Hacker Highschool
SECURITY AWARENESS FOR TEENS

LECCIÓN 12
LEGALIDAD Y ÉTICA EN INTERNET

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

Información sobre la "Licencia de Uso"

Las lecciones y cuadernos de trabajo siguientes son de acceso público y están disponibles bajo las siguientes condiciones de ISECOM:

Todos los trabajos del proyecto "Hacker Highschool" son proporcionados para su uso no comercial con estudiantes de escuelas primarias, secundarias, bachilleratos y ciclos formativos dentro de las actividades académicas propias de la institución. Dichos materiales no pueden ser reproducidos con fines comerciales de ningún tipo. La impartición con estos materiales de cualquier clase, curso o actividad de formación para el que sea necesario pagar un importe, queda totalmente prohibida sin la licencia correspondiente, incluyendo cursos en escuelas y universidades, cursos comerciales o cualquier otro similar. Para la compra de una licencia visite la sección "LICENSE" de la página web del proyecto "Hacker Highschool" en www.hackerhighschool.org/license.

El proyecto HHS es una herramienta de aprendizaje y, como tal, la formación final debe proceder realmente de la influencia del instructor y no basarse únicamente en el uso de la herramienta.

ISECOM no puede aceptar bajo ningún concepto responsabilidad alguna sobre la forma de aplicar, ni sus consecuencias, de cualquier información disponible dentro del proyecto. El proyecto HHS es un esfuerzo de una comunidad abierta, por lo que si encuentra útil este proyecto le invitamos a patrocinarlo a través de la compra de una licencia, una donación o un patrocinio.

Todos los Derechos Reservados ISECOM, 2004.

Índice

Contribuciones

Francisco de Quinto, Piqué Abogados Asociados
Jordi Saldaña, Piqué Abogados Asociados
Jaume Abella, Enginyeria La Salle (URL) – ISECOM
Marta Barceló, ISECOM

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

LA SALLE
Enginyeria
Arquitectura
Universitat Ramon Llull

12.1. Introducción

Las nuevas tecnologías, al configurarse como nuevo paradigma que invade todos los ámbitos de la actividad humana, no podían por menos de incidir también en el lado oscuro de dicha actividad: la conducta delictiva o criminal de los individuos de los grupos organizados.

Por este motivo hemos reservado la última de las lecciones del HHS a analizar varios aspectos relacionados con la legalidad y la ética en Internet, analizando las numerosas conductas que pueden desembocar en delitos y las consecuencias que estas pueden provocar.

12.2. Delitos transfronterizos versus Derechos locales

Las nuevas tecnologías, al configurarse como nuevo paradigma que invade todos los ámbitos de la actividad humana, no podían por menos de incidir también en el lado oscuro de dicha actividad: la conducta delictiva o criminal de los individuos de los grupos organizados.

Por sus especiales características dos son las fórmulas a través de las que las Tecnologías de la Información y las Comunicaciones (TICs) se relacionan con el delito:

1. Por un lado, las tecnologías ofertan la posibilidad de renovar las tradicionales formas de delinquir. Entraríamos aquí en figuras delictivas tipificadas tradicionalmente en los códigos penales pero que tienen una nueva forma de materializarse. Por poner dos ejemplos podemos citar el blanqueo de capitales y la pornografía infantil.
2. Por otro lado, por la fuerza de su propia innovación, las TICs han propiciado la aparición de nuevas figuras delictivas que, por su novedad, están en proceso de incorporación a los códigos penales de los diferentes países. A modo de ejemplo podemos citar las agresiones a la salud pública por antenas de telefonía o los ataques mediante virus.

Otra característica a destacar de las TICs es su desubicación espacial, la cual afecta mucho al entorno en general, pero sin duda cobra su máxima expresión en el ámbito del "Derecho" que desde los orígenes siempre ha presentado una clara vocación territorial tanto en lo que respecta a la autoridad judicial que juzga (JURISDICCIÓN COMPETENTE) como en lo relativo a la norma que se debe aplicar al juzgar (LEY APLICABLE). Ambos conceptos son aún hoy en día marcadamente geográficos.

En síntesis podemos decir que las TICs son globales y esencialmente transfronterizas y, por el contrario, la ley y los tribunales están limitados por definición a un determinado estado o territorio. Además, el fenómeno de la desubicación es en realidad mucho más acusado de lo que aparenta. A pesar de que no seamos conscientes de ello, una información bidireccional on-line entre un usuario en Barcelona y un Web Site alojado en un ISP de California puede pasar por más de 10 ISPs distintos domiciliados en los puntos más dispares del mundo. Ante esta diversidad de domicilios y nacionalidades cabe preguntarse ¿Qué ley se aplicará en caso de litigio? ¿Cuál de entre todos los posibles será el Tribunal idóneo para entender del caso?

A modo de ejemplo cabe citar el reciente convenio del Consejo de Europa sobre cibercrimen, firmado el 23 de Noviembre de 2001 en Budapest por 30 países entre los que figuran, lógicamente, los 15 socios de la U.E., Estados Unidos, Canadá, Japón y Sudáfrica entre otros. El convenio de Budapest instaura el PRINCIPIO DE TERRITORIALIDAD para definir la jurisdicción competente. La firma de este Convenio es la culminación de cuatro años de trabajo que se han plasmado en un documento de 48 artículos que se organizan en torno a cuatro categorías:

1. Infracciones contra la confidencialidad
2. Falsificación y fraude informático
3. Infracciones relativas a los contenidos
4. Violaciones de la propiedad intelectual

Una vez descrito el especialmente complejo marco de regulación y sanciones de la actividad criminal en Internet, es obligado cerrar a modo de primera conclusión las tres principales dificultades para alcanzar el mínimo consenso internacional deseable sobre la materia:

1ª DIFICULTAD: CONFLICTO DE JURISDICCIÓN. Elegir el tribunal competente para juzgar un delito multinacional y transfronterizo. Este problema no está definitivamente resuelto por ninguno de los sistemas judiciales conocidos.

2ª DIFICULTAD: CONFLICTO DE LEYES. Una vez elegido el tribunal la primera rigidez con que tropezará su actividad es elegir la ley aplicable al caso concreto que debe juzgar. De nuevo nos vemos obligados a concluir que los criterios jurídicos tradicionales no son operativos para su aplicación en el entorno virtual.

3ª DIFICULTAD: EJECUCIÓN DE SENTENCIA EXEQUATOR. Una vez el tribunal competente ha emitido sentencia ésta debe ser ejecutada, previsiblemente en países distintos del foro que la ha dictado. Para ello se debe contar con un compromiso supra-nacional de reconocimiento y aceptación de sentencias. Esta problemática es todavía más complicada de solucionar que las dos anteriores.

12.3. Delitos relativos a las TIC's

La clasificación de las conductas delictivas es uno de los principios imprescindibles en materia penal y en España tenemos la gran suerte de que el Código Penal vigente se promulgó hace relativamente poco tiempo. En efecto, el conocido como Código Penal Belloch se aprobó el 23 de noviembre de 1995 (Ley Orgánica del código Penal 10/1995) y en su exposición de motivos se reconoce la necesidad de introducir nuevas figuras delictivas para adaptar los criterios penales a las exigencias sociales actuales.

Entre otras podemos destacar la siguiente clasificación de las acciones potencialmente delictivas en los seis apartados siguientes:

1. Manipulación en los datos e informaciones contenidas en los archivos o soportes físicos informáticos ajenos.
2. Acceso a los datos y/o utilización de los mismos por quien no está autorizado para ello.

3. Introducción de programas o rutinas en otros ordenadores para destruir información, datos o programas.
4. Utilización del ordenador y/o los programas de otras personas, sin autorización, con el fin de obtener beneficios propios y en perjuicio de otro.
5. Utilización del ordenador con fines fraudulentos.
6. Agresión a la "privacidad" mediante la utilización y procesamiento de datos personales con fin distinto al autorizado.

El delito tecnológico se caracteriza por las dificultades que entraña descubrirlo, probarlo y perseguirlo. En efecto, son delitos que en la mayoría de los casos no se denuncian, para evitar la alarma social o el desprestigio por un fallo en la seguridad. Las víctimas prefieren sufrir las consecuencias del delito e intentar prevenirlo para el futuro antes que iniciar un procedimiento judicial. Esta situación dificulta enormemente el conocimiento del número de delitos cometidos y la planificación de las adecuadas medidas legales sancionadoras o preventivas.

Además resulta difícil tipificar penalmente situaciones sometidas a un constante cambio tecnológico.

Pese a las críticas que pueda recibir, se puede considerar que el nuevo Código Penal es una herramienta de gran valor para jueces, juristas y abogados a quienes permitirá efectuar construcciones jurídicas artificiosas para penar conductas socialmente reprochables que necesitan tener su cabida en el Código Penal del siglo XXI.

A continuación analizaremos algunos casos concretos de tipificación de delitos relacionados con las TIC's, analizando parte de los artículos donde quedan reflejados, así como las penas que puedan llegarse a imponer.

12.3.1. Delitos relacionados con la pornografía

> Artículo 189.
>
> 1. Será castigado con la pena de prisión de uno a tres años:
>
> a) El que utilizare a menores de edad o a incapaces con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados o para elaborar cualquier clase de material pornográfico, o financiare cualquiera de estas actividades.

A destacar que en el artículo anterior así como en el artículo 186 se hace referencia a venta, difusión o exhibición POR CUALQUIER MEDIO de material pornográfico genérico a menores de edad, o material elaborado mediante utilización de menores de edad o incapaces.

Ejercicio:

- Busca por Internet algún caso famoso de pornografía infantil a través de Internet, y coméntalo en clase.
- ¿Cuál ha sido la sentencia aplicada a los autores (si la ha habido)?
- ¿Cual es el perfil de usuario que comete este tipo de delito?

- ¿Por qué crees que hay gente que se dedica a estas prácticas?

12.3.2. Descubrimiento y revelación de secretos: Correo Electrónico

> Artículo 197.
>
> 1. El que, para descubrir secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

Ejercicio:

- Busca por Internet algún caso de interceptación del correo electrónico y que haya causado polémica.
- ¿Cuáles crees que son las causas de dicha polémica?
- ¿Cuál ha sido la sentencia aplicada a los culpables (si la ha habido)?

12.3.3. Descubrimiento y revelación de secretos: Secretos de Empresa

> Artículo 278.
>
> 1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
>
> 2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

Ejercicio:

- Busca por Internet algún caso de descubrimiento y revelación de secretos de empresa, relacionado con alguna multinacional famosa.
- ¿Cuál ha sido la sentencia aplicada a los autores (si la ha habido)?
- ¿Cuáles crees que son las causas que han llevado a los autores a realizar dichas acciones?

12.3.4. Delitos relacionados con instrumentos tecnológicos para la manipulación de accesos y/o contenidos

Estafa con manipulación informática.

Artículo 248.

1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de terceros.

Ejercicio:

- Busca por Internet algún caso que pueda clasificarse en este tipo de delito.
- ¿Cuál ha sido la sentencia aplicada a los autores (si la ha habido)?
- ¿Cuáles crees que son las causas que han llevado a los autores a realizar dichas acciones?

12.3.5. Daños en programas o documentos electrónicos, soportes o sistemas informáticos

Artículo 264.

1. Será castigado con la pena de prisión de uno a tres años y multa de tres a veinticuatro meses el que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Ejercicio:

- Busca por Internet algún caso que pueda clasificarse en este tipo de delito.
- ¿Cuál ha sido la sentencia aplicada a los autores (si la ha habido)?
- ¿Cuáles crees que son las causas que han llevado a los autores a realizar dichas acciones?

12.3.6. Delitos por agresión a la propiedad intelectual

> **Artículo 270.**
>
> 1. Será castigado con pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de terceros, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.
>
> 2. La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

Ejercicio:

- Busca por Internet algún caso que pueda clasificarse en este tipo de delito y coméntalo en clase con los compañeros.
- Comenta si las siguientes acciones pueden considerarse delito según el artículo anterior:
    - Fotocopiar un libro en su totalidad
    - Copiar un CD de música que no hayamos comprado
    - Hacer una copia de un CD de música que sí hayamos comprado
    - Descargar música MP3 o películas en DIVX desde Internet

12.4. Prevención de Delitos y Tecnologías de doble uso

La única manera solvente para prevenirse ante la agresión criminal en el ámbito de las TICs es aplicar razonablemente las medidas de seguridad que se han explicado a lo largo de las lecciones anteriores. También resulta extraordinariamente importante que la aplicación de dichas medidas se haga de tal forma que resulte prácticamente imposible que por nuestra parte se incurra en conductas delictivas o dudosas.

No podemos cerrar este apartado sin antes exponer la realidad de que en ocasiones determinadas tecnologías revisten un doble papel y son susceptibles de ser utilizadas para la seguridad y, a la vez, para la agresión. Se trata de las llamadas TECNOLOGÍAS DE DOBLE USO, cuyos máximos exponentes son la criptografía y las llamadas "COMINT" o tecnologías de interceptación de comunicaciones. Por su trascendencia global exponemos a continuación la realidad de este fenómeno y sus alarmantes consecuencias en todos los órdenes de la actividad humana: política, social, económica, de investigación, etc.

12.4.1. Los sistemas globales de vigilancia: el concepto "COMINT"

Recientemente se ha elaborado el término COMINT como resultado de la integración de los términos "COMmunications INTelligence" y supone la aplicación de un sistema envolvente de interceptación de comunicaciones a partir de las posibilidades que brindan el desarrollo y la masiva implantación de las TIC's. Hoy en día, COMINT representa una amplia actividad económica que se ocupa de facilitar a sus clientes, ya sean públicos o privados, de contenidos inteligentes a la carta en las áreas de la diplomacia, la economía o la ciencia. Supone la superación del obsoleto esquema espionaje/militar y la implantación más o menos abierta de los nuevos objetivos antes citados.

Los ejemplos más representativos de estas tecnologías COMINT son los sistemas "ECHELON" y "CARNIVORE" que detallamos a continuación.

12.4.2. El sistema "ECHELON"

El sistema tiene sus orígenes en 1947, recién finalizada la II Guerra Mundial, a partir del acuerdo UK/USA con fines claramente militares y de seguridad. Posteriormente se incorporan Canadá, Australia y Nueva Zelanda que actúan en gran medida como suministradores de información y subordinados.

El sistema funciona interceptando de forma indiscriminada enormes cantidades de comunicaciones, sea cual sea el medio utilizado para su transporte y almacenamiento, destacando principalmente las siguientes áreas de escucha:

- Transmisiones por banda ancha (wideband e Internet).
- Facsímil y comunicaciones telefónicas por cable: interceptación de los cables, incluso los submarinos mediante naves equipadas a tal fin.
- Telefonía móvil e Internet WAP.
- Utilización de técnicas de análisis de tráfico.
- Sistemas de reconocimiento de voz.
- Sistema de reconocimiento de facciones visuales sobre filmaciones anónimas.

Posteriormente se selecciona la información sensible y valiosa según los fines encargados al Sistema Echelon, con ayuda de diversos métodos de Inteligencia Artificial (AI) para definir y aplicar PALABRAS CLAVE.

Cada uno de los cinco componentes del Sistema facilita a los demás "DICCIONARIOS DE PALABRAS CLAVE" que se incorporan en los aparatos de interceptación de las comunicaciones y de este modo actúan como "filtro automático". Lógicamente las "palabras" y los "diccionarios" son cambiantes en el tiempo y de acuerdo con los intereses particulares de los países integrantes del Sistema. En un principio ECHELON tuvo una clara vocación militar y de seguridad en el entorno de la Política de Bloques que se materializó en la Guerra Fría siguiente hasta los años ochenta. Posteriormente se reconvirtió en un sistema dual en el que oficialmente se persigue la prevención del crimen internacional organizado (terrorismo, mafias, tráfico de armas y drogas, dictaduras, etc.) pero que en la práctica su incidencia llega a la Economía Global y Políticas Comerciales de empresas y Zonas de Influencia Económica.

En los últimos tiempos ECHELON viene operando con una estructura en estrella de cinco puntas en torno de dos núcleos. Los dos núcleos son estructuras de la NSA (National Security Agency): uno en los Estados Unidos, que coincide con su "cuartel general" en Fort Meade (Maryland), y otro en Inglaterra, al norte de Yorkshire, conocido como Meanwith Hill.

Los puntos de la estrella están ocupados por las estaciones de seguimiento de los socios colaboradores:

- USA (2): Sugar Grove y Yakima.
- New Zealand (1): Wai Pai.
- Australia (1): Geraldtown.
- UK (1): Morwenstow (Cornwell). Existía otra en Hong Kong que finalizó lógicamente con la cesión del territorio a China.

12.4.3. El sistema "CARNIVORE"

El último de los grandes sistemas globales de interceptación y espionaje es el patrocinado por el FBI americano y conocido como CARNIVORE, con una finalidad aparente de luchar contra el crimen organizado y refuerzo de la seguridad USA. La potencialidad de su tecnología y lo versátil y fácil de la aplicación de sus áreas de escucha y atención, ha propiciado el choque frontal entre este novísimo sistema y las organizaciones políticas (Congreso Federal) y medios de comunicación.

Fue desarrollado en el primer semestre del año 2.000, y constituye un sistema automático para intervenir las comunicaciones por Internet aprovechando uno de los principios fundamentales de la red: la descomposición de la información en "paquetes" o grupos de datos uniformes. El sistema llamado CARNIVORE es capaz de detectar e identificar estos "paquetes de información" a través de su implantación en un servidor de un determinado sospechoso. Todo ello en defensa de la seguridad nacional y para reforzar la lucha contra el crimen organizado y tecnológico.

Las asociaciones en defensa de los derechos humanos de U.S.A. no han tardado nada en poner el grito en el cielo, por lo que sin duda se trata de una nueva agresión a la privacidad y confidencialidad de las transacciones de información a través de las TIC'S. En este sentido el Electronic Privacy Information Center (EPIC) ha pedido a un Juez Federal que el F.B.I. permita el acceso de los ISP'S al sistema de vigilancia, si realmente no se va a utilizar éste al margen de la ley.

A principios de agosto de 2.000 el Tribunal de Apelación del distrito de Columbia rechazó un proyecto de ley impulsado por el F.B.I. para intervenir las telecomunicaciones (fundamentalmente telefonía móvil o celular) sin necesidad de solicitar permiso judicial previo, mediante un proyecto de la Comisión Federal de Telecomunicaciones que pretendía forzar a las empresas de telefonía móvil a instalar dispositivos en los aparatos y así conseguir la localización automática de las llamadas. Ello hubiera encarecido un 45% el coste de fabricación de los aparatos.

Con estos dos ejemplos vemos cómo se concretan las pretensiones del F.B.I. de generar un Echelon doméstico, centrado en Internet y en la telefonía móvil, conocido como CARNIVORE. El proyecto ha sido ampliamente rechazado por diferentes instancias judiciales de U.S.A. y por el propio Congreso, por lo que sin duda supone de agresión a los Derechos Humanos de los ciudadanos americanos, por lo menos en su versión inicial. El proyecto se está reconduciendo, al menos formalmente, incluyendo en su estructura la previa autorización judicial, como requisito para que la información obtenida así pueda ser aceptada como prueba en juicio.

12.4.4. Ejercicio 1

Circula por Internet un chiste relacionado con estos sistemas COMINT. Os lo adjuntamos en esta lección para que podáis reflexionar en clase con el resto de compañeros:

> *Un viejo árabe musulmán irakí afincado en Chicago desde hace más de 40 años, quiere plantar patatas en su jardín, pero arar la tierra es un trabajo muy pesado para él. Su único hijo, Ahmed, está estudiando en Francia. El hombre viejo le manda un mail a su hijo explicándole el problema:*
>
> *"Querido Ahmed: Me siento mal porque no voy a poder plantar mi jardín con patatas este año. Estoy muy viejo para arar la tierra. Si tú estuvieras aquí, todos mis problemas desaparecerían. Sé que tú levantarías y removerías toda la tierra por mí. Te quiere papá. "*
>
> *Pocos días después recibe un mail de su hijo:*
>
> *"Querido padre: Por todo lo que más quieras, no toques la tierra de ese jardín. Ahí es donde tengo escondido aquello.*
> *Te quiere Ahmed. "*
> *A las 4 de la madrugada siguiente aparecen la policía local, agentes del FBI, de la CIA, los S.W.A.T, los RANGERS, los MARINES, Steven Seagal, Silvester Stallone y alguno más de élite y representantes del Pentágono que remueven toda la tierra del jardín buscando materiales para construir bombas, ántrax, lo que sea. No encuentran nada y se van.*
>
> *Ese mismo día, el hombre recibe otro mail de su hijo:*
>
> *"Querido padre: Seguramente la tierra ya estará lista para plantar las patatas. Es lo mejor que pude hacer dadas la circunstancias. Te quiere Ahmed."*

12.4.5. Ejercicio 2

Busca en Internet información sobre los sistemas ECHELON y CARNIVORE, así como su aplicación en las redes y sistemas TIC de tu país, e intenta contestar a las siguientes preguntas:

- ¿Qué significa el término "ECHELON"? ¿Qué otras denominaciones recibe?
- ¿Qué elementos componen el sistema ECHELON?
- ¿Qué elementos componen el sistema CARNIVORE?
- Busca un ejemplo de controversia atribuida al sistema ECHELON y relacionada con personalidades famosas.
- Busca algún ejemplo de aplicación de CARNIVORE relacionado con algún TERRORISTA mundialmente conocido.
- ¿Cuál es tu opinión sobre la "legalidad" de dichos sistemas?

12.5. Hacking Ético

Aunque en esta lección hemos hablado únicamente de conductas delictivas, delitos y sus sanciones, debemos dejar muy claro que ser un hacker no significa por definición ser un delincuente.

Actualmente, son muchas las empresas que contratan los servicios de los llamados "Hackers éticos" para detectar las vulnerabilidades de sus sistemas informáticos y conseguir así mejorar las medidas de defensa.

Los hackers éticos, con sus conocimientos, ayudan a definir los perímetros de defensa, realizan ataques "controlados" y consentidos previamente por la organización para comprobar las defensas de ésta, y se forman constantemente para aprender nuevas técnicas de ataques, exploits, vulnerabilidades, etc.

Como decia *Sun Tzu* en el libro "El arte de la Guerra", "Para desplegar una defensa eficaz, la actitud ha de ser la de un ataque a fondo".

La metodología del hacking ético se divide en varias fases:

1. Planificación del ataque
2. Acceso a Internet
3. Test y ejecución del ataque
4. Recogida de datos
5. Análisis
6. Evaluación y diagnóstico
7. Informe final

Una de las herramientas que utilizan los hackers éticos es la metodología OSSTMM (Open Source Security Testing Methodology Manual). Es una metodología para el testeo de cualquier sistema de seguridad, desde guardias y puertas hasta torres de comunicaciones

móviles y satélites. Actualmente es aplicada y utilizada por importantes organizaciones como:

- Instituciones Financieras Españolas
- Departamento del Tesoro de U.S. para testeo de instituciones financieras americanas
- U.S. Navy & Air Force
- Etc.

12.5.1. Ejercicio

- Busca información sobre Hackers Éticos así como el papel que desempeñan actualmente en las empresas especializadas en seguridad informática.
- Busca información sobre la metodología OSSTMM y otras metodologías parecidas.
- Busca información sobre "certificaciones" relacionadas con el Hacking Ético.

12.6. Los 10 delitos y fraudes más usuales en Internet

Como cierre y a modo de ejemplo reproducimos el resumen elaborado por la Comisión Federal de Comercio de los Estados Unidos respecto de los delitos más frecuentes en la Red.

LOS 10 FRAUDES MÁS USUALES EN COMERCIO ELECTRÓNICO

- 1. SUBASTAS: subastar lo que no está disponible, no entregar el objeto, …
- 2. LETRA PEQUEÑA: Ofertar horas gratis de conexión, a cambio de conexión por un año (revocable). Luego la letra pequeña complica las bajas.
- 3. TARJETAS DE CRÉDITO: Falsificación o uso fraudulento de las mismas.
- 4. CAMBIO DE DIAL: Cambiar una conexión a Internet por una telefónica 906 sin informar al usuario.
- 5. ALBERGUE DE PÁGINAS WEB: Gratuito en período de prueba pero que luego se hace imposible de revocar.
- 6. PIRÁMIDES FINANCIERAS de dudosa legalidad.
- 7. VACACIONES GRATIS en lugares paradisíacos.
- 8. OFERTAS DE EMPLEO dudosas a cambio de aportar algo o comprar algo.
- 9. INVERSIONES de alto riesgo y sin garantías.
- 10. CURAS MILAGROSAS. Productos milagrosos de dudosa efectividad.

12.6.1. Ejercicio

Piensa detenidamente las siguientes preguntas y coméntalas luego con el resto de los compañeros:

- Después de analizar todo lo comentado en esta lección, ¿crees que has cometido alguna vez alguna acción que pueda ser considerada como delito?
- ¿Crees que has sido alguna vez víctima de alguno de los delitos comentados a lo largo de la lección?
- Comenta en voz alta alguna conclusión a la que hayas podido llegar después de haber trabajado esta lección.

12.7. Lecturas recomendadas

Si se desea tener más información sobre los temas que se han tratado en esta lección se pueden consultar los siguientes links, donde se ve de una forma más detallada toda la temática expuesta:

http://www.perantivirus.com/sosvirus/hackers/carnivor.htm

http://compnetworking.about.com/od/networksecurityprivacy/l/aa071900a.htm

http://webs.ono.com/usr016/Agika/6temas_relacionados/echelon.htm

http://www.guardiacivil.org/telematicos/formatos/ciberdelincuencia.pdf

http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html

http://www.isecom.org/