IMPLANTACIÓN DE MECANISMOS DE SEGURIDAD ACTIVA

MARÍA ÁNGELES PEÑASCO SÁNCHEZ- 2º ASIR- TEMA 2 - SAD

ÍNDICE

Ataques y contramedidas en sistemas personales:

- Clasificación de los ataques en sistemas personales.

- Anatomía de ataques.

- Análisis del software malicioso o malware:

- Historia del malware.
- Clasificación del malware: Virus, Gusanos, Troyanos, infostealers, crimeware, grayware,…)
- Métodos de infección: Explotación de vulnerabilidades, Ingeniería social, Archivos maliciosos, Dispositivos extraíbles, Cookies maliciosas, etc.

- Herramientas paliativas. Instalación y configuración.

- Software antimalware: Antivirus (escritorio, on line, portables, Live), Antispyware, Herramientas de bloqueo web.

- Herramientas preventivas. Instalación y configuración.

- Control de acceso lógico (política de contraseñas seguras, control de acceso en la BIOS y gestor de arranque, control de acceso en el sistema operativo, política de usuarios y grupos, actualización de sistemas y aplicaciones)

Seguridad en la conexión con redes públicas:

- Pautas y prácticas seguras:

Técnicas de Cifrado:

-Criptografía simétrica.
-Criptografía asimétrica.
-Criptografía híbrida.

Identificación Digital:

-Firma Electrónica y Firma Digital.
-Certificado Digital, Autoridad certificadora (CA).
- Documento Nacional de Identidad Electrónico (DNI e)
- Buenas prácticas en el uso del certificado digital y DNI e.

Seguridad en la red corporativa:

- Amenazas y ataques en redes corporativas:
* Amenaza interna o corporativa y Amenaza externa o de acceso remoto.
* Amenazas: Interrupción, Intercepción, Modificación y Fabricación.
* Ataques: DoS, Sniffing, Man in the middle, Spoofing, Pharming.

- Riesgos potenciales en los servicios de red.
* Seguridad en los dispositivos de red: terminales, switch y router.
* Seguridad en los servicios de red por niveles:
Enlace, Red (IP), Transporte (TCP-UDP) y Aplicación.

- Monitorización del tráfico en redes: Herramientas.

- Intentos de penetración.
* Sistemas de Detección de Intrusos (IDS).
* Técnicas de Detección de Intrusos.
* Tipos de IDS: (Host IDS, Net IDS).
* Software libre y comercial.

- Seguridad en las comunicaciones inalámbricas.
* Sistemas de seguridad en WLAN.
- Sistema Abierto.
- WEP.
- WPA.
* Recomendaciones de seguridad en WLAN.

Ataques y contramedidas en sistemas personales:

Clasificación de los ataques en sistemas personales

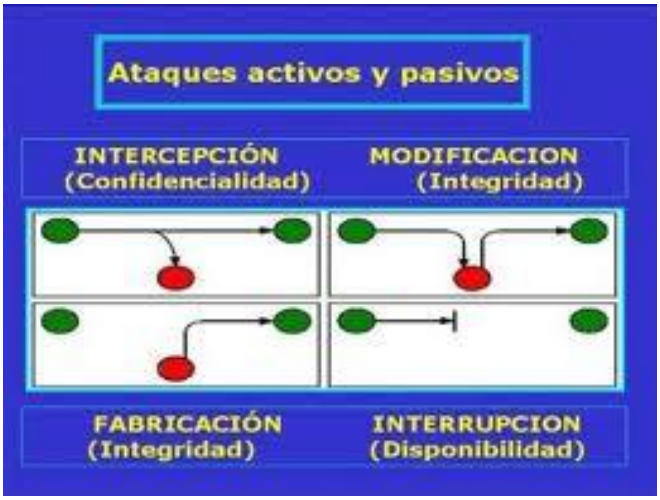
Un ataque no es más que la realización de una amenaza. Las cuatro categorías generales de amenazas o ataques son las siguientes:

Interrupción: un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

Intercepción: una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

Modificación: una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

Fabricación: una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo. Estos ataques se pueden asimismo clasificar de forma útil en términos de ataques pasivos y ataques activos.



La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios.

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero o un usuario.

Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida.

Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitorizados.
Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.
Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.
Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

Suplantación de identidad: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.
Reactuación: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
Modificación de mensajes: una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesos en la cuenta A" podría ser modificado para decir "Ingresa un millón de pesos en la cuenta B".
Degradación fraudulenta del servicio: impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes espurios. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

Anatomía de ataques

Uno de los recursos más importantes, para sobrellevar los desafíos en la seguridad de la información, es el conocimiento práctico de las técnicas de hacking.

Si se limita a seguir listas de comprobación de seguridad así como las buenas prácticas se logra tener la seguridad más básica.

Se requiere que el personal tenga una buena formación para que sea capaz de responder ante una situación valorando el posible riesgo.

Las técnicas de hacking brindan una mejor comprensión del riesgo. Un ejemplo es si un administrador detecta comportamientos extraños en un equipo y revisando los archivos de registro (logs) observa que alguien ha realizado conexiones al sitio 132.168.1.67:80 a las 3:00 de la madrugada podría pensar que es solamente una página web, sin embargo, se podría estar utilizando la herramienta netcat para enviar una Shell y posiblemente el puerto 80 sólo sea para atravesar tranquilamente el cortafuegos.

Al hablar de la seguridad en la información es importante definir muy bien el riesgo. Puede variar de acuerdo con el valor, las amenazas, vulnerabilidades y las medidas utilizadas para prevenirlo. Si no se comprenden adecuadamente las amenazas y vulnerabilidades no se podrá medir el riesgo.

El riesgo va a influir directamente en la inversión en seguridad informática. Se debe cambiar la perspectiva de la seguridad informática como un gasto más, y verla como una inversión.

LAS 5 FASES DE LA ANATOMIA DE UN ATAQUE

Fase 1 – Reconocimiento (Reconnaissance)

El reconocimiento se refiere a la fase preparatoria donde el atacante obtiene toda la información necesaria de su objetivo o victima antes de lanzar el ataque. Esta fase también puede incluir el escaneo de la red que el Hacker quiere atacar no importa si el ataque va a ser interno o externo. Esta fase le permite al atacante crear una estrategia para su ataque.

Esta fase puede incluir la Ingeniería Social, buscar en la basura (Dumpster diving), buscar que tipo de sistema operativo y aplicaciones usa el objetivo o víctima, cuales son los puertos que están abiertos, donde están localizados los routers (enrutadores), cuales son los host (terminales, computadoras) más accesibles, buscar en las bases de datos del Internet (Whois) información como direcciones de Internet (IP), nombres de dominios, información de contacto, servidores de email y toda la información que se pueda extraer de los DNS (Domain Name Server).

Esta fase le puede tomar bastante tiempo al Hacker ya que tiene que analizar toda la información que ha obtenido para lanzar el ataque con mayor precisión.

Fase 2 – Escaneo (Scanning)

Esta es la fase que el atacante realiza antes de la lanzar un ataque a la red (network). En el escaneo el atacante utiliza toda la información que obtuvo en la Fase del Reconocimiento (Fase 1) para identificar vulnerabilidades específicas. Por ejemplo, si en la Fase 1 el atacante descubrió que su objetivo o su víctima usa el sistema operativo Windows XP entonces el buscara vulnerabilidades especificas que tenga ese sistema operativo para saber por dónde atacarlo.

También hace un escaneo de puertos para ver cuáles son los puertos abiertos para saber por cual puerto va entrar y usa herramientas automatizadas para escanear la red y los host en busca de mas vulnerabilidades que le permitan el acceso al sistema.

Fase 3 – Ganar Acceso (Gaining Access)

Esta es una de las fases más importantes para el Hacker porque es la fase de penetración al sistema, en esta fase el Hacker explota las vulnerabilidades que encontró en la fase 2. La explotación puede ocurrir localmente, offline (sin estar conectado), sobre el LAN (Local Area Network), o sobre el Internet y puede incluir técnicas como buffer overflows (desbordamiento del buffer), denial-of-service (negación de servicios), sesión hijacking (secuestro de sesión), y password cracking (romper o adivinar claves usando varios métodos como: diccionary atack y brute forcé atack).

Los factores que ayudan al Hacker en esta fase a tener una penetración exitosa al sistema dependen de cómo es la arquitectura del sistema y de cómo está configurado el sistema objetivo o víctima, una configuración de seguridad simple significa un acceso más fácil al sistema, otro factor a tener en cuenta es el nivel de destrezas, habilidades y conocimientos sobre seguridad informática y redes que tenga el Hacker y el nivel de acceso que obtuvo al principio de la penetración (Fase 3).

Fase 4 – Mantener el Acceso (Maintaining Access)

Una vez el Hacker gana acceso al sistema objetivo (Fase3) su prioridad es mantener el acceso que gano en el sistema. En esta fase el Hacker usa sus recursos y recursos del sistema y usa el sistema objetivo como plataforma de lanzamiento de ataques para escanear y explotar a otros sistemas que quiere atacar, también usa programas llamados sniffers para capturar todo el trafico de la red, incluyendo sesiones de telnet y FTP (File Transfer Protocol).

En esta fase el Hacker puede tener la habilidad de subir, bajar y alterar programas y data.

Fase 5 – Cubrir las huellas (Covering Tracks)

En esta fase es donde el Hacker trata de destruir toda la evidencia de sus actividades ilícitas y lo hace por varias razones entre ellas seguir manteniendo el acceso al sistema comprometido ya que si borra sus huellas los administradores de redes no tendrán pistas claras del atacante y el Hacker podrá seguir penetrando el sistema cuando quiera, además borrando sus huellas evita ser detectado y ser atrapado por la policía o los Federales.

Las herramientas y técnicas que usa para esto son caballos de Troya, Steganography, Tunneling, Rootkits y la alteración de los “log files” (Archivos donde se almacenan todos los eventos ocurridos en un sistema informático y permite obtener información detallada sobre los hábitos de los usuarios), una vez que el Hacker logra plantar caballos de Troya en el sistema este asume que tiene control total del sistema.

Análisis del software malicioso o malware:

- Historia del malware.

Fue en 1949 cuando Von Neumann estableció la idea de programa almacenado y expuso La Teoría y Organización de Autómatas Complejos, donde presentaba por primera vez la posibilidad de desarrollar pequeños programas replicantes y capaces de tomar el control de otros programas de similar estructura. Si bien el concepto tiene miles de aplicaciones en la ciencia, es fácil apreciar una aplicación negativa de la teoría expuesta por Von Neumann: los virus informáticos, programas que se reproducen a sí mismos el mayor número de veces posible y aumentan su población de forma exponencial.

En 1959, en los laboratorios de Bell Computer, tres jóvenes programadores: Robert Thomas Morris, Douglas Mcllroy y Víctor Vysottsky crean un juego denominado CoreWar basado en la teoría de Von Neumann y en el que el objetivo es que programas combatan entre sí tratando de ocupar toda la memoria de la máquina eliminando así a los oponentes. Este juego es considerado el precursor de los virus informáticos.

Fue en 1972 cuando Robert Thomas Morris creó el que es considerado como el primer virus propiamente dicho: el Creeper era capaz de infectar máquinas IBM 360 de la red ARPANET (la precedente de Internet) y emitía un mensaje en pantalla que decía “Soy una enredadera (creeper), atrápame si puedes”. Para eliminarlo, se creó otro virus llamado Reaper (segadora) que estaba programado para buscarlo y eliminarlo. Este es el origen de los actuales antivirus.

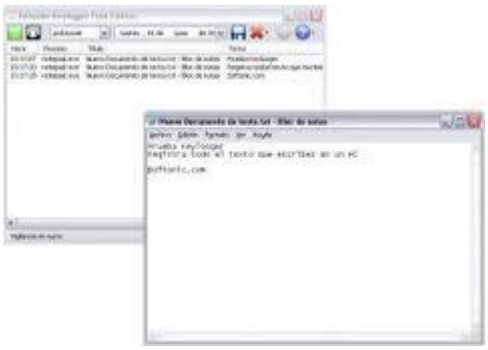
- Clasificación del malware: Virus, Gusanos, Troyanos, infostealers, crimeware, grayware,…)

- Adware: Muestra publicidad, generalmente está relacionado con los espías, por lo que se suelen conectar a algún servidor remoto para enviar la información recopilada y recibir publicidad. Algunos programas en sus versiones gratuitas o de evaluación muestran este tipo de publicidad, en este caso deberán avisar al usuario que la instalación del programa conlleva la visualización de publicidad.

- Bloqueador: Impide la ejecución de determinados programas o aplicaciones, también puede bloquear el acceso a determinadas direcciones de Internet. Generalmente impiden la ejecución de programas de seguridad para que, de este modo, resulte más difícil la detección y eliminación de programas maliciosos del ordenador.

- Bomba lógica: Programa o parte de un programa que se instala en un ordenador y no se ejecuta hasta que se cumple determinada condición, por ejemplo, ser una fecha concreta, ejecución de determinado archivo.

- Broma (Joke): No realiza ninguna acción maliciosa en el ordenador infectado pero, mientras se ejecuta, gasta una "broma" al usuario haciéndole pensar que su ordenador está infectado, por ejemplo, mostrando un falso mensaje de que se va a borrar todo el contenido del disco duro o mover el ratón de forma aleatoria.
- Bulo (Hoax): Mensaje electrónico enviado por un conocido que intenta hacer creer al destinatario algo que es falso, como alertar de virus inexistentes, noticias con contenido engañoso, etc, y solicitan ser reenviado a todos los contactos. Algunos de estos mensajes pueden ser peligrosos por la alarma innecesaria que generan y las acciones que, en ocasiones, solicitan realizar al usuario, por ejemplo, borrando ficheros del ordenador que son necesarios para el correcto funcionamiento del equipo.
- Capturador de pulsaciones (Keylogger): Monitoriza las pulsaciones del teclado que se hagan en el ordenador infectado, su objetivo es poder capturar pulsaciones de acceso a determinadas cuentas bancarias, juegos en línea o conversaciones y mensajes escritos en la máquina.



- Clicker: Redirecciona las páginas de Internet a las que intenta acceder el usuario, de este modo logra aumentar el número de visitas a la página redireccionada, realizar ataques de Denegación de Servicio a una página víctima o engañar al usuario sobre la página que está visitando, por ejemplo, creyendo que está accediendo a una página legítima de un banco cuando en realidad está accediendo a una dirección falsa.
- Descargador (Downloader): Descarga otros programas (generalmente también maliciosos) en el ordenador infectado. Suelen acceder a Internet para descargar estos programas.
- Espía (Spyware): Roba información del equipo para enviarla a un servidor remoto. El tipo de información obtenida varía según el tipo de espía, algunos recopilan información relativa a los hábitos de uso del ordenador, como el tiempo de uso y páginas visitadas en Internet; sin embargo, otros troyanos son más dañinos y roban información confidencial como nombres de usuario y contraseñas.

- Exploit: Tipo del software que se aprovecha de un agujero o de una vulnerabilidad en el sistema de un usuario para tener el acceso desautorizado al sistema.
- Herramienta de fraude: Simula un comportamiento anormal del sistema y propone la compra de algún programa para solucionarlo. Los más comunes son los falsos antivirus, que informan de que el ordenador está infectado, cuando en realidad el principal programa malicioso que tiene es la herramienta fraudulenta.
- Puerta trasera (Backdoors): Permite el acceso de forma remota a un sistema operativo, página Web o aplicación, haciendo que el usuario evite las restricciones de control y autenticación que haya por defecto.

- Rootkit: Toma control de Administrador (“root” en sistemas Unix/Linux) en el sistema, generalmente para ocultar su presencia y la de otros programas maliciosos en el equipo infectado; la ocultación puede ser para esconder los ficheros, los procesos generados, conexiones creadas… También pueden permitir a un atacante remoto tener permisos de Administrador para realizar las acciones que desee.
- Secuestrador del navegador (browser hijacker): Modifica la página de inicio del navegador, la página de búsqueda o la página de error por otra de su elección, también pueden añadir barras de herramientas en el navegador o incluir enlaces en la carpeta de “Favoritos”. Todas estas acciones las realiza generalmente para aumentar las visitas de la página de destino.

- Métodos de infección: Explotación de vulnerabilidades, Ingeniería social, Archivos maliciosos, Dispositivos extraíbles, Cookies maliciosas, etc.

Explotación de vulnerabilidades

Existen varios factores que hacen a un sistema más vulnerable al malware: homogeneidad, errores de software, código sin confirmar, sobre-privilegios de usuario y sobre-privilegios de código.

Una causa de la vulnerabilidad de redes, es la homogeneidad del software multiusuario. Por ejemplo, cuando todos los ordenadores de una red funcionan con el mismo sistema operativo, si se puede comprometer ese sistema, se podría afectar a cualquier ordenador que lo use. En particular, Microsoft Windows[16] tiene la mayoría del mercado de los sistemas operativos, esto permite a los creadores de malware infectar una gran cantidad de computadoras sin tener que adaptar el software malicioso a diferentes sistemas operativos.

La mayoría del software y de los sistemas operativos contienen bugs que pueden ser aprovechados por el malware. Los ejemplos típicos son los desbordamiento de búfer (buffer overflow), en los cuales la estructura diseñada para almacenar datos en un área determinada de la memoria permite que sea ocupada por más datos de los que le caben, sobre escribiendo otras partes de la memoria. Esto puede ser utilizado por el malware para forzar al sistema a ejecutar su código malicioso.

Las memorias USB infectadas pueden dañar la computadora durante el arranque.

Ingeniería Social

En el campo de la seguridad informática, ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón débil". En la práctica, un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente. Vía Internet o la web se usa, adicionalmente, el envío de solicitudes de renovación de permisos de acceso a páginas web o memos falsos que solicitan respuestas e incluso las famosas "cadenas", llevando así a revelar información sensible, o a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones.

Archivos maliciosos

Los códigos maliciosos que se propagan a través de dispositivos USB son cada vez más comunes y todos tienen un funcionamiento similar.

La posibilidad de que el malware aproveche los avances tecnológicos para que a través de ellos se obtengan nuevos canales y medios de infección y propagación, constituye una de las tendencias de este y los próximos años.

Los dispositivos de almacenamiento siempre constituyeron una de las vías más comunes de infección, desde los viejos discos magnéticos de 5´1/4, pasando por los ya casi olvidados disquetes de 3´1/2 hasta llegar a los dispositivos de almacenamiento que permiten guardar información a través del puerto USB.

En lo particular, los medios de almacenamiento masivo a través de conexiones del tipo USB, como lo son los PenDriver (o flashdrive, memorias USB, etc.), representan un punto vulnerable para cualquier sistema informático. Debido a la masividad de uso y facilidad de conexión, se convierten en un medio común utilizado para transportar archivos y también todo tipo de malware.

Los gusanos de Internet constituyen el principal tipo de programa dañino que comúnmente se aprovecha de estas características: la esencia de los gusanos informáticos es propagarse hacia la mayor cantidad de sistemas posibles copiando su propio código malicioso en cada infección, sin importar el medio por el cual lo haga.

En el caso de las infecciones a través de dispositivos USB, el malware se vale de un archivo llamado “autorun.inf” que se encarga de ejecutar el código malicioso en forma automática cuando el dispositivo es insertado en la computadora.

Cookies maliciosas

Cuando se navega por internet, se debe hacer de una manera responsable: debe primar la desconfianza. Generalmente, las páginas que aparentan tener un 'contenido de dudosa legalidad', material pornográfico e incluso que ofrecen descargas de programas de pago de forma gratuita, suelen ser los principales focos de cookies maliciosas, y es por ello que empresas como Google o Microsoft nos avisan si nos dirigimos desde sus buscadores a estos sitios de que podríamos estar en riesgo.

Además, los navegadores modernos, disponen de algoritmos para identificar este tipo de páginas, aunque no son ni mucho menos perfectos, por lo que no es recomendable fiarse al 100% de ellos.

- Herramientas paliativas. Instalación y configuración.

- Software antimalware: Antivirus (escritorio, on line, portables, Live), Antispyware, Herramientas de bloqueo web.

Antivirus

En informática los antivirus son programas cuyo objetivo es detectar y/o eliminar virus informáticos. Nacieron durante la década de 1980.

Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, ha hecho que los antivirus hayan evolucionado hacia programas más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectarlos y prevenir una infección de los mismos, y actualmente ya son capaces de reconocer otros tipos de malware, como spyware, Rootkits, etc. Estos son los diferentes tipos.

- Escritorio: Es un software que se encuentra instalado en el PC controlado en todo momento la actividad de los ficheros en busca de amenazas. En cualquier momento se puede analizar el equipo a fondo.
- Online: Es un software que a través del navegador analiza tu equipo sin necesidad de instalar nada. No suelen ser fiables.
- Portables: Es un software que se encuentra normalmente en una unidad portátil y que se puede ejecutar en cualquier equipo sin necesidad de instalación solamente enchufando o introduciendo la unidad portátil
- Live: Es software instalado en un CD que nos sirve para analizar el equipo sin necesidad de cargar el SO evitando así el camuflamiento de algunos virus.

Antispyware: El spyware es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.

El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware. Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up), recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono.

Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados.

Herramientas de bloqueo web.

Mediante un archivo robots.txt
Restringen el acceso de los robots de motores de búsqueda que rastrean la Web a un sitio. Estos robots están automatizados y, antes de acceder a las páginas de un sitio, verifican si existe un archivo robots.txt que les impida el acceso a determinadas páginas.

Editando el archivo host
Para ello hay que editar el archivo hosts, que en Windows98 está en el directorio c:\Windows y en XP está en el directorio c:\Windows\system32\drivers\etc.

Añadimos la página que no queremos que se cargue y al lado la ip 127.0.0.1 y nunca llegara a abrirse esa dirección.

- Herramientas preventivas. Instalación y configuración.

- Control de acceso lógico (política de contraseñas seguras, control de acceso en la BIOS y gestor de arranque, control de acceso en el sistema operativo, política de usuarios y grupos, actualización de sistemas y aplicaciones)

POLITICAS DE CONTRASEÑAS SEGURAS

Al conectarse a un sistema informático, generalmente se debe ingresar: un nombre de registro o nombre de usuario y una contraseña para acceder. Este par nombre de registro/contraseña forma la clave para tener acceso al sistema.
Mientras que al nombre de registro generalmente lo brinda el sistema o el administrador de forma automática, el usuario casi siempre tiene la libertad de elegir la contraseña. La mayoría de los usuarios, como piensan que no tienen ninguna información secreta que proteger, usan una contraseña fácil de recordar (por ejemplo, su nombre de registro, el nombre de su pareja o su fecha de nacimiento).

Esto implica, particularmente, que los empleados elijan las contraseñas a partir de ciertos requisitos, por ejemplo:

1. Que la contraseña tenga una longitud mínima
2. Que tenga caracteres especiales
3. Que combinen mayúsculas con minúsculas

Por último, es aconsejable que los administradores usen software que craquea contraseñas en sus contraseñas de usuario para probar su solidez. Sin embargo, se debe hacer dentro del marco de la política de protección y con discreción para tener el apoyo de la gerencia y los usuarios.

CONTROL DE ACCESO EN LA BIOS Y CONTROL DE ARRANQUE

La protección con contraseñas para el BIOS (o equivalentes al BIOS) y el gestor de arranque, pueden ayudar a prevenir que usuarios no autorizados que tengan acceso físico a sus sistemas, arranquen desde medios removibles u obtengan acceso como root a través del modo monousuario. Pero las medidas de seguridad que uno debería tomar para protegerse contra tales ataques dependen tanto de la confidencialidad de la información que las estaciones tengan como de la ubicación de la máquina.

Por ejemplo, si se utiliza una máquina en una exhibición y esta no contiene datos confidenciales, entonces puede que no sea crítico prevenir tales ataques. Sin embargo, si se deja al descuido en la misma exhibición, la portátil de uno de los empleados con llaves privadas SSH sin encriptar para la red corporativa, esto puede conducir a una violación de seguridad importante para la compañía completa.

Por otro lado, si la estación de trabajo está localizada en un lugar donde sólo los usuarios autorizados o de confianza tienen acceso, entonces la seguridad del BIOS o del gestor de arranque puede que no sea necesaria.

Las siguientes son las dos razones básicas por las que proteger la BIOS de una computadora con una contraseña:

1. Prevenir cambios a las configuraciones del BIOS — Si un intruso tiene acceso a la BIOS, puede configurarlo para que arranque desde un diskette o CD-ROM. Esto les permite entrar en modo de rescate o monousuario, lo que a su vez les permite plantar programas dañinos en el sistema o copiar datos confidenciales.

2. Prevenir el arranque del sistema — Algunas BIOS es le permiten proteger el proceso de arranque con una contraseña. Cuando está funcionalidad está activada, un atacante esta forzado a introducir una contraseña antes de que el BIOS lance el gestor de arranque.

Debido a que los métodos para colocar contraseñas del BIOS varían entre fabricantes de equipos, consulte el manual de su computador para ver las instrucciones específicas.

Si olvida su contraseña del BIOS, usualmente esta se puede reconfigurar bien sea a través de los jumper en la tarjeta madre o desconectando la batería CMOS. Por esta razón, es una buena idea bloquear el chasis del computador si es posible. Sin embargo, consulte el manual del computador o tarjeta madre antes de proceder a desconectar la batería CMOS

Contraseñas del gestor de arranque

A continuación se muestran las razones principales por las cuales proteger el gestor de arranque Linux:

1. Previene el acceso en modo monousuario — Si un atacante puede arrancar en modo monousuario, se convierte en el superusuario de forma automática sin que se le solicite la contraseña de acceso.
2. Previene el acceso a la consola de GRUB — Si la máquina utiliza GRUB como el gestor de arranque, un atacante puede usar la interfaz del editor para cambiar su configuración o para reunir información usando el comando cat.
3. Previene el acceso a sistemas operativos inseguros — Si es un sistema de arranque dual, un atacante puede seleccionar un sistema operativo en el momento de arranque, tal como DOS, el cual ignora los controles de acceso y los permisos de archivos.

CONTROL DE ACCESO EN EL SISTEMA OPERATIVO

Windows NT, Windows 2000, Windows XP y Windows Server 2003 comparten un modelo común de control de accesos basado en lo siguiente:

- Autorización basada en el usuario: El código se procesa en el mismo contexto de seguridad del usuario que lo inicia. No puede hacerse nada para lo que el usuario no esté autorizado.
- Acceso discrecional a objetos asegurables: El propietario de un objeto (por ejemplo, un archivo o una carpeta) puede conceder o denegar permisos para controlar cómo se utiliza y quién lo utiliza.
- Herencia de permisos: Un objeto puede heredar permisos del objeto que lo contiene (así, un objeto de archivo puede heredar los permisos del objeto de carpeta al que pertenece).
- Privilegios administrativos: Es posible controlar qué usuarios o grupos de usuarios pueden desempeñar funciones administrativas y realizar cambios que afecten a recursos de todo el sistema.
- Auditoría de eventos del sistema: Estas funciones permiten tanto detectar los intentos de burla a la seguridad del sistema como crear un registro de auditoría.

En una Lista de control de acceso (ACL) se enumeran, de forma ordenada, las entradas de control de acceso (entradas ACE) que definen las protecciones aplicables a un objeto y sus propiedades. Cada una de estas entradas identifica a un principal de seguridad y especifica el conjunto de derechos de acceso que le son concedidos o denegados o sobre los que se ha de efectuar una auditoría. A cada objeto asegurable se le asocia un descriptor de seguridad capaz de incluir dos tipos de listas de control de acceso (ACL):

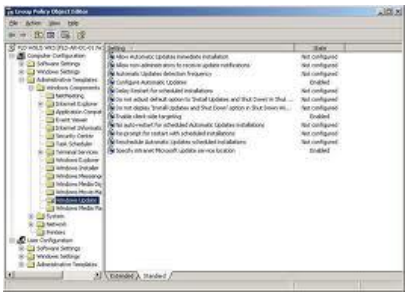
- Listas de control de acceso discrecional (DACL): identifican a los usuarios y a los grupos a los que se permiten o se deniegan los distintos tipos de acceso (lectura, lectura y escritura, etc.) al objeto asegurable.
- Listas de control de acceso al sistema (SACL): controlan cómo debe auditar el sistema operativo las cuestiones de acceso.

DEFINICIÓN DE DIRECTIVAS O POLÍTICAS DE GRUPOS

La configuración de Directiva de Grupo define los distintos componentes del entorno de Escritorio del usuario que accede de forma autenticada al dominio de nuestro servidor Windows 2000, de modo que el administrador del sistema determina cuales le serán aplicadas a cada usuario englobado en un sitio, dominio o unidad organizativa; entre las directivas que pueden especificarse, por ejemplo, podemos indicar aquellos programas que deseemos se encuentren disponibles para nuestros usuarios, los programas que aparecerán en su Escritorio, las opciones del menú Inicio, las opciones del navegador, etc.

Para crear una configuración específica de Escritorio para un grupo de usuarios en particular, se utilizan las Directivas de Grupo. La configuración de Directiva de Grupo está contenida en un objeto de Directiva de Grupo, de modo que se asocia dicha directiva a los Sitios, Dominios o Unidades Organizativas indicadas en Active Directory.

Curiosamente, y pese a su nombre, las Directivas de Grupo no pueden ser asociadas a un grupo de usuarios o grupos de equipos (sólo a Sitios, Dominios o Unidades Organizativas), aunque el resultado de su aplicación afecte únicamente a los usuarios y a los equipos de Active Directory.



Las directivas se aplican en este orden:

1. En primer lugar se aplica el objeto de Directiva de Grupo local único.
2. En segundo lugar se aplican los Objetos de Directiva de Grupo del Sitio, en orden especificado administrativamente.
3. En tercer lugar los Objetos de Directiva de Grupo del Dominio, en orden especificado administrativamente.
4. En cuarto lugar los Objetos de Directiva de Grupo de las Unidades Organizativas, de Unidad Organizativa principal a secundaria, y en orden especificado administrativamente en el nivel de cada Unidad Organizativa.
5. Finalmente, de forma predeterminada, las directivas aplicadas posteriormente sobrescriben las directivas aplicadas con anterioridad cuando las directivas son incoherentes. Sin embargo, si no hay incoherencias de configuración, tanto las directivas anteriores como las posteriores contribuyen a la directiva efectiva, es decir, se suman las configuraciones de las distintas directivas asociadas al objeto en cuestión.

En los siguientes apartados nos centraremos en definir una estructura de Unidades Organizativas para nuestro centro educativo, así como en asociar las Políticas o Directivas de Grupo al dominio o a las Unidades Organizativas anteriormente creadas.

Vamos a citar y definir los siguientes términos, con los que trabajaremos habitualmente a lo largo de este apartado:

Sitio.- Podemos definir un sitio como un conjunto de equipos en una o varias subredes IP. Los sitios suelen representar la estructura física de la red.

Dominio.- Un dominio tiene un nombre único y permite el acceso a las cuentas de usuario y de grupo centralizadas mantenidas por el administrador del dominio. Cada dominio tiene sus propias directivas de seguridad y relaciones de seguridad con otros dominios, y representa límite de seguridad en una red Windows 2000. Active Directory está compuesto de uno o varios dominios, cada uno de los cuales puede abarcar más de una ubicación física. Los dominios representan la estructura lógica de la organización.

Unidad Organizativa.- Es un objeto contenedor de Active Directory que se utiliza en los dominios. Las Unidades Organizativas son contenedores lógicos en los que pueden colocarse usuarios, grupos, equipos y otras Unidades Organizativas. Sólo pueden contener objetos de su dominio principal. Una U.O. es el ámbito más pequeño al que se puede aplicar una Directiva de Grupo.

POLÍTICA DE USUARIOS

Desactivación y/o borrado de cuentas

En la gestión del ciclo de vida de las cuentas de usuario es muy importante delimitar las cuentas temporales y aplicarles un sistema de caducidad para que no queden activas cuentas obsoletas y se mantengan únicamente aquellas que se utilizan y son realmente necesarias.

Debemos distinguir, por tanto, entre las cuentas de usuario con relaciones temporales y las que tienen relaciones fijas. La distinción se hace a través de un atributo del directorio corporativo que recogerá la fecha de expiración de las cuentas temporales. Tienen fecha de expiración los usuarios con relaciones ALUMNOEEPP, ALUMNOSECUNDARIA, EXALUMNO, MISCELANEA, PDIEXTERNO, PROFESORSECUNDARIA y algunos casos de PDI particulares, que son las cuentas de investigadores, colaboradores honorarios, becarios, etc.

Las cuentas que tienen asociada una fecha de expiración reciben 30, 15 y 7 días antes de la fecha de expiración un mensaje a su cuenta de correo electrónico indicándole que debe renovar dicha cuenta. En el cuerpo del mensaje se le indicará la cuenta que pierde y la fecha en la que se producirá, además contendrá un enlace a una URL donde se explica la política de desactivaciones y borrados, formas de reactivar o renovar la cuenta y personas de contacto para cada caso. Si no renueva la cuenta en dicho plazo, el día que expira la cuenta, ésta se deshabilita y se borra la relación 3 meses después. En el caso particular que sea la única relación que tenía el usuario se borrará la cuenta en el directorio corporativo.

Solo se avisará a los usuarios que pierden una de sus cuentas en el directorio corporativo. Los usuarios que pierdan alguna relación pero mantengan el usuario porque tienen otra relación no se les notificarán.

Política de claves

Se ha implementado una política de contraseñas. Con la implantación de la Gestión de Identidad, sólo hay un único punto de gestión de la contraseña; todos los cambios de contraseña realizados por el propio usuario o por las administraciones delegadas son realizados en todos los recursos asignados al usuario, por lo que se aplica a todas las cuentas de usuarios la misma política de contraseñas.

La nueva política de contraseñas es la siguiente:

- La longitud de la nueva contraseña debe ser como mínimo de 8 caracteres
- La nueva contraseña debe contener al menos 4 caracteres alfabético
- La nueva contraseña debe contener al menos 2 caracteres numéricos
- El número máximo de repeticiones de caracteres adyacentes de la nueva contraseña es 4
- El número máximo de caracteres numéricos en secuencia de la nueva contraseña es 4
- La nueva contraseña no podrá contener el nombre o apellido del usuario, ni el documento de identidad del mismo o su UVUS.

ACTUALIZACIÓN DE SISTEMAS

Los Sistemas Operativos requieren de actualizaciones periódicas, por varios motivos:

• Actualizaciones hardware: Debido a que el hardware de las máquinas evoluciona, es necesario crear programas capaces de gestionar este nuevo hardware.

• Actualizaciones de los programas: En ocasiones, se detectan vulnerabilidades o fallos en los programas que son subsanados en posteriores actualizaciones.

• Nuevas funcionalidades: Con frecuencia, los sistemas operativos incorporan nuevas funcionalidades que los usuarios pueden aprovechar descargándoselas en las actualizaciones.

Seguridad en la conexión con redes públicas:

- Pautas y prácticas seguras:

Técnicas de Cifrado:

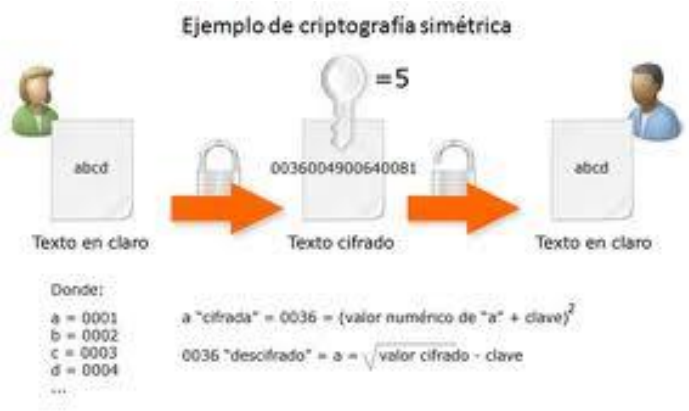
-Criptografía simétrica.
-Criptografía asimétrica.
-Criptografía híbrida.

CRIPTOGRAFÍA SIMÉTRICA

La criptografía simétrica es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma.

Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando. Sólo si el atacante obtuviera la clave, le serviría conocer el algoritmo. Los algoritmos de cifrado ampliamente utilizados tienen estas propiedades (por ejemplo: GnuPG en sistemas GNU).

Actualmente, los ordenadores pueden descifrar claves con extrema rapidez, y ésta es la razón por la cual el tamaño de la clave es importante en los criptosistemas modernos. El algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 2 elevado a 56 claves posibles (72.057.594.037.927.936 claves). Esto representa un número muy alto de claves, pero un ordenador genérico puede comprobar el conjunto posible de claves en cuestión de días. Una máquina especializada puede hacerlo en horas. Algoritmos de cifrado de diseño más reciente como 3DES, Blowfish e IDEA usan claves de 128 bits, lo que significa que existen 2 elevado a 128 claves posibles. Esto equivale a muchísimas más claves, y aun en el caso de que todas las máquinas del planeta estuvieran cooperando, tardarían más tiempo en encontrar la clave que la edad del universo.



CRIPTOGRAFÍA ASIMÉTRICA

La criptografía asimétrica es el método criptográfico que usaba el ejército Nazi y está compuesta por un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

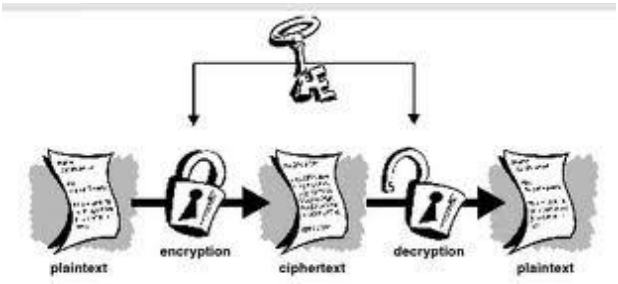
Si el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la identificación y autentificación del remitente, ya que se sabe que sólo pudo haber sido él quien empleó su clave privada (salvo que alguien se la hubiese podido robar). Esta idea es el fundamento de la firma electrónica.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

CRIPTOGRAFÍA HÍBRIDA

La criptografía híbrida es un método criptográfico que usa tanto un cifrado simétrico como un asimétrico. Emplea el cifrado de clave pública para compartir una clave para el cifrado simétrico. El mensaje que se esté enviando en el momento, se cifra usando la clave y enviándolo al destinatario. Ya que compartir una clave simétrica no es seguro, la clave usada es diferente para cada sesión.

Un sistema de cifrado híbrido no es más fuerte que el de cifrado asimétrico o el de cifrado simétrico de los que hace uso, independientemente de cuál sea más débil. En PGP y GnuPG el sistema de clave simétrica es probablemente la parte más débil de la combinación. Sin embargo, si un atacante pudiera descifrar una clave de sesión, sólo sería útil para poder leer un mensaje, el cifrado con esa clave de sesión. El atacante tendría que volver a empezar y descifrar otra clave de sesión para poder leer cualquier otro mensaje.



Identificación Digital:

-Firma Electrónica y Firma Digital.

Una firma digital es un esquema matemático que sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico. Las firmas digitales se utilizan comúnmente para la distribución de software, transacciones financieras y en otras áreas donde es importante detectar la falsificación y la manipulación.

Mientras que la firma electrónica es una firma digital que se ha almacenado en un soporte de hardware; mientras que la firma digital se puede almacenar tanto en soportes de hardware como de software. La firma electrónica reconocida tiene el mismo valor legal que la firma manuscrita.
De hecho se podría decir que una firma electrónica es una firma digital contenida o almacenada en un contenedor electrónico, normalmente un chip de ROM. Su principal característica diferenciadora con la firma digital es su cualidad de ser inmodificable.

-Certificado Digital, Autoridad certificadora (CA).

Un certificado digital (también conocido como certificado de identidad) es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y una clave pública.

Este tipo de certificados se emplea para comprobar que una clave pública pertenece a un individuo o entidad. La existencia de firmas en los certificados aseguran por parte del firmante del certificado (una autoridad de certificación, por ejemplo) que la información de identidad y la clave pública perteneciente al usuario o entidad referida en el certificado digital están vinculadas.

Una Autoridad Certificadora (AC, en inglés CA) es una entidad de confianza del emisor y del receptor de una comunicación. Esta confianza de ambos en una 'tercera parte confiable' (trusted third party) permite que cualquiera de los dos confíe a su vez en los documentos firmados por la Autoridad Certificadora, en particular, en los certificados que identifican ambos extremos.

- Documento Nacional de Identidad Electrónico (DNI e)

El Documento Nacional de Identidad (DNI), emitido por la Dirección General de la Policía (Ministerio del Interior), es el documento que acredita, desde hace más de 50 años, la identidad, los datos personales que en él aparecen y la nacionalidad española de su titular.

Con la llegada de la Sociedad de la Información y la generalización del uso de Internet se hace necesario adecuar los mecanismos de acreditación de la personalidad a la nueva realidad y disponer de un instrumento eficaz que traslade al mundo digital las mismas certezas con las que operamos cada día en el mundo físico y que, esencialmente, son:

- Acreditar electrónicamente y de forma indubitada la identidad de la persona
- Firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita

Para poder incorporar el chip, el Documento Nacional de Identidad cambia su soporte tradicional (cartulina plastificada) por una tarjeta de material plástico, dotada de nuevas y mayores medidas de seguridad. A esta nueva versión del Documento Nacional de Identidad nos referimos como DNI electrónico nos permitirá, además de su uso tradicional, acceder a los nuevos servicios de la Sociedad de la Información, que ampliarán nuestras capacidades de actuar a distancia con las Administraciones Públicas, con las empresas y con otros ciudadanos.

En la medida que el DNI electrónico vaya sustituyendo al DNI tradicional y se implanten las nuevas aplicaciones, podremos utilizarlo para:

- Realizar compras firmadas a través de Internet
- Hacer trámites completos con las Administraciones Públicas a cualquier hora y sin tener que desplazarse ni hacer colas
- Realizar transacciones seguras con entidades bancarias
- Acceder al edificio donde trabajamos
- Utilizar de forma segura nuestro ordenador personal
- Participar en un conversación por Internet con la certeza de que nuestro interlocutor es quien dice ser

- Buenas prácticas en el uso del certificado digital y DNI e.

Un usuario que tenga su certificado electrónico puede realizar todo tipo de trámites de forma que queda garantizada su verdadera identidad. Por lo tanto, se pueden firmar electrónicamente formularios y documentos electrónicos con la misma validez jurídica que si firmara el mismo documento en papel. De esta forma se puede realizar todo tipo de gestiones a través de la red, tal como compras, transacciones bancarias, pagos, etc.

Seguridad en la red corporativa:

- Amenazas y ataques en redes corporativas:

* Amenaza interna o corporativa y Amenaza externa o de acceso remoto.

Cualquier empleado puede convertirse en un punto de fuga de información. Lo único que necesita es acceso a la misma, ya que para extraerla hoy en día en muy fácil a través de dispositivos portátiles (Pendrives, discos duros, USB, etc) o incluso directamente a un servidor vía internet.

Lo más lógico es aplicar una política de gestión de usuarios, cada uno con sus permisos correspondientes para acceder a determinadas aplicaciones. También es preciso definir en los procesos de baja de personal algún procedimiento que impida, o al menos dificulte, que una persona pueda sacar información fuera de las fronteras de la empresa.

Otra via interna son los despistes. Instalar una aplicación que deje abierta una puerta trasera o enviar un correo electrónico a múltiples destinatarios incluyendo las direcciones en un campo diferente al de “copia oculta”, es decir, dejándolas al descubierto para cualquiera que lo reciba. Esta práctica ha sido recientemente sancionada por la AEPD. Se trata errores que pueden salir caros, y no solo por la sanción administrativa. La solución pasa por controlar lo que instala cada usuario en su equipo y, en el caso del correo, usar una herramienta profesional de marketing via email, en lugar del cásico cliente de correo electrónico.

Con la llegada de internet, las amenazas pueden venir desde el exterior. No se necesita poner un pie en las instalaciones de la empresa para que alguien pueda acceder a información propiedad de esta. Se necesita una protección del perímetro de la red informática, asi como un control de los accesos de sus usuarios ¿Quién hace esto? Un experto en sistemas. Se le contrata para que monte la red y su posterior mantenimiento periódico.

Las amenazas en el exterior también aparecen cuando alguien no autorizado se hace con un equipo informático de la empresa. Situaciones de extravío o robo de un ordenador portátil, un teléfono móvil o un disco duro USB o un uso indebido de los mismos en el domicilio de algún empleado, pueden poner a disposición de gente no deseada información protegida. La solución pasa por la encriptación de los datos en equipos portátiles y la educación de los usuarios a la hora de usarlos fuera de la red corporativa.

* Amenazas: Interrupción, Intercepción, Modificación y Fabricación.

Interrupción

En una interrupción un activo del sistema se pierde, este queda no disponible o inoperable, como consecuencia de una destrucción maliciosa de un dispositivo de equipo, haber borrado un programa o archivo de datos u ocasionado el malfuncionamiento de un administrador de archivos del sistema operativo, para que el sistema no pueda encontrar un archivo particular en disco.

Intercepción

Una intercepción significa que un tercero no autorizado ha ganado acceso a un activo. Este tercero puede ser una persona, un programa o un sistema de cómputo. Ejemplos de este tipo de ataque son: la copia ilícita de programas o archivos de datos, o la intrusión en la red de comunicaciones para obtener datos.
La intercepción puede basarse en Ingeniería Social donde el intruso obtiene información privada proporcionada en forma voluntaria. Este método es conocido bajo el término "Phishing".

Modificación

La modificación consiste en que alguien cambie los datos de una base de datos, altere el código de programa para ejecutar algún código adicional, o modifique los datos que se transmiten electrónicamente.
Terceros pueden fabricar objetos plagiados en un sistema de cómputo. Un intruso puede insertar en una red de comunicación transacciones fingidas o puede agregar nuevos registros a una base de datos.

Fabricación

En este tipo de ataque, una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.

*** Ataques: DoS, Sniffing, Man in the middle, Spoofing, Pharming.**

Denegación de Servicio: Comúnmente llamado DoS (Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.
Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios.
Una ampliación del ataque Dos es el llamado ataque distribuido de denegación de servicio, también llamado ataque DDoS (Distributed Denial of Service) el cual lleva a cabo generando un gran flujo de información desde varios puntos de conexión.

Sniffing: Se trata de una técnica por la cual se puede "escuchar" todo lo que circula por una red. Esto que en principio es propio de una red interna o Intranet, también se puede dar en la red de redes: Internet.
Esto se realiza mediante aplicaciones que actúan sobre todos los sistemas que componen el tráfico de una red. Capturan, interpretan y almacenan los paquetes de datos que viajan por la red, para su posterior análisis (contraseñas, mensajes de correo electrónico, datos bancarios,…)

Man in the middle: un ataque man-in-the-middle o JANUS es un ataque en el que una persona adquiere la capacidad de leer, insertar y modificar a voluntad los mensajes entre dos partes cifradas sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

Spoofing: Es el conjunto de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.
Se pueden clasificar los ataques de Spoofing, en función de la tecnología utilizada. Entre ellos tenemos el IP Spoofing, ARP Spoofing, DNS Spoofing, Web Spoofing o email Spoofing, aunque en general se puede englobar dentro de Spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

Pharming: es la explotación de una vulnerabilidad en el software de los servidores DNS o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador a la página web que el atacante haya especificado para ese nombre de dominio.

- Riesgos potenciales en los servicios de red.
*** Seguridad en los dispositivos de red: terminales, switch y router.**

Seguridad en los terminales: instalaciones por defecto no pensadas para la seguridad o la facilitación a los usuarios son algunos de los motivos por los que nuestros quipos no son seguros. Algunas medidas que se pueden tomar son:

- Conocimientos del sistema
- Verificación de la integridad
- Protocolos cifrados
- Revisión de los registros
- Paranoia (evitar ejecución de código externo. Aplicaciones “seguras”)
- Eliminación de servicios innecesarios
- Reglas de acceso (cortafuegos)

- Mantener el sistema actualizado
- A nivel de administración
    - Políticas de seguridad
    - Diseño estricto de la red
    - Barreras de acceso
    - Copias de seguridad (recuperación ante desastres)
    - Cifrado de las comunicaciones
    - Protocolos de autentificación seguros
    - Medidas preventivas
    - Trampas (Honeypots)

Protección de los switch: los puertos de entrada pueden ser un punto de entrada a la red por parte de usuarios no autorizados. Para evitarlo, los switch ofrecen una función que se conoce como seguridad de puertos. La seguridad de puertos limita la cantidad de direcciones MAC validas que se permiten por puerto. El puerto no reenvía paquetes con direcciones MAC de origen que se encuentran fuera del grupo de direcciones definidas.

Routers: debemos tomar las siguientes políticas de seguridad:

- Seguridad física
    - Designar al personal para actividades de instalación y desinstalación
    - Designar la persona para realizar actividades de mantenimiento
    - Designar al personal para realizar la conexión física
    - Definir controles de colocación y usos de la consola y los puertos de acceso
    - Definir procedimientos de recuperación ante eventualidades físicas
- Seguridad de configuración física
    - Designar las personas que acceden al router via consola o en forma remota
    - Designar la persona con privilegios de administración.
    - Definir procedimientos para realizar cambios a la configuración.
    - Definir políticas de contraseñas de usuario y administración.
    - Definir protocolos, procedimientos y redes para acceso remoto.

    - Definir plan de recuperación que incluya responsabilidades individuales ante incidentes.
    - Definir políticas de revisión de bitácoras.
    - Definir procedimientos y limitaciones del monitoreo remoto (SNMP)
- Seguridad de configuración estática
    - Definir directrices para la detección de ataques directos
    - Definir políticas de administración en intercambio de información (Protocolos de ruteo, RADIUS, SNMP, TACAS+, NTP).
    - Definir políticas de intercambio de llaves de encriptación.
- Seguridad de configuración dinámica
    - Identificar los servicios de configuración dinámica del router, y las redes permitidas para acceder a dichos servicios.
    - Identificar los protocolos de router a utilizar, y sus esquemas de seguridad que proveen.
    - Designar mecanismos y políticas de actualización del reloj (manual o por NTP)
    - Identificar los algoritmos criptográficos autorizados para levantar VPNs
- Seguridad en servicios de red
    - Enumerar protocolos, puertos y servicios a ser permitidos o filtrados en cada interface, así como los procedimientos para su autorización.
    - Describir procedimientos de seguridad y roles para interactuar con proveedores externos.

*** Seguridad en los servicios de red por niveles:**
Enlace, Red (IP), Transporte (TCP-UDP) y Aplicación.

Ataque en la Capa Red (ip) Sin medidas de seguridad, tanto las redes públicas como las privadas están expuestas a la observación y el acceso no autorizados. Los ataques internos pueden ser la consecuencia de una seguridad de intranet mínima o incluso inexistente. Los riesgos provenientes del exterior de la red privada se originan en las conexiones a Internet y a extranet. Los controles de acceso de usuarios basados en contraseñas no protegen por sí solos los datos transmitidos a través de una red.

Suplantación de identidad (direcciones IP ficticias) La mayoría de las redes y sistemas operativos utilizan la dirección IP para identificar un equipo como válido en una red. En algunos casos, es posible utilizar una dirección IP falsa. Esta práctica se conoce como suplantación. Un atacante podría utilizar programas especiales para construir paquetes IP que

parezcan provenir de direcciones válidas dentro de la intranet de una organización. Una vez obtenido el acceso a la red con una dirección IP válida, el atacante podrá modificar, desviar o eliminar datos. También podrá realizar ataques de otros tipos, como se describe en las secciones siguientes.

Ataque en la Capa Transporte (TCP-UDP) es un protocolo criptográfico de la capa de aplicación Proporciona autenticación, integridad y confidencialidad. No proporciona "No repudio" Utiliza TCP Transparente para las capas superiores (aplicaciones). Es el protocolo más utilizado en Internet para proporcionar servicios de seguridad Utiliza criptografía simétrica y asimétrica desarrollado por Netscape hasta la versión 3.0 En el año 1996, en plena Guerra de Navegadores con Microsoft SSLv3.0 sirve de base al IETF para TLS Transport Layer Security, RFC 2246 (actualizado en la RFC 3546)

Ataque en la Capa de aplicación Los ataques en la capa de aplicación se dirigen a los servidores de aplicaciones e intentan provocar errores en su sistema operativo o en sus aplicaciones. De este modo el atacante puede llegar a eludir los controles de acceso normales. El atacante aprovecha esta situación para obtener el control de una aplicación, sistema o red, con lo que podrá hacer lo siguiente:

- Leer, agregar, eliminar o modificar datos o un sistema operativo.
- Introducir un virus que utilice los equipos y las aplicaciones de software para copiarse por toda la red.
- Introducir un programa husmeador que analice la red y obtenga información que pueda utilizarse para hacer que la red deje de responder o que resulte dañada.
- Cerrar aplicaciones de datos o sistemas operativos de forma anormal.
- Deshabilitar otros controles de seguridad para posibilitar futuros ataques

- Monitorización del tráfico en redes: Herramientas.

Whireshark

Para muchos el principal programa de referencia en su sector. Se trata de un analizador de protocolos que permite realizar análisis y solucionar problemas en redes de comunicaciones. Posee una interfaz gráfica que nos permitirá interpretar mejor la información que nos proporciona. Nos permite analizar todo el tráfico de una red Ethernet, aunque también se puede utilizar en redes de otro tipo, estableciendo la configuración en modo promiscuo lo que le permite capturar todo el tráfico de la LAN.

Es un programa de software libre y multiplataforma, que podremos instalar tanto en Windows, como en Mac o Linux. Para capturar tramas directamente de red es necesario ejecutarlo con permisos de superusuario, razón por la cual es recomendable utilizarlo con mucho cuidado y establecer la configuración de forma adecuada para los propósitos de nuestra empresa. Para sacarle todo el partido deberemos saber realizar filtros para la información recibida de forma que no nos veamos desbordados por la información que nos proporciona.

WinDump

Es la versión para sistemas Windows de TCPDump, un paquete disponible en Linux y Unix, entre otros sistemas para capturar los paquetes de datos que circulan por la red de nuestra empresa. Tiene una gran funcionalidad, pero muchos pensarán que le falla el aspecto gráfico, puesto que funciona por línea de consola, algo cada día más en desuso sobre todo en sistemas Windows, donde muchos prefieren disponer de una interfaz gráfica aún a costa de un rendimiento algo menor.

Es una herramienta de análisis muy potente, que para utilizar correctamente debemos dominar los comandos básicos y saber extraer la información necesaria en la que estamos interesados. De igual modo que en el caso anterior, establecer filtros para tratar de segmentar el filtrado de paquetes es fundamental para poder analizar la información y no vernos desbordados.

Fing

Quizás se trate de una herramienta que nos ofrece menos información de la red que las dos anteriores, pero más ordenada, más estructurada y en base a los informes que nos permite construir podemos sacar más información. Nos ofrece toda la información recopilada como resultado del análisis: dirección IP, estado, grupo de red, sistema operativo, nombre de host, usuario entre otras cuestiones.

Al igual que en los casos anteriores se trata de un programa multiplataforma y gratuito, que podemos descargar e instalar de forma sencilla para comenzar a auditar nuestra red interna. Visualmente quizás es el más atractivo de los tres, aunque a la hora de determinar problemas quizás sea el menos útil. A la vez es el más sencillo de usar y requiere menos conocimientos de administración de redes que los dos anteriores

Como hemos comentado antes, para sacar el mejor partido de estas herramientas los conocimientos de redes son más que necesarios. Cuanto mayor sea nuestro conocimiento de la estructura de la red, la interpretación de los datos recibidos o el establecimiento de filtros que nos ayuden a separar la información que estamos recibiendo sin duda nos servirán para saber interpretar correctamente todos los datos recibidos.

- Intentos de penetración.
*** Sistemas de Detección de Intrusos (IDS).**

Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

El término IDS (Sistema de detección de intrusiones) hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Existen dos tipos de IDS:

El grupo N-IDS (Sistema de detección de intrusiones de red), que garantiza la seguridad dentro de la red.

El grupo H-IDS (Sistema de detección de intrusiones en el host), que garantiza la seguridad en el host.

*** Técnicas de Detección de Intrusos.**

El tráfico en la red (en todo caso, en Internet) generalmente está compuesto por datagramas de IP. Un N-IDS puede capturar paquetes mientras estos viajan a través de las conexiones físicas a las que está sujeto. Un N-IDS contiene una lista TCP/IP que se asemeja a los datagramas de IP y a las conexiones TCP. Puede aplicar las siguientes técnicas para detectar intrusiones:

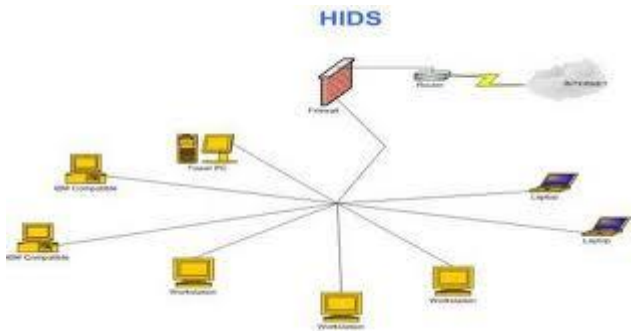
Verificación de la lista de protocolos: Algunas formas de intrusión, como "Ping de la muerte" y "escaneo silencioso TCP" utilizan violaciones de los protocolos IP, TCP, UDP e ICMP para atacar un equipo. Una simple verificación del protocolo puede revelar paquetes no válidos e indicar esta táctica comúnmente utilizada.

Verificación de los protocolos de la capa de aplicación: Algunas formas de intrusión emplean comportamientos de protocolos no válidos, como "WinNuke", que utiliza datos NetBIOS no válidos (al agregar datos fuera de la banda). Para detectar eficazmente estas intrusiones, un N-IDS debe haber implementado una amplia variedad de protocolos de la capa de aplicación, como NetBIOS, TCP/IP, etc.

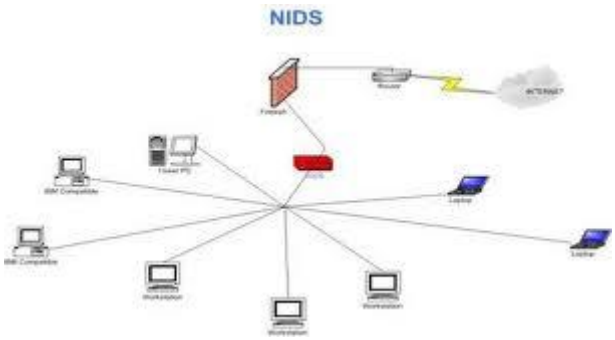
Esta técnica es rápida (el N-IDS no necesita examinar la base de datos de firmas en su totalidad para secuencias de bytes particulares) y es también más eficiente, ya que elimina algunas falsas alarmas. Por ejemplo, al analizar protocolos, N-IDS puede diferenciar un "Back Orifice PING" (bajo peligro) de un "Back Orifice COMPROMISE" (alto peligro).

*** Tipos de IDS: (Host IDS, Net IDS).**

HIDS (HostIDS): el principio de funcionamiento de un HIDS, depende del éxito de los intrusos, que generalmente dejaran rastros de sus actividades en el equipo atacado, cuando intentan adueñarse del mismo, con propósito de llevar a cabo otras actividades. El HIDS intenta detectar tales modificaciones en el equipo afectado, y hacer un reporte de sus conclusiones.



NIDS (NetworkIDS): un IDS basado en red, detectando ataques a todo el segmento de la red. Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red.



*** Software libre y comercial.**

El software libre, es la denominación del software que respeta la libertad de los usuarios sobre su producto adquirido y, por tanto, una vez obtenido puede ser usado, copiado, estudiado, modificado y redistribuido libremente. Según la Free Software Foundation, el software libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, modificar el software y distribuirlo modificado.

El software libre suele estar disponible gratuitamente, o al precio de costo de la distribución a través de otros medios; sin embargo no es obligatorio que sea así, por lo tanto no hay que asociar software libre a "software gratuito" (denominado usualmente freeware), ya que, conservando su carácter de libre, puede ser distribuido comercialmente ("software comercial"). Análogamente, el "software gratis" o "gratuito" incluye en ocasiones el código fuente; no obstante, este tipo de software no es libre en el mismo sentido que el software libre, a menos que se garanticen los derechos de modificación y redistribución de dichas versiones modificadas del programa.

Software Libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. De modo más preciso, se refiere a cuatro libertades de los usuarios del software:

1. La libertad de usar el programa, con cualquier propósito (libertad 0).
2. La libertad de estudiar cómo funciona el programa, y adaptarlo a tus necesidades (libertad 1). El acceso al código fuente es una condición previa para esto.
3. La libertad de distribuir copias, con lo que puedes ayudar a tu vecino (libertad 2).
4. La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie.

'Software libre' no significa 'no comercial'. Un programa libre debe estar disponible para uso comercial, desarrollo comercial y distribución comercial. El desarrollo comercial del software libre ha dejado de ser inusual; el software comercial libre es muy importante.

Cuando se habla de software libre, es mejor evitar términos como: `regalar' o `gratis', porque esos términos implican que lo importante es el precio, y no la libertad.

El software comercial es el software, libre o no, que es comercializado, es decir, que existen sectores de la economía que lo sostiene a través de su producción, su distribución o soporte.

El software comercial cuenta con las siguientes características:

1. Tienen licencias, las cuales están limitadas por usuarios y son pagadas. Estas licencias restringen las libertades de los usuarios a usar, modificar, copiar y distribuir el software.
2. El desarrollo, programación y actualización de este software sólo lo hace la empresa que tiene los derechos. Como sucede con los productos Microsoft (Windows, Office, etc).
3. En el software comercial se suele esconder y mezquinar los avances y descubrimientos tecnológicos entre las empresas que lo desarrollan.
4. Muchas veces con estrategias comerciales se suele hacer que los usuarios actualicen su software comercial, sin que exista una necesidad verdadera de ello, consiguiendo de esta forma hacer que el usuario invierta en nuevas licencias, la mayoría de las veces innecesarias.

- Seguridad en las comunicaciones inalámbricas.
*** Sistemas de seguridad en WLAN.**

Las redes WiFi pueden ser abiertas o cerradas. En una red abierta, cualquier ordenador cercano al punto de acceso puede conectarse a Internet a través de él, siempre que tenga una tarjeta WiFi incorporada, claro. En la red cerrada el ordenador detectará una red inalámbrica cercana disponible, pero para acceder habrá que introducir la contraseña. Es lo que suele ocurrir en los aeropuertos y algunos hoteles, donde la contraseña se obtiene previo pago.

- Sistema Abierto.

El identificador SSID: es el nombre de la red WiFi que crea el punto de acceso. Por defecto suele ser el nombre del fabricante, pero se puede cambiar en cualquier momento.

El canal: por lo general se usa el canal 6, pero si el vecino también tiene un punto de acceso en este canal habrá que cambiarlo para evitar interferencias. Puede ser un número entre 1 y 11.

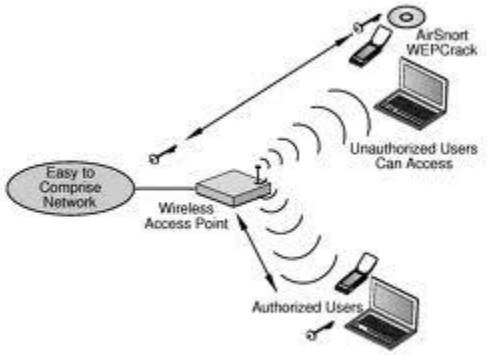
La clave WEP: si se utiliza WEP para cerrar la red WiFi, hay que indicar la contraseña que tendrá que introducirse en los ordenadores que se quieran conectar.

La clave compartida WPA: Como en el caso anterior, si se emplea seguridad WPA hay que seleccionar una clave de acceso para poder conectarse a la red WiFi.

Cifrado de 128 bits: En WEP y WPA las comunicaciones se transmiten cifradas para protegerlas. Esto quiere decir que los números y letras se cambian por otros mediante un factor. Sólo con la clave adecuada se puede recuperar la información. Cuanto más grande sea el factor de cifrado (más bits), tanto más difícil resulta romper la clave.

- WEP.

Es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad.



- WPA.

Es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado). Los investigadores han encontrado varias debilidades en el algoritmo WEP (tales como la reutilización del vector de inicialización (IV), del cual se derivan ataques estadísticos que permiten recuperar la clave WEP, entre otros). WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era finalizado. WPA fue creado por "The Wi-Fi Alliance" (La Alianza Wi-Fi).

WPA adopta la autenticación de usuarios mediante el uso de un servidor, donde se almacenan las credenciales y contraseñas de los usuarios de la red. Para no obligar al uso de tal servidor para el despliegue de redes, WPA permite la autenticación mediante clave compartida ([PSK], Pre-Shared Key), que de un modo similar al WEP, requiere introducir la misma clave en todos los equipos de la red.

*** Recomendaciones de seguridad en WLAN.**

- Instale el router en el ambiente más alejado de la calle y las ventanas. Muchos routers permiten controlar la intensidad de la señal, por esto, disminuya la intensidad para restringir la propagación fuera del edificio.

- Cambie la contraseña por default del router inalámbrico: en general, el nombre de usuario es admin y la contraseña también es admin.

- Cambie el SSID por default del router inalámbrico y deshabilite el broadcast del SSID. Si es posible, no hay que permitir acceder a la red local a través de la red inalámbrica sino solamente a través de la red cableada conectada a uno de los puertos LAN del router.

- Utilice WPA, en caso de que no estar disponible utilice WEP con una contraseña de 128 bits, si es posible.

- Instale actualizaciones de firmware cuando estén disponibles por el fabricante.

- Desconecte el router o deshabilite la red inalámbrica cuando no la utilice.

- Tenga siempre en mente la seguridad de todo el sistema instalando un firewall, actualizando el antivirus, el sistema operativo y los programas.