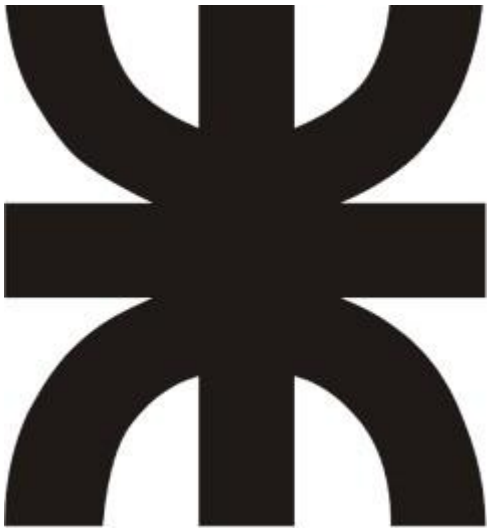


Principales Vulnerabilidades en las componentes de las TIC.

Universidad Tecnológica Nacional
Facultad Regional Mendoza

Ing. David Roco

Tabla de contenido

Principales vulnerabilidades y ataques más importantes a componentes de las TIC.

Ing. David Roco.

1. TIPOS DE ATAQUES INFORMÁTICOS

A la hora de estudiar los distintos tipos de ataques informáticos, podríamos diferenciar en primer lugar entre los ataques activos, que producen cambios en la información y en la situación de los recursos del sistema, y los ataques pasivos, que se limitan a registrar el uso de los recursos y/o a acceder a la información guardada o transmitida por el sistema.

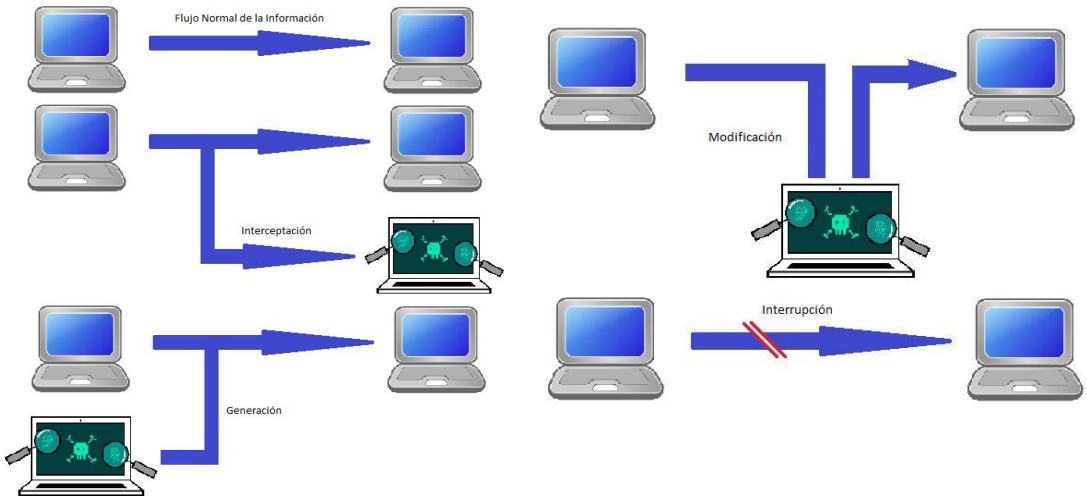


Figura 1: Distintos Tipos de ataques en las Tecnologías de las Información y Comunicación.

1.1. Actividades de reconocimiento de sistemas.

Estas actividades directamente relacionadas con los ataques informáticos, si bien no se consideran ataques como tales ya que no provocan ningún daño, persiguen obtener información previa sobre las organizaciones y sus redes y sistemas informáticos, realizando para ello un escaneo de puertos para determinar qué servicios se encuentran activos o bien un reconocimiento de versiones de sistemas operativos y aplicaciones, por citar dos de las técnicas más conocidas.

Los comandos o herramientas más utilizados son para scaneos de dispositivos y puertos son:

- ping + IP (nos devuelve si hay comunicación con el dispositivo el tamaño del paquete enviado y tiempo de respuesta)

- arping +IP (nos devuelve el MAC Adress, información muy útil ya que con los primeros dos pares de números podemos identificar el fabricante y nos orienta que tipo de dispositivo puede ser.

-tracerouter + IP (nos devuelve los saltos de dispositivos que cruza para llegar al destino).

-nmap -sC -sV + IP (framework que nos devuelve un scaneo de puertos y que tipo de interacción espera cada puerto del host o dispositivo).

-whois “nombre del dominio” (nos devuelve información del registro del dominio).

-nslookup (nos devuelve información de los DNS).

Existen más herramientas para automatizar a las ya nombradas, pero todas se enfocan en devolver información del estado de los dispositivos.

1.2. Detección de vulnerabilidades en los sistemas.

Este tipo de ataques tratan de detectar y documentación las posibles vulnerabilidades de un sistema informático, para a continuación desarrollar alguna herramienta que permita explotarlas fácilmente (herramientas conocidas popularmente como “exploits”).

Metasploit es el framework más utilizado (www.metasploit.com) permite explotar las vulnerabilidades más conocidas en forma accesible para los usuarios que desean ingresar a nuestro sistema por un ingreso no convencional. Metasploit es mantenido por una la comunidad GNU con fines de descubrir nuevos ataques y posibles vulnerabilidades a los sistemas.

1.3. Robo de información mediante la interceptación de mensajes.

Ataques que tratan de interceptar los mensajes de correo o los documentos que se envían a través de redes de ordenadores como Internet, vulnerando de este modo la confidencialidad del sistema informático y la privacidad de sus usuarios.

Acceso a la información por parte de personas no autorizadas. Uso de privilegios no adquiridos. Su detección es difícil, a veces no deja huellas. Ejemplos: Copias ilícitas de programas, escucha en línea de datos.

1.4. Modificación del contenido y secuencia de los mensajes transmitidos.

En estos ataques los intrusos tratan de reenviar mensajes y documentos que ya habían sido previamente transmitidos en el sistema informático, tras haberlos modificado de forma maliciosa (por ejemplo, para generar una nueva transferencia bancaria contra la cuenta de la víctima del ataque). También se conocen como “ataques de repetición” (“replay attacks”).

Ejemplos: Modificación de bases de datos, modificación de elementos del Hardware.

1.5. Análisis del tráfico.

Estos ataques persiguen observar los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando para ello herramientas como los "sniffers". Así, se conoce como "eavesdropping" a la interceptación del tráfico que circula por una red de forma pasiva, sin modificar su contenido.

Los analizadores de paquetes tienen diversos usos, como monitorear redes para detectar y analizar fallos, o para realizar ingeniería inversa en protocolos de red. También es habitual su uso para fines maliciosos, como robar contraseñas, interceptar correos electrónicos, espiar conversaciones de chat, etc.

Una organización podría protegerse frente a los "sniffers" recurriendo a la utilización de redes conmutadas ("switches" en lugar de "hubs") y de redes locales virtuales (VLAN).

No obstante, en redes locales que utilizan "switches" (es decir, en redes conmutadas), un atacante podría llevar a cabo un ataque conocido como "MAC flooding" para provocar un desbordamiento de las tablas de memoria de unswitch (tablas denominadas CAM por los fabricantes, "Content Addresable Memory") para conseguir que pase a funcionar como un simple "hub" y retransmita todo el tráfico que recibe a través de sus puertos (al no poder "recordar" qué equipos se encuentran conectados a sus distintas bocas o puertos por haber sido borradas sus tablas de memoria).

Por otra parte, en las redes VLAN (redes locales virtuales) un atacante podría aprovechar el protocolo DTP (Dynamic Trunk Protocol), utilizado para poder crear una VLAN que atraviese varios switches, para intentar saltar de una VLAN a otra, rompiendo de este modo el aislamiento físico impuesto por la organización para separar sus distintas redes locales.

1.6. Ataques de suplantación de la identidad.

IP Spoofing.

Los ataques de suplantación de la identidad presentan varias posibilidades, siendo una de las más conocidas la denominada "IP Spoofing" ("enmascaramiento de la dirección IP"), mediante la cual un atacante consigue modificar la cabecera de los paquetes enviados a un determinado sistema informático para simular que proceden de un equipo distinto al que verdaderamente los ha originado. Así, por ejemplo, el atacante trataría de seleccionar una dirección IP correspondiente a la de un equipo legítimamente autorizado para acceder al sistema que pretende ser engañado.

Los propietarios de las redes y operadores de telecomunicaciones podrían evitar en gran medida el "IP Spoofing" implantando filtros para que todo el tráfico saliente de sus redes llevara

asociado una dirección IP de la propia red desde la que se origina el tráfico. Otro posible ataque sería el secuestro de sesiones ya establecidas ("hijacking", en el ámbito informático hace referencia a toda técnica ilegal que lleve consigo el adueñarse o robar algo por parte de un atacante.), donde el atacante trata de suplantar la dirección IP de la víctima y el número de secuencia del próximo paquete de datos que va a transmitir. Con el secuestro de sesiones se podrían llevar a cabo determinadas operaciones en nombre de un usuario que mantiene una sesión activa en un sistema informático como, por ejemplo, transferencias desde sus propias cuentas corrientes si en ese momento se encuentra conectado al servidor de una entidad financiera.

DNS Spoofing.

Los ataques de falsificación de DNS pretenden provocar un direccionamiento erróneo en los equipos afectados, debido a una traducción errónea de los nombres de dominio a direcciones IP, facilitando de este modo la redirección de los usuarios de los sistemas afectados hacia páginas Web falsas o bien la interceptación de sus mensajes de correo electrónico.

Para ello, en este tipo de ataque los intrusos consiguen que un servidor DNS legítimo acepte y utilice información incorrecta obtenida de un ordenador que no posee autoridad para ofrecerla.

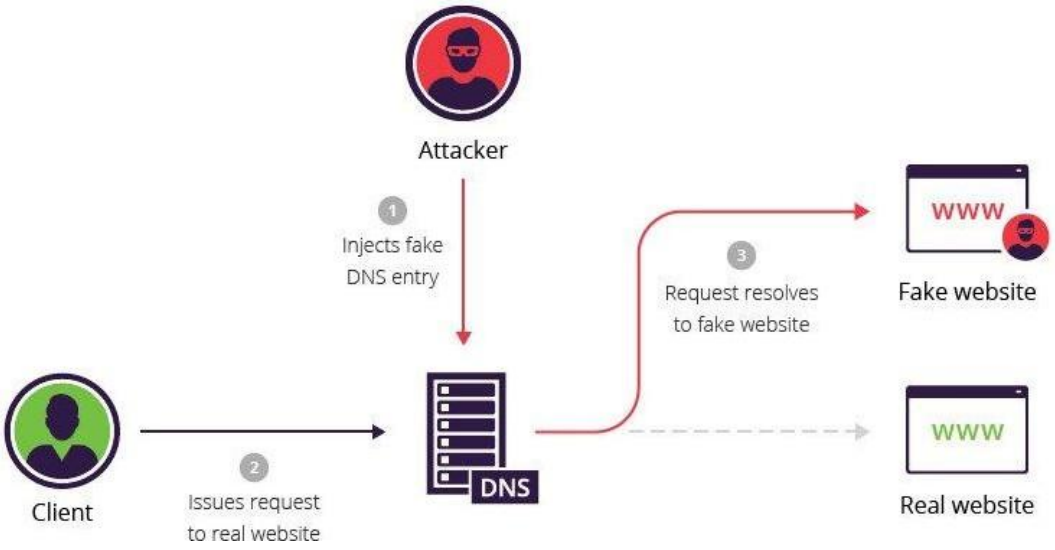
De este modo, se persigue "inyectar" información falsa en el base de datos del servidor de nombres, procedimiento conocido como "envenenamiento de la caché del servidor DNS", ocasionando con ello serios problemas de seguridad, como los que se describen de forma más detallada a continuación:

• Redirección de los usuarios del servidor DNS atacado a Websites erróneos en Internet, que simulan ser los Websites reales. De este modo, los atacantes podrían provocar que los usuarios descargasen de Internet software modificado en lugar del legítimo (descarga de código dañino, como virus o troyanos, desde Websites maliciosos).

• La manipulación de los servidores DNS también podría estar detrás de algunos casos de "phishing", mediante la redirección de los usuarios hacia páginas Web falsas creadas con la intención de obtener datos confidenciales, como sus claves de acceso a servicios de banca electrónica.

• Otra posible consecuencia de la manipulación de los servidores DNS serían los ataques de Denegación de Servicio (DoS), al provocar la redirección permanente hacia otros servidores en lugar de hacia el verdadero, que de este modo no podrá ser localizado y, en consecuencia, visitado por sus legítimos usuarios.

• Los mensajes de correo podrían ser redirigidos hacia servidores de correo no autorizados, donde podrían ser leídos, modificados o eliminados. Para ello, basta con modificar el registro MX ("Mail Exchanger") de la tabla de datos del servidor DNS atacado. Por otra parte, un servidor DNS afectado por este tipo de ataque podría provocar falsas respuestas en los restantes servidores DNS que confíen en él para resolver un nombre de dominio, siguiendo el modelo jerárquico del servicio DNS, extendiendo de este modo el alcance del ataque de "DNS Spoofing".



SMTP Spoofing.

El envío de mensajes con remitentes falsos(“masquerading”) para tratar de engañar al destinatario o causar un daño en la reputación del supuesto remitente es otra técnica frecuente de ataque basado en la suplantación de la identidad de un usuario. De hecho, muchos virus emplean esta técnica para facilitar su propagación, al ofrecer información falsa sobre el posible origen de la infección. Asimismo, este tipo de ataque es muy utilizado por los “spammers”, que envían gran cantidad de mensajes de “correo basura” bajo una identidad falsa.

En la actualidad, falsificar mensajes de correo resulta bastante sencillo porque el protocolo SMTP carece totalmente de autenticación. Así, un servidor configurado para aceptar conexiones SMTP en el puerto 25 podría ser utilizado por un usuario externo a la organización, empleando los comandos propios del protocolo, para que envíe mensajes que aparenten tener un origen seleccionado por el atacante cuando realmente tienen otro distinto. La dirección de origen puede ser una dirección existente o una inexistente con el formato adecuado. No obstante, los servidores de correo también podrían ser configurados para no aceptar envíos de mensajes desde equipos externos a la red local.

Captura de cuentas de usuario y contraseñas.

También es posible suplantar la identidad de los usuarios mediante herramientas que permitan capturar sus contraseñas, como los programas de software espía o los dispositivos hardware especializados que permitan registrar todas las pulsaciones en el teclado de un ordenador (“keyloggers”). De hecho, es posible localizar soluciones disponibles en el mercado como KeyGhost (www.keyghost.com) o Key-Logger(www.keylogger.com). Se conoce como “Snooping” a la técnica que permite observar la actividad de un usuario en su ordenador para obtener determinada información de interés, como podrían ser sus contraseñas. Los programas que permiten realizar esta

actividad se conocen con el nombre de “snoopers”, los cuales pueden ser troyanos u otros “parásitos” que monitorizan dispositivos de entrada como los ratones y los teclados. Por otra parte, mediante las técnicas de “Ingeniería Social” un usuario podría ser engañado por una persona ajena a la organización para que le facilite sus contraseñas y claves de acceso.

1.7. Modificaciones del tráfico y de las tablas de enrutamiento.

Los ataques de modificación del tráfico y de las tablas de enrutamiento persiguen desviar los paquetes de datos de su ruta original a través de Internet, para conseguir, por ejemplo, que atraviesen otras redes o equipos intermedios antes de llegar a su destino legítimo, para facilitar de este modo las actividades de interceptación de datos. Así, la utilización del encaminamiento fuente (“source routing”) en los paquetes IP permite que un atacante pueda especificar una determinada ruta prefijada, que podría ser empleada como ruta de retorno, saltándose todas las reglas de enrutamiento definidas en la red. De este modo, utilizando además el “IP Spoofing”, un atacante se podría hacer pasar por cualquier máquina en la que el destino pueda confiar, para recibir a continuación los datos correspondientes al equipo que está suplantando. También es posible llevar a cabo una modificación de las tablas de enrutamiento, utilizando para ello determinados paquetes de control del tráfico, conocidos como paquetes “ICMP Redirect”, que permiten alterar la ruta a un determinado destino. Otra alternativa sería la de modificar las rutas a través de los propios protocolos de enrutamiento utilizados, como RIP (puerto UDP 520) o BGP. Al modificar las rutas, el tráfico atravesará otros equipos y redes antes de alcanzar su destinatario final, facilitando de este modo el “sniffing”.

1.8. Conexión no autorizada a equipos y servidores.

Existen varias posibilidades para establecer una conexión no autorizada a otros equipos y servidores, entre las que podríamos destacar las siguientes:

- Violación de sistemas de control de acceso.
- Explotación de “agujeros de seguridad” (“exploits”).
- Utilización de “puertas traseras” (“backdoors”), conjunto de instrucciones no documentadas dentro de un programa o sistema operativo, que permiten acceder o tomar el control del equipo saltándose los controles de seguridad.
- Utilización de “rootkits”, programas similares a los troyanos, que se instalan en un equipo reemplazando a una herramienta o servicio legítimo del sistema operativo. Los “rootkits”, además de cumplir con las funciones de la herramienta o servicio que reemplazan en el equipo para no despertar sospechas, incorporan otras funciones ocultas que facilitan, entre otras cosas, el control remoto del equipo comprometido.
- “Wardialing”: conexión a un sistema informático de forma remota a través de un módem. Los “wardialers” son dispositivos que permiten realizar de forma automática multitud de llamadas telefónicas para tratar de localizar módems que se encuentren a la espera de nuevas conexiones y que no hayan sido protegidos y configurados de forma adecuada. Tampoco debemos olvidar las posibles pérdidas o robos de equipos que contienen

información sensible y que, por este motivo, puedan caer en manos de personas ajenas a la organización, las cuales podrían tratar de tomar el control de estos equipos para extraer la información que almacenan o para utilizarlos en conexiones remotas a la red de la organización.

1.9. Consecuencias de las conexiones no autorizadas a los sistemas informáticos.

Las conexiones no autorizadas a los sistemas informáticos pueden acarrear graves consecuencias para la organización afectada por este tipo de ataques e incidentes, entre las que podríamos destacar las siguientes:

- Acceso a información confidencial guardada en un servidor. Los atacantes incluso podrían tener acceso a datos y ficheros que habían sido "borrados" del sistema.
- Utilización inadecuada de determinados servicios por parte de usuarios no autorizados, suponiendo una violación de los permisos establecidos en el sistema.
- Transmisión de mensajes mediante un servidor de correo por parte de usuarios ajenos a la organización ("mail relaying"). Esto podría facilitar el reenvío masivo de mensajes de spam a través de un servidor SMTP configurado de forma inadecuada.
- Utilización de la capacidad de procesamiento de los equipos para otros fines, como, por ejemplo, para tratar de romper las claves criptográficas de otros sistemas.
- Creación de nuevas cuentas de usuario con privilegios administrativos, que faciliten posteriores accesos al sistema comprometido.
- Consumo del ancho de banda de la red de la organización para otros fines.
- Almacenamiento de contenidos ilegales en los equipos: muchos atacantes aprovechan los equipos comprometidos de una organización para guardar y distribuir copias piratas de software, canciones o vídeos, pornografía, etcétera.
- Modificación o destrucción de archivos y documentos guardados en un servidor.
- "Website vandalism": modificación del contenido y de la apariencia de unas determinadas páginas Web pertenecientes a la organización.

1.10. Introducción en el sistema de "malware" (código malicioso).

Entendemos por código malicioso o dañino ("malware") cualquier programa, documento o mensaje susceptible de causar daños en las redes y sistemas informáticos. Así, dentro de esta definición estarían incluidos los virus, troyanos, gusanos, bombas lógicas, etcétera. Cabe destacar la rapidez de propagación de estos programas dañinos a través del correo electrónico, las conexiones mediante redes de ordenadores y los nuevos servicios de intercambio de ficheros (P2P) o de mensajería instantánea. Hasta ahora algunos técnicos y administradores de redes se centraban en otros problemas de mayor nivel de complejidad, como los ataques contra servidores por parte de crackers o el análisis de agujeros de seguridad, relegando la protección contra los virus y códigos dañinos a un segundo plano, ya que se consideraba como una tarea que realizan de forma automática los programas antivirus. Sin embargo, las nuevas formas de propagación de estos

códigos dañinos y los graves problemas que ocasionan a las empresas y a los usuarios obligan a replantearse esta estrategia, prestando una mayor atención a la contención y erradicación de este tipo de ataques e incidentes de seguridad informática.

1.11. Ataques de "Cross-Site Scripting"(XSS).

Los ataques de "Cross-Site Scripting" consisten básicamente en la ejecución de código "Script" (como Visual Basic Script o Java Script) arbitrario en un navegador, en el contexto de seguridad de la conexión a un determinado servidor Web.

Son ataques dirigidos, por lo tanto, contra los usuarios y no contra el servidor Web. Mediante "Cross-Site Scripting", un atacante pueda realizar operaciones o acceder a información en un servidor Web en nombre del usuario afectado, suplantando su identidad. Estos ataques se pueden producir cuando el servidor Web no filtra correctamente las peticiones HTTP de los usuarios, los cuales pueden enviar cadenas de texto a través de formularios o directamente a través de la propia dirección URL de la página Web. Estas cadenas de texto podrían incluir código en lenguaje "Script", que a su vez podría ser reenviado al usuario dentro de una página Web dinámica generada por el servidor como respuesta a una determinada petición, con la intención de que este código "Script" se ejecutase en el navegador del usuario, no afectando por lo tanto al servidor Web, pero sí a algunos de los usuarios que confían en él. Entre las posibilidades de ataque a través de "Cross-Site Scripting" podríamos destacar las siguientes:

- Obtención de "cookies" e identificadores de usuarios, que permiten capturar sesiones y suplantar la identidad de los afectados.
- Modificación de contenidos para engañar al visitante víctima del ataque "Cross-Site Scripting", con la posibilidad de construir formularios para robar datos sensibles, como contraseñas, datos bancarios, etcétera.

1.12. Ataques de Inyección de Código SQL.

SQL, "Structured Query Language" (Lenguaje de Consulta Estructurado), es un lenguaje textual utilizado para interactuar con bases de datos relacionales. La unidad típica de ejecución de SQL es la consulta ("Query"), conjunto de instrucciones que permiten modificar la estructura de la base de datos (mediante instrucciones del tipo "Data Definition Language", DDL) o manipular el contenido de la base de datos (mediante instrucciones del tipo "Data Manipulation Language", MDL). En los servidores Web se utiliza este lenguaje para acceder a bases de datos y ofrecer páginas dinámicas o nuevas funcionalidades a sus usuarios.

El ataque por inyección de código SQL se produce cuando no se filtra de forma adecuada la información enviada por el usuario. Un usuario malicioso podría incluir y ejecutar textos que representen nuevas sentencias SQL que el servidor no debería aceptar. Este tipo de ataque es independiente del sistema de bases de datos subyacente, ya que depende únicamente de una inadecuada validación de los datos de entrada.

Como consecuencia de estos ataques y, dependiendo de los privilegios del usuario de base de datos bajo el cual se ejecutan las consultas, se podría acceder no sólo a las tablas relacionadas con la operación de la aplicación del servidor Web, sino también a las tablas de otras bases de datos

alojadas en el mismo servidor Web. También pueden propiciar la ejecución de comandos arbitrarios del sistema operativo del equipo del servidor Web.

1.13. Ataques contra los sistemas criptográficos.

Los ataques contra la seguridad de los sistemas criptográficos persiguen descubrir las claves utilizadas para cifrar unos determinados mensajes o documentos almacenados en un sistema, o bien obtener determinada información sobre el algoritmo criptográfico utilizado. Podemos distinguir varios tipos de ataques contra los sistemas criptográficos:

- Los "ataques de fuerza bruta", que tratan de explorar todo el espacio posible de claves para romper un sistema criptográfico.
- Los "ataques de diccionario", que trabajan con una lista de posibles contraseñas: palabras de un diccionario en uno o varios idiomas, nombres comunes, nombres de localidades o accidentes geográficos, códigos postales, fechas del calendario, etcétera.
- Los ataques contra el diseño del algoritmo.
- Los ataques contra los dispositivos hardware o software que lo implementan. Las distintas técnicas de criptoanálisis: criptoanálisis lineal, diferencial, técnicas de análisis estadístico de frecuencias, etcétera.

1.14. Fraudes, engaños y extorsiones.

Los fraudes y estafas financieros a través de Internet se han hecho muy frecuentes en estos últimos años. Se utiliza el término de "phishing" para referirse al tipo de ataques que tratan de obtener los números de cuenta y las claves de acceso a servicios bancarios, para realizar con ellos operaciones fraudulentas que perjudiquen a los legítimos propietarios. Generalmente, se utilizan páginas Web falsas que imitan a las originales de los servicios bancarios que pretenden suplantar.

El "pharming" es una variante del "phishing" en la que los atacantes utilizan un virus que conecta a las víctimas desde su ordenador a páginas falsas en lugar de a las legítimas correspondientes a sus propias entidades financieras, para sustraer sus datos (números de cuenta y claves de acceso). El "pharming" y el "phishing" también pueden ser empleados para robar y utilizar de forma fraudulenta números de tarjetas de crédito.

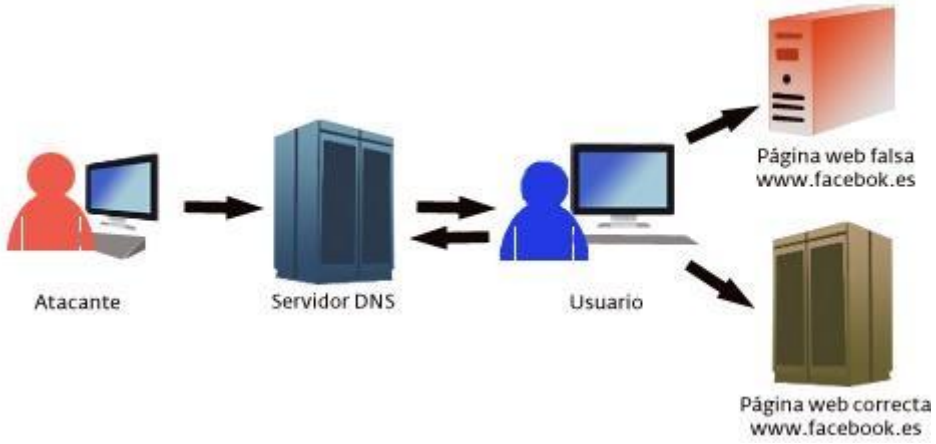


Figura 2: Estructura de un ataque pharming.

Estos datos podrían ser utilizados para realizar ataques del tipo "salami", consistentes en la repetición de gran cantidad de pequeñas operaciones, como transferencias bancarias de importe reducido, que podrían pasar inadvertidas a nivel individual, pero que en conjunto ocasionan un importante daño económico. Por otra parte, se han desarrollado virus y otros programas dañinos para facilitar las extorsiones y estafas a usuarios de Internet. Es lo que se conoce como "ransom-ware", software malicioso cuyo fin es el lucro de su creador por medio de rescates. Así, podríamos mencionar casos como el del troyano PGPCoder, de mayo de 2005, que cifraba determinados archivos en el sistema infectado, dejando a continuación un mensaje solicitando dinero a los usuarios perjudicados si querían volver a restaurar sus ficheros (mediante el envío de una clave para descifrarlos). También podemos considerar dentro de este tipo de ataques la difusión de correos electrónicos con ofertas falsas o engañosas, así como la publicación de falsas noticias en foros y grupos de noticias, con distintas intenciones, como podría el caso de intentar alterar el valor de las acciones de una empresa (de hecho, ya se han producido varias de estas actuaciones en Estados Unidos y en Europa). En mayo de 2005 se informaba de varios casos de "crackers" que habían conseguido "secuestrar" archivos o páginas Web de otros usuarios, solicitando un rescate para proceder a su "liberación". Para ello, los atacantes codificaban los documentos afectados para impedir que su propietario los pudiera abrir, solicitando a continuación un importe de 200 dólares en concepto de "rescate" para devolver al usuario el acceso a sus archivos.

De hecho, los casos de chantaje y extorsión on-line se están extendiendo en países como Estados Unidos, a tenor de los últimos estudios publicados. En muchos de estos casos, los chantajistas aseguran tener información confidencial sobre la empresa y amenazan con difundirla si no reciben una determinada cantidad de dinero. Se ha podido comprobar que un porcentaje elevado de estas amenazas eran realizadas por un antiguo empleado de la propia empresa con acceso a datos internos o, incluso, alguien de la competencia.

También han aumentado los casos de extorsión a particulares a través de Internet, consistentes en la publicación o amenaza de publicación de alguna información difamatoria sobre la víctima, utilizando algún medio de la Red (páginas Web, foros, grupos de noticias…). En marzo de 2006 se anunciaba la propagación de un nuevo tipo de virus a través de Internet, capaz de bloquear el equipo informático de sus víctimas, solicitando un "rescate" de 300 dólares para revelar la clave para liberar el equipo en cuestión.

1.15. Denegación del Servicio (Ataques DoS – Denial of Service).

Los ataques de Denegación de Servicio (DoS) consisten en distintas actuaciones que persiguen colapsar determinados equipos o redes informáticos, para impedir que puedan ofrecer sus servicios a sus clientes y usuarios. Para ello, existen varias posibilidades de conseguirlo:

- Ejecutar algunas actividades que produzcan un elevado consumo de los recursos de las máquinas afectadas: procesador, memoria y/o disco duro, provocando una caída en su rendimiento. Entre ellas podríamos citar el establecimiento de múltiples conexiones simultáneas, el envío masivo de ficheros de gran tamaño o los ataques lanzados contra los puertos de configuración de los routers.
- Provocar el colapso de redes de ordenadores mediante la generación de grandes cantidades de tráfico, generalmente desde múltiples equipos.

- Transmisión de paquetes de datos malformados o que incumplan las reglas de un protocolo, para provocar la caída de un equipo que no se encuentre preparado para recibir este tipo de tráfico malintencionado.
- Sabotajes mediante routers "maliciosos", que se encarguen de proporcionar información falsa sobre tablas de enrutamiento que impidan el acceso a ciertas máquinas de la red.
- Activación de programas "bacteria", cuyo objetivo es replicarse dentro de un sistema informático, consumiendo la memoria y la capacidad del procesador hasta detener por completo al equipo infectado.
- Envío masivo de miles mensajes de correo electrónico ("mail bombing"), provocando la sobrecarga del servidor de correo y/o de las redes afectadas.
- "Ataque reflector" ("reflector attack"), que persigue generar un intercambio ininterrumpido de tráfico entre dos o más equipos para disminuir su rendimiento o incluso conseguir su completo bloqueo dentro de una red informática.
- Incumplimiento de las reglas de un protocolo. Para ello, se suelen utilizar protocolos no orientados a conexión, como UDP o ICMP, o bien el protocolo TCP sin llegar a establecer una conexión completa con el equipo atacado.

En relación con esta última posibilidad, el incumplimiento de las reglas de un protocolo, podemos enumerar varios tipos de ataques que han ocasionado numerosos problemas a distintos tipos de sistemas informáticos en los últimos años:

- **"El ping de la muerte":** mediante el comando "ping –l 65510 ip_victima", que envía un paquete IP de un tamaño superior a los 65.536 bytes, provocando el reinicio o "cuelgue" del equipo víctima que lo recibe (si no ha sido protegido frente a esta eventualidad).
- **"Land Attack":** debido a un error en la implementación del protocolo TCP/IP en algunos sistemas Windows, se consigue "colgar" un equipo vulnerable mediante el envío de una serie de paquetes maliciosamente construidos, en los que la dirección y el puerto de origen son idénticos a la dirección y el puerto de destino.
- **"Supernuke"** o **"Winnuke":** ataque contra algunos sistemas Windows, que se quedan "colgados" o disminuyen drásticamente su rendimiento al recibir paquetes UDP manipulados (fragmentos de paquetes "Out-Of-Band") dirigidos contra el puerto 137.
- **"Teardrop":** tipo de ataque consistente en el envío de paquetes TCP/IP fragmentados de forma incorrecta. Los equipos vulnerables que no hayan sido conveniente parcheados se "cuelgan" al recibir este tipo de paquetes maliciosos.
- **"SYN Flood":** este ataque se basa en un incumplimiento de las reglas básicas del protocolo TCP por parte del cliente. Al establecer la conexión mediante el procedimiento "three-way handshake", se envía una petición de conexión al equipo víctima, pero no se responde a la aceptación de la conexión por parte de este equipo (generalmente se facilita una dirección IP falsa). El equipo víctima deja la conexión en estado de "semi-abierta", consumiendo de este modo recursos de la máquina. Las conexiones "semi-abiertas" caducan al cabo de un cierto tiempo, liberando sus recursos. No obstante, si se envían muchas peticiones de conexión siguiendo el ataque de SYN Flood, se colapsarán los recursos del equipo víctima, que no podrá atender nuevas conexiones legítimas.

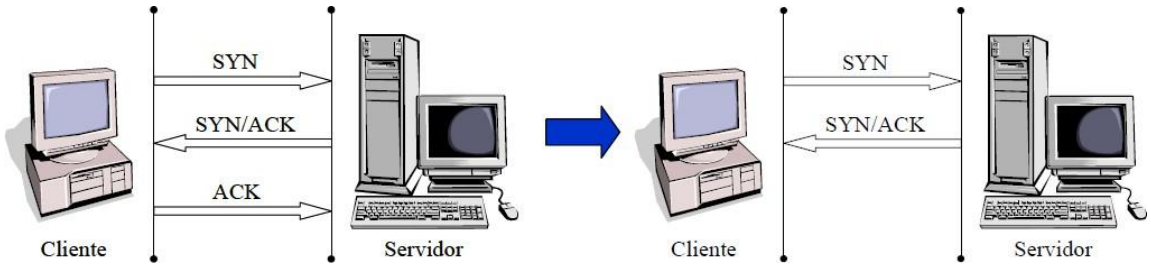


Figura 3: Esquema de funcionamientos de protocolo de comunicación.

Asimismo, podemos señalar otros tipos de ataques de Denegación de Servicio (DoS) que se han hecho famosos en los últimos años:

• **"Connection Flood":** tipo de ataque que consiste en intentar establecer cientos o miles de conexiones simultáneas contra un determinado servidor víctima del ataque, con lo que se consumen sus recursos y se degrada de forma notable su respuesta ante usuarios legítimos. Este tipo de ataques se han lanzado con éxito contra los Websites de algunas empresas, como en el caso de la tienda de juguetes on-line eToys, cuyo Website llegó a estar colapsado durante varios días por un ataque coordinado llevado a cabo desde cientos de equipos.

• **"Net Flood":** ataque similar al que se ha expuesto anteriormente, consiste en el envío de tráfico masivo contra una determinada red conectada a Internet, para tratar de degradar su funcionamiento.

• **"Smurf" ("pitufo"):** ataque DoS que se lleva a cabo mediante el envío de una gran cantidad de mensajes de control ICMP (Internet Control Message Protocol) de solicitud de eco dirigidos a direcciones de difusión (direcciones "broadcast"), empleando para ello la dirección del equipo víctima del incidente, que se verá desbordado por la cantidad de mensajes de respuesta generados en la red de equipos sondeados, que actúa como una red amplificadora del ataque.

• **"Bomba UDP":** se considera un ataque del tipo "reflector attack" ("ataque reflector"), en el que se emplea el protocolo UDP (User Datagram Protocol) y uno de los muchos servicios que responden a los paquetes que reciben para crear una congestión en la red que provoque el DoS, generando un flujo de paquetes UDP continuo entre dos sistemas seleccionados. Así, por ejemplo,
se podría elegir en el primer equipo el servicio "chargen" (es una herramienta de pruebas disponible en el puerto 9, que genera una serie de caracteres), mientras que en el segundo equipo se podría hacer uso del servicio "echo" (servicio disponible en el puerto 7, que responde a cada uno de los paquetes que recibe), para de este modo conseguir un intercambio interminable de paquetes UDP entre los dos equipos, generando una especie de "tormenta de paquetes UDP". Para evitar este tipo de ataques conviene desactivar estos servicios en los equipos de la red, así como filtrar este tráfico a través de un cortafuego.

• **"Snork UDP":** ataque similar al anteriormente descrito ("bomba UDP"), dirigido contra sistemas Windows. En este caso se emplea un paquete de datos UDP con origen en el puerto 7 (servicio "echo") o el puerto 19 (servicio "chargen"), utilizando como puerto de destino el 135, en el que se ubica el servicio de localización de Microsoft a través del protocolo NetBIOS. De este modo, se consigue un intercambio de paquetes UDP innecesario que reduce el rendimiento de los equipos y de la red afectada. Se trata, por tanto, de otro ataque del tipo "reflector attack".

Hay que tener en cuenta que en los ataques de Denegación del Servicio (DoS) el atacante suele ocultar su verdadera dirección mediante técnicas de "IP Spoofing". Además, en numerosas ocasiones se han empleado este tipo de ataques para encubrir otros ataques simultáneos que pretendían comprometer un sistema o red informático.

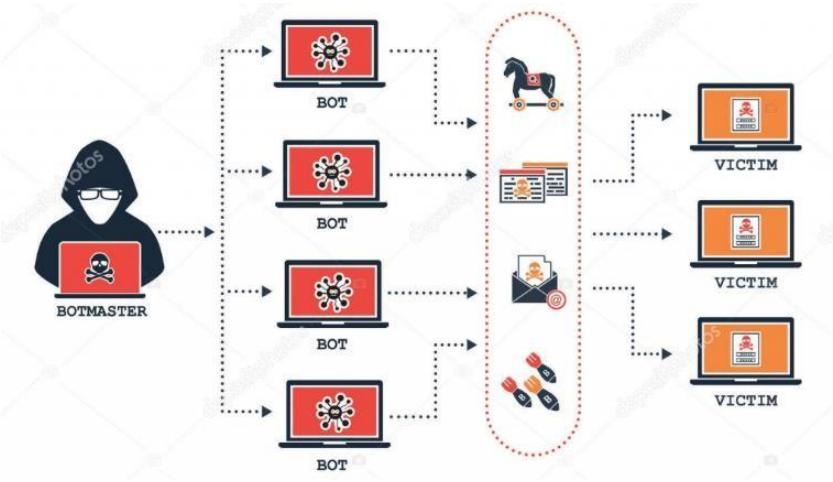


Figura 4: Estructura de un ataque DoS.

1.16. Ataques de Denegación de Servicio Distribuidos (DDoS).

Los Ataques de Denegación de Servicio Distribuidos (DDoS) se llevan a cabo mediante equipos "zombis". Los equipos "zombis" son equipos infectados por virus o troyanos, sin que sus propietarios lo hayan advertido, que abren puertas traseras y facilitan su control remoto por parte de usuarios remotos. Estos usuarios maliciosos suelen organizar ataques coordinados en los que pueden intervenir centenares o incluso miles de estos equipos, sin que sus propietarios y usuarios legítimos lleguen a ser conscientes del problema, para tratar de colapsar las redes y los servidores objeto del ataque. Generalmente los equipos "zombis" cuentan con una conexión ADSL u otro tipo de conexión de banda ancha, de tal modo que suelen estar disponibles las 24 horas. Para luchar de forma eficaz contra este tipo de ataques es necesario contar con la colaboración de los proveedores de acceso a Internet, para filtrar o limitar el tráfico procedente de los equipos que participan en el ataque. En este sentido, cabría destacar una iniciativa pionera llevada a cabo a finales de mayo de 2005 por la FTC (Comisión Federal de Comercio estadounidense) para tratar de identificar y poner en "cuarentena" a los clientes de los proveedores de acceso a Internet cuyos ordenadores se hayan convertido (seguramente sin su conocimiento) en una máquina "zombi". Los equipos "zombis" también están siendo utilizados por los "spammers" para la difusión masiva de sus mensajes de correo no solicitados. Incluso en algunos países ya se han dado casos de alquiler de redes "zombi" (conocidas como "botnets") para poder llevar a cabo ataques de Denegación de Servicio Distribuidos (DDoS). Así, por ejemplo, en el Reino Unido varios jóvenes "crackers" alquilaban redes con 30.000 ordenadores "zombi" por un precio de 100 dólares la hora para realizar ataques masivos de denegación de servicio. Y en el verano de 2004 un empresario de Massachussets pagó a tres "crackers" menores de edad para realizar ataques con una red "zombi" de 10.000 equipos contra los servidores de las empresas de la competencia. Asimismo, la disponibilidad de herramientas como TFN ("Tribe Flood Net") y TFN2K facilita el desarrollo de este tipo de ataques. En concreto, esta herramienta mejora la comunicación y control de los equipos "zombis" utilizando paquetes TCP, UDP o ICMP, así como técnicas criptográficas (como el algoritmo CAST-256) para dificultar la detección del atacante.

TFN2K permite programar distintos tipos de ataques ("Flooding", "Smurf", etc.) y cambia de forma frecuente las cabeceras de los paquetes que envía a los equipos "zombis" para dificultar su detección por los Sistemas de Detección de Intrusiones (IDS).

2. CLASIFICACIÓN DE LOS INTRUSOS EN LAS REDES.

2.1. Hackers.

Los hackers son intrusos que se dedican a estas tareas como pasatiempo y como reto técnico, entran en los sistemas informáticos para demostrar y poner a prueba su inteligencia y conocimientos de los entresijos de Internet, pero no pretenden provocar daños en estos sistemas. Sin embargo, hay que tener en cuenta que pueden tener acceso a información confidencial, por lo que su actividad está siendo considerada como un delito en bastantes países de nuestro entorno. El perfil típico de un hacker es el de una persona joven, con amplios conocimientos de informática y de Internet (son auténticos expertos en varios lenguajes de programación, arquitectura de ordenadores, servicios y protocolos de comunicaciones, sistemas operativos, etcétera), que invierte un importante número de horas a la semana a su afición.

En la actualidad muchos "hackers" defienden sus actuaciones alegando que no persiguen provocar daños en los sistemas y redes informáticas, ya que sólo pretenden mejorar y poner a prueba sus conocimientos. Sin embargo, el acceso no autorizado a un sistema informático se considera por sí mismo un delito en muchos países, puesto que, aunque no se produzca ningún daño, se podría revelar información confidencial. Por otra parte, la actividad de un "hacker" podría provocar otros daños en el sistema: dejar "puertas traseras" que podrían ser aprovechadas por otros usuarios maliciosos, ralentizar su normal funcionamiento, etcétera. Además, la organización debe dedicar tiempo y recursos para detectar y recuperar los sistemas que han sido comprometidos por un "hacker".

2.2. Crackers ("blackhats").

Los crackers son individuos con interés en atacar un sistema informático para obtener beneficios de forma ilegal o, simplemente, para provocar algún daño a la organización propietaria del sistema, motivados por intereses económicos, políticos, religiosos, etcétera.

A principios de los años setenta comienzan a producirse los primeros casos de delitos informáticos, provocados por empleados que conseguían acceder a los ordenadores de sus empresas para modificar sus datos: registros de ventas, nóminas.

2.3. Sniffers.

Los sniffers son individuos que se dedican a rastrear y tratar de recomponer y descifrar los mensajes que circulan por redes de ordenadores como Internet.

2.4. Phreakers.

Los Phreakers son intrusos especializados en sabotear las redes telefónicas para poder realizar llamadas gratuitas. Los Phreakers desarrollaron las famosas "cajas azules", que podían emitir distintos tonos en las frecuencias utilizadas por las operadoras para la señalización interna de sus redes, cuando éstas todavía eran analógicas.

2.5. Spammers.

Los spammers son los responsables del envío masivo de miles de mensajes de correo electrónico no solicitados a través de redes como Internet, provocando el colapso de los servidores y la sobrecarga de los buzones de correo de los usuarios.

Además, muchos de estos mensajes de correo no solicitados pueden contener código dañino (virus informáticos) o forman parte de intentos de estafa realizados a través de Internet (los famosos casos de "phishing").

2.6. Piratas informáticos.

Los piratas informáticos son los individuos especializados en el pirateo de programas y contenidos digitales, infringiendo la legislación sobre propiedad intelectual.

2.7. Creadores de virus y programas dañinos.

Se trata de expertos informáticos que pretenden demostrar sus conocimientos construyendo virus y otros programas dañinos, que distribuyen hoy en día a través de Internet para conseguir una propagación exponencial y alcanzar así una mayor notoriedad.

En estos últimos años, además, han refinado sus técnicas para desarrollar virus con una clara actividad delictiva, ya que los utilizan para obtener datos sensibles de sus víctimas (como los números de cuentas bancarias y de las tarjetas de crédito, por ejemplo) que posteriormente emplearán para cometer estafas y operaciones fraudulentas.

2.8. Lamers ("wannabes"): "Scriptkiddies" o "Click-kiddies".

Los "Lamers", también conocidos por "script kiddies" o "click kiddies", son aquellas personas que han obtenido determinados programas o herramientas para realizar ataques informáticos (descargándolos generalmente desde algún servidor de Internet) y que los utilizan sin tener conocimientos técnicos de cómo funcionan.

A pesar de sus limitados conocimientos, son los responsables de la mayoría de los ataques que se producen en la actualidad, debido a la disponibilidad de abundante documentación técnica y de herramientas informáticas que se pueden descargar fácilmente de Internet, y que pueden ser

utilizadas por personas sin conocimientos técnicos para lanzar distintos tipos de ataques contra redes y sistemas informáticos.

2.9. Amenazas del personal interno

También debemos tener en cuenta el papel desempeñado por algunos empleados en muchos de los ataques e incidentes de seguridad informática, ya sea de forma voluntaria o involuntaria. Así, podríamos considerar el papel de los empleados que actúan como "fisgones" en la red informática de su organización, los usuarios incautos o despistados, o los empleados descontentos o desleales que pretenden causar algún daño a la organización. Por este motivo, conviene reforzar la seguridad tanto en relación con el personal interno ("insiders") como con los usuarios externos del sistema informático ("outsiders").

2.10. Exempleados

Los exempleados pueden actuar contra su antigua empresa u organización por despecho o venganza, accediendo en algunos casos a través de cuentas de usuario que todavía no han sido canceladas en los equipos y servidores de la organización. También pueden provocar la activación de "bombas lógicas" para causar determinados daños en el sistema informático (eliminación de ficheros, envío de información confidencial a terceros) como venganza tras un despido.

2.11. Intrusos remunerados

Los intrusos remunerados son expertos informáticos contratados por un tercero para la sustracción de información confidencial, llevar a cabo sabotajes informáticos contra una determinada organización, etcétera.

3. MOTIVACIONES DE LOS ATACANTES

El FBI ha acuñado el acrónimo MICE para resumir las distintas motivaciones de los atacantes e intrusos en las redes de ordenadores: Money, Ideology, Compromise y Ego (Dinero, Ideología, Compromiso y Autorrealización personal).

En general, podemos considerar la siguiente tipología de motivaciones de los atacantes:

- **Consideraciones económicas:** llevar a cabo operaciones fraudulentas; robo de información confidencial que posteriormente es vendida a terceros; extorsiones (si no se paga un determinado "rescate" se elimina información o se daña de forma irreparable un sistema que haya sido comprometido); intentos de manipulación de las cotizaciones de valores bursátiles, etcétera.
- **Diversión:** algunos usuarios de Internet realizan estos ataques como una forma de pasar el rato delante de su ordenador.
- **Ideología:** ataques realizados contra determinadas organizaciones, empresas y Websites gubernamentales, con un contenido claramente político.
- **Autorrealización.**

- Búsqueda de **reconocimiento social** y de un cierto estatus dentro de una comunidad de usuarios.

4. FASES DE UN ATAQUE INFORMÁTICO

Los ataques contra redes de ordenadores y sistemas informáticos suelen constar de las etapas o fases que se presentan a continuación:

1. Descubrimiento y exploración del sistema informático.
2. Búsqueda de vulnerabilidades en el sistema.
3. Explotación de las vulnerabilidades detectadas (para ello, se suelen utilizar herramientas específicamente construidas para tal fin, conocidas como "exploits").
4. Corrupción o compromiso del sistema: modificación de programas y ficheros del sistema para dejar instaladas determinadas puertas traseras o troyanos; creación de nuevas cuentas con privilegios administrativos que faciliten el posterior acceso del atacante al sistema afectado; etcétera.
5. Eliminación de las pruebas que puedan revelar el ataque y el compromiso del sistema: eliminación o modificación de los registros de actividad del equipo ("logs"); modificación de los programas que se encargan de monitorizar la actividad del sistema; etcétera. Muchos atacantes llegan incluso a parchear la vulnerabilidad descubierta en el sistema para que no pueda ser utilizada por otros intrusos.

5. HACKING TOOL´S

En cuanto a las herramientas de disponibles en la actualidad para llevar a cabo sus ataques ("Hacking Tools"), podríamos citar las siguientes:

- **Escáneres de puertos**, que permiten detectar los servicios instalados en un determinado sistema informático.
- **Sniffers:** dispositivos que capturan los paquetes de datos que circulan por una red. Para ello, también se podría utilizar un equipo conectado a la red con su tarjeta de red (NIC) configurada en "modo promiscuo", para poder procesar todo el tráfico que recibe (aunque vaya dirigido a otros equipos). Por otra parte, existen sniffers especializados en la captura de contraseñas u otros datos sensibles (como los números de cuenta o de tarjetas de crédito).
- **"Exploits":** herramientas que buscan y explotan vulnerabilidades conocidas.
- **"Backdoors kits":** programas que permiten abrir y explotar "puertas traseras" en los sistemas.
- **"Rootkits":** programas utilizados por los atacantes para ocultar "puertas traseras" en los propios ficheros ejecutables y servicios del sistema, que son modificados para facilitar el acceso y posterior control del sistema.
- **"Auto-rooters":** herramientas capaces de automatizar totalmente un ataque, realizando toda la secuencia de actividades para localizar un sistema, escanear sus posibles

vulnerabilidades, explotar una determinada vulnerabilidad y obtener el acceso al sistema comprometido.

- **"Password crackers":** aplicaciones que permiten averiguar las contraseñas de los usuarios del sistema comprometido.
- **Generadores** de virus y otros programas malignos.
- Herramientas que facilitan la ocultación y la suplantación de direcciones IP (**técnicas de "spoofing"**), dificultando de este modo la identificación del atacante.
- **Herramientas de cifrado y protocolos criptográficos** (como PGP, SSH, SSL o IPSec): cada vez es más frecuente que el atacante utilice protocolos criptográficos en sus conexiones con los sistemas y máquinas que ha conseguido comprometer, dificultando de este modo su detección y estudio.

Conclusiones

Para concluir el hecho de llevar a cabo un ataque informático, indica que los intrusos deben disponer de los medios técnicos, los conocimientos y las herramientas adecuadas, deben contar con una determinada motivación o finalidad, y se tiene que dar además una determinada oportunidad que facilite el desarrollo del ataque (como podría ser el caso de un fallo en la seguridad del sistema informático elegido). Estos tres factores constituyen lo que podríamos denominar como el "Triángulo de la Intrusión", concepto que se presenta de forma gráfica en la siguiente figura:

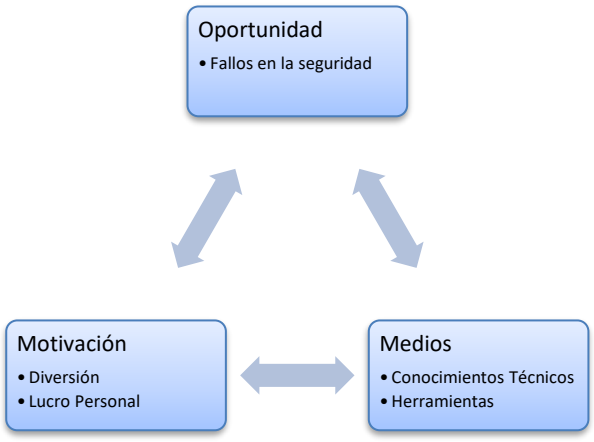


Figura 5: Triangula de la intrusión HACKING.

Si bien el termino de seguridad informática en su totalidad es una utopía, se pueden seguir algunas pautas o buenas costumbres para los usuarios:

1. No repetir contraseñas e incluir en ellas letras mayúsculas, minúsculas, números y caracteres especiales con más de 8 caracteres.
2. Tener actualizado el antivirus y escanear el equipo con frecuencia para revisar que todo está en orden.
3. No ignorar las actualizaciones del sistema operativo y aplicaciones que ayudan a mantener un sistema con las menores vulnerabilidades.
4. No dejar los dispositivos desbloqueados y con la sesión abierta si no se está trabajando en ellos.
5. Desconfiar de los dispositivos externos.
6. Habilitar el spam, no abrir ningún mail de origen desconocido ni enlaces de correos no deseados.
7. Navegación segura, desconfía de la publicidad engañosa que ofrecen premios a cambio de click, comprobar que en la barra del navegador el protocolo https.
8. Las descargas de programas sólo realizarlas a través de páginas web oficiales.