensajes cifrados de forma sencilla.

Existen dos tipos de criptosistemas, simétricos y asimétricos. Los sistemas simétricos, son sistemas de cifrado basados en " *claves secretas* ", estos, emplean la misma clave para encriptar y desencriptar el mensaje o los datos de control del descodificador. Los sistemas asimétricos, sin embargo, operan con dos claves distintas. Emplean una " *clave pública* " para encriptar y otra " *clave secreta* " para desencriptar. Este cifrado es mas complejo y por tanto posee un mayor nivel de seguridad.

Los sistemas de cifrado simétricos, como se habrá intuido son mas débiles que los sistemas de cifrado asimétricos, esto es así, porque ambos, emisor y receptor deben de emplear la misma clave, tanto para el proceso de encriptacion como para el proceso de desencriptacion. De esta forma esta clave debe ser

enviada a través de un medio de transmisión. Un Hacker podría leer esta clave y emplearla para desencriptar el mensaje. Si ciframos esta clave con otra clave, siempre estaríamos igual, ya que la ultima clave revelaría siempre la clave oculta. Sin embargo los sistemas de cifrado asimétricos, al emplear distintas claves, permite el uso de medios de transmisión poco seguros.

Después de estos sistemas de cifrado enunciados, podemos encontrar otros no menos importantes, que siempre se han empleado para cifrar textos o mensajes. Estos sistemas de cifrado son útiles para ordenadores y equipos de impresión de textos. Los sistemas de cifrado simétrico y asímétricos son sistemas útiles para encriptar datos e información digital que será enviado después por medios de transmisión libres.

Pero el texto siempre se cifro de alguna manera, y aquí también surgen grupos de interés. Podríamos hacer una división en dos grandes familias. En primer lugar tenemos los *" métodos clásicos "* y en segundo lugar *" los métodos modernos "*. Es obvio que sabemos a que nos referimos. Los métodos clásicos son aquellos que existieron desde siempre y son métodos desarrollados para cifrar mensajes escritos a mano o en maquinas de impresión. Los métodos modernos son los ya mencionados sistemas simétricos o asímétricos.
Los métodos clásicos se basan en la sustitución de letras por otra y en la transposición, que juegan con la alteración del orden lógico de los caracteres del mensaje. Así a los métodos clásicos les han salidos dos formas de cifrado, denominados grupos, que son *" métodos por sustitución "* y *" métodos por transposición "*.

*Los métodos por sustitución son aquellos que cambian palabras por otras, esta simple forma de cifrar siempre ha obtenido buenos resultados.*

*Los métodos por transposición son aquellos que alteran el orden de las palabras del mismo mensaje.*

Los métodos modernos se basan en combinar secuencias de dígitos creados de forma aleatoria con los dígitos del mensaje, mediante puertas lógicas, en el caso de los módulos PRG sencillos. Otros emplean algoritmos matemáticos de gran complejidad para permutar mensajes de cierta longitud de bits.

Dentro de los métodos clásicos podemos encontrarnos con varios sistemas como los que siguen a continuación ;

*Cifrado Cesar o monoalfabetico Simple.*
*Cifrado monoalfabetico General.*
*Cifrado por sustitución polialfabetica.*
*Cifrado inverso.*
*Cifrado en figura Geométrica.*

*Cifrado por filas.*

De los seis sistemas de cifrado mencionados los tres primeros están basados en los métodos por sustitución y los restantes están, obviamente basados en los métodos de transposición. Explicaremos cada uno de ellos y veremos que efecto de cifrado se obtienen en los mensajes.

*El sistema de cifrado Cesar o monoalfabetico simple :* es un método extremadamente simple y fue empleado por los romanos para encriptar sus mensajes, de hay el nombre de Cesar, ya que fue en su reinado cuando nació este sistema de cifrado. Este sistema de cifrado se consiste en reemplazar cada letra de un texto por otra que se encuentre a una distancia determinada. Se sabe que Cesar empleaba una distancia de 3, así ;

Sustituir A B C D E F G H Y J K L M N Ñ O P Q R S T U V W X Y Z
Por D E F G H Y J K L M N Ñ O P Q R S T U V W X Y Z C B A

Así el mensaje El Hacker acecha de nuevo, quedaría de la siguiente manera ;

HÑ KDFNHU DFHFKD GH PXHYR

*El sistema de cifrado monoalfabetico general ;* es un sistema que se basa en sustituir cada letra por otra de forma aleatoria. Esto supone un grado mas de complejidad en el método de cifrado anterior. Un ejemplo seria la siguiente ;

Sustituir A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z
Por Z C Q V A J G Ñ W N FB U M R H Y O D Y X T P E S L K

Y empleando el mismo mensaje anterior quedaría de la siguiente forma ;

AF ÑZQNAO ZQAQÑZ VA UXATR

*El sistema por sustitución Polialfabetica ;* es un método que emplea mas de un alfabeto de sustitución. Esto es, se emplean varias cadenas de palabras aleatorias y diferentes entre si, para después elegir una palabra distinta según una secuencia establecida. Aquí nacen las claves secretas basadas en números. Este sistema es algo mas complejo que las anteriores y a veces resulta difícil descifrar mensajes cuando empleamos mas de diez columnas de palabras aleatorias. Un ejemplo de ello es lo que sigue ;

Sustituir A B C D E F G H Y J K L M N Ñ O P Q R S T U V W X Y Z

Por 1/ F Q R A L K Z S J Ñ M Y T Y V D B E W V N O C X H P G
2/ G A W H V M U Y F Q L B R C J N D S K T Ñ P Z O Y X E
3/ C Ñ O G D Q H A R P Y T X E W V B M V L Y F S N Z K J

Con una clave 2-3-1, el mensaje seria así ;

HY SGOMHM FWDRVAF HD YPDCJ

*El sistema de cifrado inverso ;* es quizas una de las formas mas simples de cifrar una imagen y es probablemente reconocida por todos nosotros. Es normal escribir del revés cuando estamos aburridos, pero lo cierto es que este es un sistema de cifrado. La forma de hacerlo es simplemente escribiendo el mensaje al revés.

El hacker esta al acecho *( oveun de ehceca rekcah le )*

*El sistema en figura geometrica ;* ya es mas complejo que la versión anterior. En esta ocasión el mensaje ya se empieza por escribir siguiendo un patrón preestablecido y se encripta siguiendo una estructura geométrica basado en otro patrón. Este último patrón puede ser verdaderamente complejo según la extensión del mensaje escrito y la forma de seguimiento de la linea. Un ejemplo simple seria el que sigue ;

El HAC
KER ESTA
AL ACE
CHO

Patrón de cifrado ;
Mensaje cifrado ; ECALHKAHOACRECEATSE

*El método por transposición de filas ;* consiste en escribir el mensaje en columnas y luego utilizar una regla para reordenarlas. Esta regla elegida al azar será la clave para cifrar el mensaje. También aquí es importante saber la clave secreta para poder descifrar el mensaje. En esta ocasión el mensaje puede estar fuertemente encriptado si se emplean textos relativamente largos. Un buen ejemplo sencillo es el que sigue ;

| | | |
|---|---|---|
| ELHACK | Si la clave es 6 3 1 5 4 2 | KHECAL |
| ERESTA | | AEETSR |
| ALACEC | | CAAECL |

CHO OCH

Como hemos podido ver, todos los métodos criptográficos clásicos emplean la misma clave para cifrar y descifrar un mismo mensaje. Con la llegada de los ordenadores, la resolución de estos sistemas se torno prácticamente trivial y por eso han surgido nuevos métodos de encriptacion mas trabajados y seguros. Algunos de ello también basados en claves secretas, cuya computación es prácticamente inalcanzable o bastante compleja.

Tal como se ha dicho los métodos modernos son mas complejos de elaborar y un buen ejemplo de ello se puede ver en el capitulo 11 de este libro, ademas de los ordenadores las tarjetas de acceso electrónicas, son capaces de trabajar con estas encriptaciones por la elevada velocidad de computación que presentan. Al estar basados en complejas transformaciones matemáticas de una secuencia, es indispensable disponer de memoria volátil y capacidad de procesamiento. Estos sistemas de cifrado modernos, son capaces de cifrar palabras de mas de 128 bits y normalmente se cifran en bloques.

Aunque aquí no vamos a detallar de nuevo estos sistemas criptográficos si vamos a enumerarlos, por supuesto los mas importantes, empleados en la red de Internet. Para ello vamos a dividir la situación en tres grupos, uno que nombrara los sistemas de cifrado basados en claves publicas, otro grupo de cifradores basados en claves secretas y un último grupo mas reciente y empleado en la televisión digital, los métodos empleados en algoritmos.

Sistemas de cifrado de clave pública ;

* *RSA*.....es quizas el sistema de cifrado mas empleado en la actualidad. Este sistema es el elegido para trabajar con los códigos del sistema de codificación Videocrypt, algoritmo que el Capitán Zap consiguió romper. Aunque después de ello se dice que sigue siendo el sistema de cifrado mas fuerte del mundo, existe una anécdota que hace pensar lo contrario. En 1997 un chaval de 16 años, un cerebro de la informática, fue capaz de romper el código RSA con una longitud de 200 bits en menos de cuatro horas. El sistemas RSA se basa en la multiplicación de números primos, por lo que conlleva grandes operaciones matemáticas. Fue inventado en 1977 por Rivest, Shamir y Adelman, de hay el nombre RSA. También es cierto que el sistema de cifrado comentado ha sido modificado por sus inventores aumentando el grado de seguridad. El sistema permite utilizar documentos de diferentes tamaños ; 512 bits, 768 bits, 1029 bits, 2048 bits...

* *Diffie - Hellman*....Data de 1976 y se emplea fundamentalmente para el intercambio de claves. Como ya se ha comentado y se comentara en otras paginas, es bastante delicado enviar la clave que permite el descifrado de un mensaje. Por ello se creo este sistema de cifrado empleado únicamente para proteger claves.

Otros métodos no menos importantes son los siguientes ;

* *Sistema de curvas elípticas ;* esta diseñado exclusivamente para cifrar textos escritos en ordenador y no se emplea para sistemas de encriptacion de señales de televisión analógicas o digitales. El sistema se basa en los movimientos del ratón que el usuario hace antes de la instalación del programa. Este sistema puede resultar realmente complejo.

* *DDS ;* el sistema no ha sido publicado hasta ahora, pero se sabe que se basa en transmutar la secuencia de los dígitos o bits. También emplea métodos de permutación y rotación de dígitos en un modulo pseudoaleatorio. Ya hay Hackers que han trajinado con el...

* *El garral ;* parece un sistema español por lo menos por el nombre, pero no es así. También se basa en palabras de longitudes mas o menos extensas para el cifrado de mensajes. También esta desarrollado para sistemas informáticos y transacciones.

* *LUC*....solo se sabe de el que fue creado en 1993.

Los sistemas de cifrado basados en claves secretas también han conocido una muy buena aceptación, gracias a la tecnología de los ordenadores que permiten hacer computaciones elevadas sea cual sea la longitud de bits elegidas. Vamos a mencionar solo tres de ellos. El mas importante quizas sea el código DES. Este sistema de encriptacion es habitual verlo emplear en sistemas de encriptacion de señales de televisión para proteger los datos ECM de control de descodificación de la señal. Sin embargo según los Hackers todos los sistemas de seguridad tienen sus fallos y por lo tanto pueden dejar de ser seguros, si el pirata es lo suficientemente hábil.

* *DES*...este si que es un sistema de cifrado, altamente seguro, rey de los sistemas basados en claves secretas, que ha demostrado su fuerza en los últimos 20 años desde su creación. Hasta ahora no ha podido ser abierto. Básicamente es empleado para las transiciones de datos interbancarios y transferencias de alto riesgo. Las tarjetas de acceso inteligente de los telebancos también operan según esta clave, con una palabra de unos 200 bits. El sistema de encriptacion de señales de video Nagravision lo emplea para proteger los datos ECM y EMM del sistema. El sistema de cifrado DES se basa en la permutación de la longitud de bits, unos 200 por lo general, en al menos 16 permutaciones en la primera versión de este sistema de cifrado, después los datos son rotados a situaciones irrelevantes. El sistema esta descrito en el capitulo Carding, pero es mas que probable que a estas alturas hayan modificado la estructura del algoritmo de cifrado, pero de cualquier manera es prácticamente imposible de abrir aun cuando se sabe que ruta siguen los bits, en toda la secuencia.

* *IDEA*....este sistema fue desarrollado en Zurich en 1990 y emplea claves de encriptacion de 128 bits de longitud y se considera muy seguro. Es uno de los algoritmos mas conocidos actualmente. El método de cifrado se puede esperar, esta basado en modificar la orientación de cada bit, y combinarla con una

puerta lógica variable.

* *RC4*.....este algoritmo fue desarrollado por el grupo RSA y un buen día fue publicado, por lo que su seguridad descendió vertiginosamente. El sistemas se basa en combinar cada bit con otro bit de otra secuencia. Acepta claves de cualquier longitud y emplea un generador de números aleatorios. Es muy difícil de romper y su fuerte, esta en la velocidad de computación admisible. Ademas es el método empleado por el SSL de Nestcape en su versión con clave de 40 bits.

Ademas de estos sistemas de cifrado basados en claves publicas o secretas, existen otros sistemas de cifrado basados en algoritmos. Estos nuevos sistemas no emplean claves de ningún tipo, si no que se basan en extraer una determinada cantidad de bits a partir de un texto de longitud arbitraria. Esto es, cada cierta cantidad de texto elegido de forma arbitraria, se procede a realizar una transformación de bits, de esta transformación se obtiene una palabra longitud clave, esta palabra longitud tiene una extensión de x bits preestablecidos, de esta forma el texto es irreconocible ya que solo se pueden leer números secuenciales y no guardan relación alguna entre si. Este es el método, quizas, mas complejo que existe hasta el momento. Trabajar con estos algoritmos requiere sistemas informáticos, esto es, ordenadores o tarjetas de acceso inteligentes que solo comuniquen el tipo de algoritmo empleado. Estos algoritmos normalmente se basan en complejas operaciones matemáticas de difícil resolución. Y el secreto precisamente esta hay, en que operaciones matemáticas sigue el algoritmo.

Entre los sistemas desarrollados a partir de la creación de algoritmos, cabe destacar al menos dos, por su complejidad e importancia sociales ;

* *MD5*.....este algoritmo esta desarrollado por el grupo RSA y es un intento de probar con otros sistemas criptográficos que no empleen claves. El algoritmo desarrollado es capaz de obtener 128 bits a partir de un determinado texto. Como es lógico hasta el momento no se sabe cuales son las operaciones matemáticas a seguir, pero hay alguien que dice que es mas que probable que se basen en factores de números primos.

* *SHA*.....es un algoritmo desarrollado por el gobierno de los EE.UU y se pretende implantar en los sistemas informáticos de alta seguridad del estado como estándar de protección de documentos. El algoritmo obtiene 160 bits de un texto determinado. Se sabe que existen Hackers que han probado suerte, pero hasta el momento nadie ha dicho nada mas al respecto.

## 10.2 Criptoanálisis

Este si que es un tema complejo. Esta ciencia o parte de ella también denominada Hacking por los

*underground* o *Chiberpunks*, es el arte de estudiar los mensajes ilegibles, esto es, encriptados, para transformarlos en legibles sin conocer la clave o el método empleado. Esto es, romper el cifrado y hacer Crack.

Como ya se ha comentado en otros capítulos de este libro, un buen principio es tener mucha paciencia y gran capacidad de intuición. Este último es quizas el factor mas importante de todos, sin ella probablemente estés perdido. También es lógico que debes ser un experto en sistemas criptográficos, lo primero que puedes hacer es estudiar los sistemas ya existentes. Que probablemente te sirvan de algo.

Estudiar los sistemas de cifrado basados en métodos clásicos, te aportara una gran creatividad y es probable que puedas abrir cualquier mensaje encriptado en alguno de ellos. Sin embargo los textos encriptados con cualquier sistema basado en métodos modernos, ya es algo mas complejo. En tal caso debes emplear un ordenador como mínimo y crear un programa que resuelva con elegancia algunas combinaciones lógicas y algunas operaciones matemáticas.

La operación para abrir un sistema criptográfico te puede llevar días, cuando no semanas, ademas estos métodos modernos, sobre todo los métodos basados en algoritmos son muy difíciles de descubrir. Por otro lado, como ya se ha dicho, los métodos basados en claves publicas son los sistemas mas fuertes.

Los principales Hacks realizados en la red se basan en falsear lo IP, protocolos de entrada en ordenadores remotos. Muy pocos Hackers son capaces de descubrir y reventar los algoritmos o mensajes cifrados. Estos, son de reducido numero de componentes y normalmente no lo hacen para hacer daño, si no para demostrar que todos los programas tienen bugs. El hacker mas peligroso es el que crea virus informáticos y abre puertas lógicas y te modifica los ficheros de tu ordenador.

Los virus informáticos también pueden ser algoritmos complejos de desencriptar. Esto se crea así, para que los sysops o policías cibernéticos no puedan descubrir la forma de anular tal virus. En este caso también se procede al criptoanálisis del virus.

Por otro lado los Hackers mas deseados siempre estarán bien protegidos, ya que son los mas adecuados para suministrar ayuda en operaciones delicadas como el espionaje del enemigo. Sin ir mas lejos en la guerra del golfo pérsico, fueron necesarios desencriptar muchos mensajes para frenar las fuerzas de Sadam hussein, algo que muchos han ignorado desde siempre.

Cualquier guerra mas o menos importante de hoy día y desde las miticas y no olvidadas guerras mundiales primera y segunda, siempre se han empleado encriptaciones en los mensajes. Y desde siempre existió el criptoanálisis para desencriptar los mensajes del enemigo. Una famosa alusión de ello, es el " *Enigma* " una maquina de escribir que imprimía la Z en lugar de la A, por citar un ejemplo.

Este hecho ha pasado a la historia de la criptografía y el criptoanálisis, por la dureza del sistema enigma,

ya que el caso no es de menospreciar. En los años 20, los alemanes desarrollaron para aquella época, " la segunda guerra mundial " una maquina altamente sofisticada a la que llamaron " *Enigma* ". Su misión, era la de crear textos cifrados de alta seguridad totalmente incomprensibles. Su aspecto exterior era la de una maquina de escribir convencioanl, pero con la salvedad de que , al teclear la letra Z esta, imprimía una A y así con todas las letras del alfabeto. En un principio esto, podía tratarse de un método clásico siguiendo un patrón fijo, sin embargo el truco no estaba hay. La relación pulsación/resultado cambiaba de forma aleatoria y de eso se trataba. Con lo cual era prácticamente imposible descubrir un orden.

De esta forma Enigma fue el instrumento para cifrar las ordenes y mensajes durante la segunda guerra mundial y fue entonces cuando entro de lleno la ciencia del criptoanálisis y de los Hackers " *oficiales* ".

Sin embargo fue en 1933 cuando un experto en criptografía, Marian Rajewsky, perteneciente al servicio de inteligencia polaco, consiguió descifrar los mensajes de Enigma. Para ello tardaron varios años de criptoanálisis continuados con el fin de clonar o fabricar una maquina exacta a la Enigma de los alemanes.

Pero la maquina experimento ciertas evoluciones y Marian Rajewsky junto con la ciencia polaca no pudo enterarse de la inminente invasión Nazi. Sin embargo los ingleses, muy activos a la hora de hacer hacking, siempre han sido los pioneros en sistemas de desencriptacion de canales de pago, continuaron con la investigación del sistema Enigma mejorado, y por fin, en 1940, apareció el primer mensaje descifrado de las nuevas Enigma. Fue un genio llamado Alan Turing y un grupo de personas sacados de " *debajo de las piedras* " y que otra cosa podían ser que verdaderos Hackers.

También la Biblia pudo ser cifrada mientras se escribió, o esto es lo que afirma un tal Michael Drosnin, el cual asegura también, que ha conseguido mediante el criptoanálisis y la ayuda de una potente computadora, descifrar mensajes muy importantes para la humanidad, entre ellas cuando será el fin del mundo.

## 10.3 Un poco de historia

Ya en el antiguo Egipto se emplearon sistemas criptográficos y prueba de ello son los jeroglíficos no estándar escritos en las paredes de las pirámides y algunas tumbas. Esto, data de 4.000 años atrás y el sistema se basaba en figura geométricas y dibujos, que conformaban un mensaje no descifrable. Este sistemas, podría ser realmente complejo ya que una forma geométrica indefinida podría decir muchas cosas y no decir nada.

Por otro lado los griegos ya empleaban sistemas criptográficos, aproximadamente en el año 500 a.C. Estos empleaban un curioso artilugio llamado " *scytale* " que consistía en un cilindro alrededor del cual, se enrollaba una tira de cuero. Se escribía un mensaje sobre la tira, y al desenrollarla, se podía ver una ristra de letras, aparentemente sin sentido alguno. Nótese que ya desde esa temprana edad, los sistemas

de cifrado se sostenían sobre la base de intercambiar las palabras de los textos, y por tanto se trataban de sistemas de cifrado clásicos, ya que únicamente se necesitaban encriptar mensajes escritos.

Julio Cesar también empleo un sistema de cifrado durante su reinado. Dicho sistema ya ha sido convenientemente detallado en párrafos anteriores, dentro de uno de los métodos clásicos. Pero vamos a recordarlo aquí y ahora. Su sistema se basaba en sustituir la letra a encriptar por otra letra distanciada a 3 posiciones mas adelante. De esta forma se obtenían mensajes ininteligibles y durante su reinado y posterior el sistema nunca fue desencriptado por aquel entonces.

En el siglo XII, el sabio ingles Roger Bacon, describió diversos métodos criptográficos al igual que Gabriel di Lavinde *" quien invento el sistema Nomemclator "*, quien publicó en 1379 una compilación de sistemas a petición del Papa Clemente VII. Es bien curioso saber que hasta la propia iglesia tenía que echar mano a sistemas criptográficos. Los sistemas empleados por esas fechas indudablemente se basaban en métodos clásicos por sustitución.

En 1467 León Battista Alberti invento el primer sistema criptográfico polialfabetico y no fue hasta el siglo XVIII, cuando fue descifrado. En 1790 Thomas Jefferson invento su cilindro de transposiciones, que fue ampliamente utilizado durante la segunda guerra mundial por la armada de los Estados Unidos. Pero el sistema no duraría mucho, ya que se basaba en un sistema polialfabetico y en 1861 se publicó la primera solución generalizada para resolver cifrados polialfabeticos, poniendo fin a 400 años de silencio.

Sin embargo los sistemas criptográficos no experimentaron ni parada alguna ni mucho menos demora en sus sistemas de cifrado. Las grandes guerras impulsaron la creación de nuevos sistemas criptográficos mas potentes y difíciles de entender. La maquina Enigma desarrollada por los alemanes a mediados de los 70 fue un duro golpe para el criptoanálisis y sobre todo para los expertos en sistemas criptográficos.

Poco después de los 70 aparecieron los sistemas criptográficos denominados modernos. Así en 1976 el código DES hizo su aparición gracias al desarrollo de computadores digitales. A partir de hay los algoritmos y sistemas de criptografía experimentarían un interés ineludible. El sistemas DES fue el primero de los sistemas complejos, pero introdujo la clave secreta, que debía, esta, ser muy guardada si se quería mantener la fuerza del sistema, pero ese mismo año hacían la aparición estelar Diffie y Hellman, creadores del primer sistema de cifrado basado en claves publicas. Sistemas altamente seguros.

Un año después Rivert, Shamir y Adelman se sacaban de la manga el sistema criptográfico de actualidad, el RSA. Un sistema basado en buscar números primos, nada fácil de solucionar. Hasta la fecha el sistema esta siendo empleado por comptudadores y sistemas de codificación de canales de televisión.

Finalmente, el sistema criptográfico mas conocido en la red de Internet para todos los cibernautas, es el sistema PGP de Phil Zimmerman, creado en 1991. Sin embargo hay que decir que este sistema criptográfico, mas que eso, es un programa que reúne los sistemas criptográficos mas fuertes del mercado como el DSS

o el de Diffie-Hellman. Pero lo que hace es jugar con ellos y así se obtienen brillantes encriptaciones realmente seguras.

Hoy por hoy el sistema objetivo por un gran numero de Hackers es el mencionado PGP, ya que es el mas ampliamente utilizado por los navegantes. De momento no se ha conocido apertura ninguna de este sistema, sin embargo los nuevos ordenadores del futuro, ponen en manos de Hackers herramientas verdaderamente potentes que acabaran con todos estos sistemas criptográficos de gran seguridad.

Si no, tiempo al tiempo.

# Capitulo 11

# Echelon, espías en el cielo

Hace 40 años Nueva Zelanda creo un servicio de inteligencia llamado GCSB "Government Communications Security Bureau " el equivalente a la NSA americana. Ahora y en colaboración con la NSA, crean Echelon. Un avanzado sistema de espionaje a escala mundial, que junto con UKUSA y el empleo de Satélites Intelsat, las nuevas inteligencias gubernamentales pueden desde hace tiempo acceder e interceptar todas las comunicaciones tradicionales como el teléfono, el fax o el correo electrónico. Es esto una realidad ?

Las nuevas tecnologías y la enorme evolución de la informática en ella, ha transformado el mundo en un cumulo de tecnologías las cuales por un lado, nos facilitan el quehacer diario y la eficacia de nuestro trabajo, por otro, nuestra intimidad se ve seriamente dañada con los sistemas criptográficos, los accesos restringidos y ahora Echelon.

Y que es Echelon ?, la respuesta en las próximas lineas y como dirían en los expedientes X, lo que vamos a presentar ahora va mas allá de todo lo expuesto hasta ahora en estas paginas. Desde 1996 Nicky Hagar´s nos muestra otro tipo de espionaje secreto, descubierto en su libro Secret Power, Nicky revela que estamos siendo espiados en todo momento.

Según su libro, Nicky afirma que lo que estoy escribiendo ahora es susceptible de ser espiado incluso en el borrador desde mi PC, mediante el método TEMPEST. Este sistema de espionaje aprovecha la radiación electromagnética de la pantalla de mi monitor para recibir todo lo que se muestra en mi monitor. Por otro lado cuando termine este articulo y lo envíe por el correo electrónico, este será inmediatamente interceptado por la estructura Echelon y por supuesto analizado.

Por otro lado si envío un fax a mi editor o le llamo telefónicamente para confirmar que ha recibido el articulo, Echelon también dispondrá de una copia del fax y de la conversación telefónica. Pensar en todo esto, simplemente le pone a uno los pelos de punta.

En 1948 se formaliza UKUSA después de interceptar varias comunicaciones de radio secretas durante la segunda guerra mundial. Junto con Echelon, UKUSA " denominada Spy Network " potencia las posibilidades de controlar las comunicaciones globales desde los satélites Intelsat.

El jueves, 12 de junio de 1984, Rob Muldoon conviene en el parlamento lo que seria el primer paso para crear Echelon. Diez años mas tarde, el 15 de enero de 1994 los técnicos de satélites interceptan comunicaciones extrañas en los satélites, fecha en la que se revela la existencia de UKUSA.

Desde entonces todas las comunicaciones son interceptadas por echelon y ukusa y descifradas por técnicos expertos en busca de información confidencial de un posible movimiento militar, terrorista o de otra índole.

## 11.1 Enemigo publico

La película Enemigo Publico de Jerry Bruckheimer " dirigida por Tony scott " narra la historia de un abogado " Will Smith " que de la noche a la mañana se ve involucrado en una desesperante persecución por parte de la CSA " algo así como la NSA actual " la cual despliega todo tipo de artilugios electrónicos de extremada tecnología, así como de un despliegue de satélites especiales, capaces de ver una hormiga en su hormiguero.

Esta película, queriendo o sin querer, nos muestra como los gobiernos " preferentemente el americano " han avanzado en este tipo de tareas. Por otro lado, la película arranca con una polémica sobre la " intimidad " de las personas, ya que estas pueden ser espiadas en todo momento. Esta polémica causada por la " violación de la intimidad humana " es la que arranca la película hacia un despliegue de tecnologías posibles dentro de la ciencia ficción.

En estas líneas no quiero explicar la película en si, aunque si describir por lo menos de que se trata, para que con ello, el lector comprenda de que hablamos. Lo que quiero decir es que " Enemigo Publico " podría no ser una película en cuestión, si no una visión de lo que realmente existe fuera de las pantallas de cine.

Los expertos de la CSA consiguen cambiar " por clones idénticos " el reloj, el bolígrafo o el pantalón de Will Smith, " en la película " que no son mas que radiotransmisores de alta frecuencia. También, son capaces de interceptar todas las llamadas telefónicas que realiza nuestro abogado, pero lo mas sorprendente de la película, es la visión de los satélites redirigidos desde una base de control, que permiten obtener imágenes claras de nuestro protagonista angustiado corriendo sobre los tejados de palm sprit.

En un principio esto bien podría ser el derroche de ideas de un buen guionista de Hollywod, pero Nicki y su libro nos muestra como todo esto, esta sucediendo realmente fuera de las pantallas de cine. Llegados a este punto, solo podemos optar por estudiar que pueden interceptar realmente desde Echelon o UKUSA y comprobar si realmente es tan alarmante como se plantea.

## 11.2 Espias desde el cielo

Las principales formas de espionaje se basan en interceptar las comunicaciones por radio sea cual sea su banda. Pero las potentes cámaras de vídeo de ultima generación y las nuevas lentes ópticas, permiten obtener imágenes sorprendentes desde una distancia mas que alarmante comprendida en varios cientos de kilómetros de distancia.

Esta técnica, se sobreimpone a la captacion de ondas de radio. Por otro lado Internet, el gran complejo de comunicaciones digitales mundial también esta siendo espiado por la nueva inteligencia gubernamental. Otro peligro se sobreimpone por el empleo de teléfonos móviles. Todos los datos " pinchados " se

codifican y se envían al espacio hacia los satélites donde se multiplexan todas las señales para ser distribuidas hacia los centros de computación y control.

Estas bases terrestres además de recibir toda la información están diseñadas para " escanear " y recibir todas las frecuencias de los satélites en busca de información conflictiva. En los centros de control de estas bases tiene lugar el estudio de todas las señales " interceptadas " entre las cuales pueden existir informaciones en claro e informaciones encriptadas.

Las informaciones en claro se entienden por todas aquellas que están codificadas bajo cualquier estándar analógico o digital, pero que los ingenieros conocen perfectamente. Las señales encriptadas son aquellas que se basan en contenidos cifrados imposibles de descifrar sin la clave adecuada.

Estos últimos mensajes son quizás los que mas preocupaciones causa dentro de la red " de espionaje mundial " ya que a menudo no se pueden obtener los mensajes en claro aun empleando métodos de " descifrado " de señales.

Por ello, quizás quede alguna esperanza por mantener la privacidad aunque no la intimidad de nuestras comunicaciones y es empleando sistemas criptograficos para la voz y el correo electrónico.

## 11.3 Investigación, conexo a Echelon, la NSA y otros espías

En la actualidad debemos hacer referencia al denominador común investigar, ya que como se demuestra desde la prensa diaria, algo esta sucediendo en el mundo y mas concretamente en el aspecto tecnológico. La guerra de los Balcanes ha desplegado de una sola vez la mas alta tecnología militar y hoy por hoy esta tecnología esta cubierta de sistemas de comucacion y ordenadores.

Esta guerra esta plagada de misterios y situaciones un tanto difíciles de controlar. Solo en la armada tiene lugar un autentico estado de investigación profunda. Los serbios emplean sistemas de cifrado para sus comunicaciones secretas, siendo estas, sumamente útiles para la Alianza Atlantica para conocer en todo momento la posición de las posiciones Serbias.

Sin embargo, la Alianza Atlantica, lejos de poder interpretar estas comunicaciones decide destruir todas las estaciones de comunicaciones y repetidores del país, como una clara respuesta a la incapacidad de descifrar las comunicaciones. Obligándole así, al ejercito Serbio a emplear teléfonos móviles para comunicarse. Las frecuencias radiadas por estos teléfonos, son recibidas por los aviones espías de la OTAN y transcodificadas, algo muy posible ya que el sistema GSM posee un modo de cifrado estándar.

Sin embargo la guerra no solo tiene lugar en el suelo Belgrado, en el Pentágono, la Casablanca y la propia OTAN, están siendo atacadas por Hackers Serbios a los que esporádicamente se unen sus colegas Rusos. Las intenciones, buscar pistas sobre los movimientos de la Alianza Atlantica. Pero en medio de esta guerra nace Enfopol, un sistema para " pinchar " Internet, homologo a su antecesor Echelon, Enfopol intercepta todas las tramas de Internet y bajo un sistema de inteligencia artificial, filtra la información que cree buena.

Dentro de tanta polémica se conoce la noticia de la liberación, al fin, del mayor forajido de Estados Unidos, Kevin Mitcnik uno de los Hackers mas inteligentes de la actualidad. Experto en sistemas de

telefonía y con gran capacidad para acceder a cualquier ordenador remoto Kevin podría jugar muy bien un papel importante en todo este conflicto.

Pero queda siempre la sospecha y no la certeza de lo dicho. Lo que si es cierto es que todo este conflicto podría desatar una guerra dentro y fuera del terreno. La red esta siendo invadida por nuevas formas de vida mas inteligentes, estamos hablando de nuevos virus mas avanzados que los polimorficos. Virus encriptados y mensajes que se multiplican en la red como el Melissa, creado por David L.Smith, quien le ha llevado a crear Melissa por no se sabe muy bien.

Después de todo esto, lo que si queda claro es que al final se prevé que solo los Hackers tendrán una clara intervención en todo conflicto ya que se demuestra que todo funciona bajo el influjo de los ordenadores y la criptografia, y solo los Hackers tienen palabra para ello.

The End

# Glosario de términos

El glosario de términos es parte fundamental en un libro como el que tiene delante, dado que se encuentra lleno de acrónimos y palabras que mas o menos nos recuerdan algo, pero no sabemos que. En el argot de la informática, y sobre todo en la nueva cibercultura, existe todo un diccionario de acrónimos y significados. En esta sección, de obligada visita, os mostrare los detalles y significado de cada acrónimo citado en el presente libro.

**address (dirección)** En Internet dícese de la serie de caracteres, numéricos o alfanuméricos, que identifican un determinado recurso de forma única y permiten acceder a él. En la red existen varios tipos de dirección de uso común: «dirección de correo electrónico» (*email address*); «IP» (dirección internet); y «dirección hardware» o «dirección MAC» (*hardware or MAC address)*.

**alias (alias, apodo)** Nombre usualmente corto y fácil de recordar que se utiliza en lugar de otro nombre usualmente largo y difícil de recordar.

**anonymous FTP (FTP anónimo)** El FTP anónimo permite a un usuario de Internet la captura de documentos, ficheros, programas y otros datos contenidos en archivos existentes en numerosos servidores de información sin tener que proporcionar su nombre de usuario y una contraseña (*password*). Utilizando el nombre especial de usuario *anonymous*, o a veces *ftp*, el usuario de la red podrá superar los controles locales de seguridad y podrá acceder a ficheros accesibles al público situados en un sistema remoto.

**Apache (Apache)** Servidor HTTP de dominio público basado en el sistema operativo Linux. Apache fue desarrollado en 1995 y es actualmente uno de los servidores HTTP más utilizados en la red.

**applet (aplicacioncita, aplique)** Pequeña aplicación escrita en Java y que se difunde a través de la red para ejecutarse en el navegador cliente.

**application (aplicación)** Un programa que lleva a cabo una función directamente para un usuario. WWW, FTP, correo electrónico y Telnet son ejemplos de aplicaciones en el ámbito de Internet.

**authentication (autentificación)** Verificación de la identidad de una persona o de un proceso para acceder a un recurso o poder realizar determinada actividad. También se aplica a la verificación de identidad de origen de un mensaje.

**backbone (columna vertebral, eje central, eje troncal)** Nivel más alto en una red jerárquica. Se garantiza que las redes aisladas (*stub*) y de tránsito (*transit*) conectadas al mismo eje central están interconectadas.

**banner (anuncio, pancarta)** Imagen, gráfico o texto de carácter publicitario, normalmente de pequeño tamaño, que aparece en una página web y que habitualmente enlaza con el sitio web del anunciante.

**baud (baudio)** Cuando se transmiten datos, un baudio es el numero de veces que cambia el «estado» del medio de transmisión en un segundo. Como cada cambio de estado puede afectar a más de un bit de datos, la tasa de bits de datos transferidos (por ejemplo, medida en bits por segundo) puede ser superior a la correspondiente tasa de baudios.

**bit (bit, bitio)** Unidad mínima de información digital que puede ser tratada por un ordenador. Proviene de la contracción de la expresión *binary digit* (dígito binario).

**bounce (rebote)** Devolución de un mensaje de correo electrónico debido a error en la entrega al destinatario.

**browser (hojeador, navegador, visor, visualizador)** Aplicación para visualizar documentos WWW y navegar por el espacio Internet. En su forma más básica son aplicaciones hipertexto que facilitan la navegación por los servidores de información Internet; cuentan con funcionalidades plenamente multimedia y permiten indistintamente la navegación por servidores WWW, FTP, Gopher, el acceso a grupos de noticias, la gestión del correo electrónico, etc.

***Bucaneros :*** Son peores que los Lamers, ya que no aprenden nada ni conocen la tecnología. Comparados con los piratas informáticos, los bucaneros solo buscan el comercio negro de los productos entregados por los Copyhackers. Los bucaneros solo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos « Crackeados « pasan a denominarse « piratas informáticos « así puestas las cosas, el bucanero es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de Cracking a nivel masivo.

**bug (error, insecto, gazapo)** Término aplicado a los errores descubiertos al ejecutar un programa informático. Fue usado por primera vez en el año 1945 por Grace Murray Hooper, una de las pioneras de la programación moderna, al descubrir como un insecto (*bug*) había dañado un circuito del ordenador Mark.

**Business Software Alliance — BSA (Alianza del Sector del Software)** Organismo creado en 1988 por diversas empresas del sector del software para defender sus derechos de propiedad intelectual sobre los programas que desarrollan.

**byte (byte, octeto)** Conjunto significativo de ocho bits que representan un carácter.

**cellular phone (teléfono celular, móvil, telefonino, teléfono móvil)** Teléfono portátil sin hilos conectado a una red celular y que permite al usuario su empleo en cualquier lugar cubierto por la red. Una red celular, y los teléfonos a ellos conectados, puede ser digital o analógica. Si la red es digital el teléfono puede enviar y recibir información a través de Internet.

**chat (conversación, charla, chateo, tertulia)** Comunicación simultánea entre dos o más personas a través de Internet. Hasta hace poco tiempo sólo era posible la «conversación» escrita pero los avances tecnológicos permiten ya la conversación audio y vídeo.

**chip (chip)** Circuito integrado en un soporte de silicio, formado por transistores y otros elementos electrónicos miniaturizados. Son uno de los elementos esenciales de un ordenador. Literalmente «astilla» o «patata frita».

**click (clic, cliqueo/cliquear, pulsación/pulsar)** Acción de tocar un mando cualquiera de un ratón una vez colocado el puntero del mismo sobre una determinada área de la pantalla con el fin de dar una orden al ordenador. Ver también: **«mouse»**.

**client (cliente)** Un sistema o proceso que solicita a otro sistema o proceso que le preste un servicio. Una estación de trabajo que solicita el contenido de un fichero a un servidor de ficheros es un cliente de este servidor.

**Clipper chip** Dispositivo de cifrado que el Gobierno de los EE.UU. intentó hacer obligatorio mediante ley en 1995 para poder controlar el flujo de transmisiones criptografiadas a través de redes digitales de telecomunicación.

***Copyhackers :*** Es una nueva raza solo conocida en el terreno del crackeo de Hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de televisión de pago. Este mercado mueve al año mas de 25.000 millones de pesetas solo en Europa.

En el año 1994 los Copyhackers vendieron tarjetas por valor de 16.000 millones de pesetas en pleno auge de canales de pago como el grupo SKY y Canal+ plus- Estos personajes emplean la ingeniería social para convencer y entablar amistad con los verdaderos Hackers, les copian los métodos de ruptura y después se los venden a los « bucaneros « personajes que serán detallados mas adelante.

Los Copyhackers divagan entre la sombra del verdadero Hacker y el Lamer. Estos personajes poseen

conocimientos de la tecnología y son dominados por la obsesión de ser superiores, pero 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.

**cookie (cuqui, espía, delator, fisgón, galletita, pastelito, rajón, soplón)** Conjunto de carecteres que se almacenan en el disco duro o en la memoria temporal del ordenador de un usuario cuando accede a las páginas de determinados sitios web. Se utilizan para que el servidor accedido pueda conocer las preferencias del usuario. Dado que pueden ser un peligro para la intimidad de los usuarios, éstos deben saber que los navegadores permiten desactivar los cuquis.

***Crackers :*** Es el siguiente eslabón y por tanto el primero de una familia rebelde. Cracker es aquel Hacker fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas.
Para los grandes fabricantes de sistemas y la prensa este grupo es el mas rebelde de todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica ahí, si no en que esta rotura es difundida normalmente a través de la Red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers.
En la actualidad es habitual ver como se muestran los Cracks de la mayoría de Software de forma gratuita a través de Internet. El motivo de que estos Cracks formen parte de la red es por ser estos difundidos de forma impune por otro grupo que será detallado mas adelante.
Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware. 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. Mas adelante hablaremos de los Cracks mas famosos y difundidos en la red.

**Cryptography (Criptografía)** Término formado a partir del griego *kruptos*, «oculto» ... significa, según el diccionario académico, «Arte de escribir con clave secreta o de un modo enigmático» ... Es criptográfico cualquier procedimiento que permita a un emisor ocultar el contenido de un mensaje de modo que sólo personas en posesión de determinada clave puedan leerlo, tras haberlo descifrado.

**Cryptology (Criptología)** Es la parte de la Criptografía que tiene por objeto el descifrado de criptogramas cuando se ignora la clave.

**cyber- (ciber-)** Prefijo utilizado ampliamente en la comunidad Internet para denominar conceptos relacionados con las redes (cibercultura, ciberespacio, cibernauta, etc.). Su origen es la palabra griega «cibernao», que significa «pilotar una nave».

**cybercop (ciberpolicía)** Funcionario policial especializado en Internet o en utilizar la red para sus investigaciones.

**Cyberculture (Cibercultura)** Conjunto de valores, conocimientos, creencias y experiencias generadas por la comunidad internáutica a lo largo de la historia de la red. Al principio era una cultura elitista; más tarde, con la popularización de Internet, la cibercultura es cada vez más parecida a la «cultura» a secas, aunque conserva algunas de sus peculiaridades originales.

**cybernaut (cibernauta)** Persona que navega por la red.

**Cyberspace (Ciberespacio)** Término creado por William Gibson en su novela fantástica "Neuromancer" para describir el "mundo" de los ordenadores y la sociedad creada en torno a ellos.

**cybertrash (ciberbasura)** Todo tipo de información almacenada o difundida por la red que es manifiestamente molesta o peligrosa para la salud mental de los internautas. Dícese también de quienes arrojan basura la red.

**cyberzapping (ciberzapeo)** Acción de pasar de forma rápida y compulsiva de una página a otra dentro de un sitio web o de un sitio web a otro.

**Daemon (Daemon)** Aplicación UNIX que está alerta permanentemente en un servidor Intenet para realizar determinadas tareas como, por ejemplo, enviar un mensaje de correo electrónico o servir una página web. «Daemon» es una palabra latina que significa «espíritu» (bueno o malo) o «demonio».

**Data Encryption Standard — DES (Estándar de Cifrado de Datos)** Algoritmo de cifrado de datos estandarizado por la administración de EE.UU.

**de-encryption (descifrado, deencriptación)** Recuperación del contenido real de una información cifrada previamente.

**Defense Advanced Research Projects Agency — DARPA (Agencia de Proyectos de Investigación Avanzada para la Defensa)** Organismo dependiente del Departamento de Defensa norteamericano (DoD) encargado de la investigación y desarrollo en el campo militar y que jugó un papel muy importante en el nacimiento de Internet a través de la red ARPANET.

**dialup (conexión por línea conmutada)** Conexión temporal, en oposición a conexión dedicada o permanente, establecida entre ordenadores por línea telefónica normal. Dícese también del hecho de marcar un número de teléfono.

**digital signature (firma digital)** Información cifrada que identifica al autor de un documento electrónico y autentifica que es quien dice ser.

**download (bajar, descargar)** En Internet proceso de transferir información desde un servidor de información al propio ordenad**encryption (cifrado, encriptación)** El cifrado es el tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red. or personal.

**file (archivo, fichero)** Unidad significativa de información que puede ser manipulada por el sistema operativo de un ordenador. Un fichero tiene una identificación única formada por un «nombre» y un «apellido», en el que el nombre suele ser de libre elección del usuario y el apellido suele identificar el contenido o el tipo de fichero. Así, en el fichero prueba.txt el apellido «txt» señala que se trata de un fichero que contiene texto plano.

**File Transfer Protocol — FTP (Protocolo de Transferencia de Ficheros)** Protocolo que permite a un usuario de un sistema acceder a, y transferir desde, otro sistema de una red. FTP es también habitualmente el nombre del programa que el usuario invoca para ejecutar el protocolo.

**finger (apuntar con el dedo, dedo)** Programa que muestra información acerca de un usuario(s) especifico(s) conectado(s) a un sistema local o remoto. Habitualmente se muestra el nombre y apellidos, hora de la ultima conexión, tiempo de conexión sin actividad, línea del terminal y situación de éste. Puede también mostrar ficheros de planificación y de proyecto del usuario.

**firewall (cortafuegos)** Sistema que se coloca entre una red local e Internet. La regla básica es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc.

**Free Software (Software Libre)** Programas desarrollados y distribuidos según la filosofía de dar al usuario la libertad de ejecutar, copiar, distribuir, estudiar, cambiar y mejorar dichos programa (Linux es un ejemplo de esta filosofía). El software libre no es siempre software gratuito (equivocación bsatante habitual que tiene su origen en que la palabra inglesa *free* significa ambas cosas).

**freeware (programas de libre distribución, programas gratuitos, programas de dominio público)** Programas informáticos que se distribuyen a través de la red de forma gratuita.

**gateway (pasarela)** Hoy se utiliza el término *router* (direccionador, encaminador, enrutador) en lugar de la definición original de *gateway*. Una pasarela es un programa o dispositivo de comunicaciones que transfiere datos entre redes que tienen funciones similares pero implantaciones diferentes. No debería confundirse con un convertidor de protocolos.

**Global System for Mobile communication — GSM (Sistema Global para comunicaciones Móviles)** Sistema compatible de telefonía móvil digital desarrollado en Europa con la colaboración de

operadores, Administraciones Públicas y empresas. Permite la transmisión de voz y datos.

**guru (gurú)** Persona a la que que se considera, no siempre con razón, como el sumo manantial de sabiduría sobre un determinado tema. Nicholas Negroponte es considerado el máximo gurú en lo que se refiere a Internet y la llamada Sociedad de la Información.

***Hackers :*** El primer eslabón 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 para lograr comprender sistemas tan complejas como la comunicación móvil. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. Les encanta entrar en ordenadores remotos, con el fin de decir aquello de « 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.

El perfil del Hacker idóneo es aquel que se interesa por la tecnología, al margen de si lleva gafas, es delgado o lleva incansablemente encima un teléfono celular de grandes proporciones. emplea muchas horas delante del ordenador, pero para nada debe ser un obsesivo de estas maquinas. No obstante puede darse el caso.

Este grupo es el mas experto y menos ofensivo, ya que no pretenden serlo, a pesar de que poseen conocimientos de programación, lo que implica el conocimiento de la creación de Virus o Crack de un software o sistema informático.

**hoax (bulo, camelo)** Término utilizado para denominar a rumores falsos, especialmente sobre virus inexistentes, que se difunden por la red, a veces con mucho éxito causando al final casi tanto daño como si se tratase de un virus real.

**host (sistema anfitrión, sistema principal / albergar, dar albergue )** Ordenador que, mediante la utilización de los protocolos TCP/IP, permite a los usuarios comunicarse con otros sistemas anfitriones de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet, WWW y FTP. La acepción verbal (*to host*) describe el hecho de almacenar algún tipo de información en un servidor ajeno.

**IP address (dirección IP)** Dirección de 32 bits definida por el Protocolo Internet en STD 5, RFC 791. Se representa usualmente mediante notación decimal separada por puntos. Un ejemplo de dirección IP es 193.127.88.345

**key (clave)** Código de signos convenidos para la transmisión de mensajes secretos o privados.

**keyword (clave de búsqueda, palabra clave)** Conjunto de caracteres que puede utilizarse para buscar una información en un buscador o en un sitio web.

***Lamers :*** Este grupo es quizás el que mas numero de miembros posee y quizás son los que mayor presencia tienen en la red. Normalmente son individuos con ganas de hacer Hacking, pero que carecen de cualquier conocimiento. Habitualmente son individuos que apenas si saben lo que es un ordenador, pero el uso de este y las grandes oportunidades que brinda Internet, convierten al nuevo internauta en un obsesivo ser que rebusca y relee toda la información que le fascina y que se puede encontrar en Internet. Normalmente la posibilidad de entrar en otro sistema remoto o la posibilidad de girar un gráfico en la pantalla de otro ordenador, le fascinan enormemente.

Este es quizás el grupo que mas peligro acontece en la red ya que ponen en practica todo el Software de Hackeo que encuentran en la red. Así 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 autodenominandose Hacker.

También emplean de forma habitual programas sniffers para controlar la Red, interceptan tu contraseña y correo electrónico y después te envían varios mensajes, con dirección falsa amenazando tu sistema, pero en realidad no pueden hacer nada mas que cometer el error de que poseen el control completo de tu disco duro, aun cuando el ordenador esta apagado.

Toda una negligencia en un terreno tan delicado.

**mail bombing (bombardeo postal)** Envío indiscriminado y masivo de mensajes de correo electrónico.

***Newbie :*** Es un novato o mas particularmente es aquel que navega por Internet, tropieza con una pagina de Hacking y descubre que existe un área de descarga de buenos programas de Hackeo. Después se baja todo lo que puede y empieza a trabajar con los programas.

Al contrario que los Lamers, los Newbies aprenden el Hacking siguiendo todos los cautos pasos para lograrlo y no se mofa de su logro, si no que aprende.

**packet (paquete)** La unidad de datos que se envía a través de una red. En Internet la información transmitida es dividida en paquetes que se reagrupan para ser recibidos en su destino.

**password (contraseña, palabra de paso)** Conjunto de caracteres alfanuméricos que permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado.

**pay-per-view (pago por pase, pago por visión)** Servicio de televisión que permite al usuario ver un determinado programa (por ejemplo, un partido de fútbol, un concierto o una película) emitido en formato codificado, mediante el pago de una tarifa.

***Phreaker :*** Este grupo es bien conocido en la Red por sus conocimientos en telefonía. Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente.

Sin embargo es, en estos últimos tiempos, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta y/o emplean la informática para su procesado de datos.

**Pretty Good Privacy — PGP (Privacidad Bastante Buena, Privacidad de las Buenas)** Conocido programa de libre distribución, escrito por Phil Zimmermann, que impide, mediante técnicas de criptografía, que ficheros y mensajes de correo electrónico puedan ser leídos por otros. Puede también utilizarse para firmar electrónicamente un documento o un mensaje, realizando así la autentificación del autor.

**Rivest, Shamir, Adleman — RSA (Rivest, Shamir, Adleman)** Clave criptográfica de amplia utilización, patentada por los autores, que le dan nombre.

**set-top box (caja de conexión, módulo de conexión)** Dispositivo multifunción que permite la recepción y distribución en el ámbito doméstico de señales procedentes de diversos tipos de redes de comunicación (radio, televisión, teléfono, cable, satélite, Internet, ...).

**shareware (programas compartidos)** Dícese de los programas informáticos que se distribuyen a prueba, con el compromiso de pagar al autor su precio, normalmente bajo, una vez probado el programa y/o pasado cierto tiempo de uso.

**spam (bombardeo publicitario, buzonfia)** Envío masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico. Literalmente quiere decir “loncha de mortadela”.

**Sysop (Operador del sistema)** Persona responsable del funcionamiento de un sistema o de una red.

**Trojan Horse (Caballo de Troya)** Programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema que lo procesa.

**UNIX, Unix (UNIX, Unix)** Sistema operativo interactivo y de tiempo compartido creado en 1969 por Ken Thompson. Reescrito a mitad de la década de los ’70 por ATT alcanzó enorme popularidad en los ambientes académicos y, más tarde en los empresariales, como un sistema portátil robusto, flexible y portable, muy utilizado en los ambientes Internet.

**virus (virus)** Programa que se duplica a si mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar problemas de diversa gravedad en los sistemas que los almacenan.

**wetware (materia húmeda)** En la jerga de los piratas informáticos significa “cerebro”.

**worm (gusano)** Programa informático que se autoduplica y autopropaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes. Los gusanos de redes fueron definidos por primera vez por Shoch & Hupp, de Xerox, en “ACM Communications” (Marzo 1982). El gusano de Internet de Noviembre de 1988 es quizás el más famoso y se propagó por íi solo a más de 6.000 sistemas a lo largo de Internet.

Algunas partes del presente glosario de terminos, han sido extraidas del glosario basico Ingles-Español para usuarios de Internet de Rafael Fernández Calvo, dado que creo mas que interesante, ademas de que esta autorizada su reproducción de parte o la totalidad de la obra, si la presente no posee animo de lucro.

# Bibliografía

Los piratas del Chip de Bryan Clough y Paul Mungo, Ediciones B 1992
A prueba de Hackers de Lars Klander, Anaya Multimedia 1998
Hacking en Internet de Claudio Hernández, Luis A.Iñigo e Israel Robla 1998
Takedown de Tsutomu Shimomura y John Markoff, el País Aguilar 1997
Hackers, piratas tecnológicos de Claudio Hernández, Coelma 1998

**Este libro se encuentra en la revisión 1.0**
**8-11-99**


**The End**