Seguridad y Alta Disponibilidad

INDICE

TEMA2:

1. CLASIFICACIÓN DE LOS ATAQUES EN SISTEMAS PERSONALES:

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo).

La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestados, 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.

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

1. **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.

2. **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.

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.

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.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos.

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:

a. **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.

b. **Repetición:** 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.
c. **Modificación de mensajes:** una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado.
d. **Interrupción:** o 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.

2. Anatomía de ataques.

Importancia de la anatomía de un ataque 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*.

Las técnicas de **hacking** brindan una mejor comprensión del riesgo.

Las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad. Desde la perspectiva del profesional de seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque.

Fase 1: Reconocimiento Esta etapa involucra la obtención de información con respecto a una potencial víctima que puede ser una persona u organización.Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo.

Fase 2: Exploración En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros.

Entre las herramientas que un atacante puede emplear durante la exploración se encuentra el network mappers, port mappers, network scanners, port scanners, y vulnerability scanners.

Fase 3: Obtener acceso. En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema descubiertos durante las fases de reconocimiento y exploración.

Fase 4: Mantener el acceso Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet.

Fase 5: Borrar huellas Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red.

3. 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.
En 1959, en los laboratorios de Bell Computer, tres jóvenes programadores: Robert Thomas Morris, Douglas Mcllroy y Victor 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.

Fue en 1972 cuando Robert Thomas Morris creó el que es considerado cómo 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”.

En la década de los 80 los PC ganaban popularidad y cada vez más gente entendía la informática y experimentaba con sus propios programas.

Skrenta escribe el primer virus de amplia reproducción: Elk Cloner, que contaba el número de veces que arrancaba el equipo y al llegar a 50 mostraba un poema.
En 1984, Frederick B. Cohen acuña por primera vez el término virus informático en uno de sus estudios definiéndolo como “Programa que puede infectar a otros programas incluyendo una copia posiblemente evolucionada de sí mismo”.

En 1987 hace su aparición el virus Jerusalem o Viernes 13, que era capaz de infectar archivos .EXE y .COM. Su primera aparición fue reportada desde la Universidad Hebrea de Jerusalem y ha llegado a ser uno de los virus más famosos de la historia.

En 1999 surge el gusano Happy desarrollado por el francés Spanska que crea una nueva corriente en cuanto al desarrollo de malware que persiste hasta el día de hoy: el envío de gusanos por correo electrónico. Este gusano estaba encaminado y programado para propagarse a través del correo electrónico. En el año 2000 hubo una infección que tuvo muchísima repercusión mediática debido a los daños ocasionados por la infección tan masiva que produjo. Fuel el gusano I Love You o LoveLetter, que, basándose en técnicas de ingeniería social infectaba a los usuarios a través del correo electrónico.

Fue en ese año cuando aparecieron gusanos como el Mydoom, el Netsky, el Sasser, o el Bagle, que alarmaron a toda la sociedad y lo que buscaban era tener la mayor repercusión y reconocimiento posible. Ese fue el año más duro de este tipo epidemias y curiosamente el último.

El Gran Cambio
Fue en 2005 cuando, tras 5 años de tendencia sostenida en la que los virus tal y como los conocíamos fueron dejando su lugar a gusanos y troyanos encargados de formar redes de bots para obtener dinero, cuando vieron que el entretenimiento que podía suponer la creación de malware se podía convertir en un negocio muy rentable.

Quizá la mejor prueba de ello sean los denominados Troyanos Bancarios de los que existen miles de variantes dado que los creadores, para dificultar su detección modificaban permanente el código de los mismos. Este tipo de malware actualmente se distribuye mediante exploits, spam o a través de otro malware que descarga el troyano bancario. Este último tipo de troyano es el encargado de robar información relacionada con las transacciones comerciales y/o datos bancarios del usuario infectado.

Malware también llamado badware, software malicioso o software malintencionado) es un software que tiene como objetivo infiltrarse en el sistema y dañar la computadora sin el conocimiento de su dueño, con finalidades muy diversas, ya que en esta categoría encontramos desde un troyano a un spyware.

Virus es una secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

Algunas acciones que puede realizar un virus son:

Mostrar en la pantalla mensajes o imágenes humorísticas, generalmente molestas.
- Ralentizar o bloquear el ordenador.
-Destruir la información almacenada en el disco, en algunos casos vital para el sistema, que impedirá el funcionamiento del equipo.
-Reducir el espacio en el disco.
-Molestar al usuario cerrando ventanas, moviendo el ratón.

Gusano es un malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

A diferencia de un virus, un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Los gusanos casi siempre causan problemas en la red (aunque sea simplemente consumiendo ancho de banda), mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan.

Troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas (generalmente en detrimento de la seguridad) sin el conocimiento del usuario.

Infostealer puede afectar también al servicio de correo electrónico MSN Messenger, enviando mensajes falsos e incluso introduciendo en ellos datos incluidos por los usuarios en sus mensajes a través de dicho servicio.

Crimeware es un tipo de software que ha sido específicamente diseñado para la ejecución de delitos financieros en entornos en línea. El término fue creado por Peter Cassidy, Secretario General del Anti-Phishing Working Group para diferenciarlo de otros tipos de software malicioso.

El **crimeware** ha sido diseñado, mediante técnicas de ingeniería social u otras técnicas genéricas de fraude en línea, con el fin de conseguir el robo de identidades para acceder a los datos de usuario de las cuentas en línea de compañías de servicios financieros (típicamente clínicas) o compañías de venta por correo, con el objetivo de obtener los fondos de dichas cuentas, o de completar transacciones no autorizadas por su propietario legítimo, que enriquecerán al ladrón que controla el **crimeware.**

El **crimeware** puede, de forma subrepticia, instalar un *keylogger* con el objetivo de obtener los datos (logins, passwords, etc.) que permitirán al ladrón, acceder a cuentas bancarias accesibles a través de Internet.

Stealer es el nombre genérico de programas informáticos maliciosos del tipo troyano, que se introducen a través de internet en un ordenador con el propósito de obtener de forma fraudulenta información confidencial del propietario, tal como su nombre de acceso a sitios web, contraseña o número de tarjeta de crédito.

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…

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.

Grayware es un tipo de programa maligno que involucra aquellos programas que se comportan de forma molesta o indeseada. Los grayware abarcan otros tipos de malwares (programas malignos) como espías, adwares, dialers, etc. Grayware no incluye virus o troyanos.

Suelen afectar el rendimiento de la computadora. También a menudo los grayware suelen realizar acciones que son molestas para los usuarios, como ventanas pop-up con publicidad, entre otras.

Posibles problemas que acarrean los graywares
-***Reducción del rendimiento de la computadora.***
- Incremento de los cuelgues en aplicaciones y errores fatales.
- Reducen la eficiencia del usuario.

Métodos de infección Malware

Internet. La red global es el origen principal de distribución de todos tipos de malware. En general, los virus y otros programas maliciosos se colocan en unas páginas Web populares pretendiéndose algún software útil y gratis. Muchos de los scripts que se ejecutan automáticamente al abrir las páginas Web también pueden contener programas maliciosos.

Correo electrónico. Los emails en los buzones privados y las bases de correo pueden contener virus. Los archivos adjuntos y el cuerpo de email pueden contener malware. Los tipos principales de malware distribuido por correo electrónico son virus y gusanos. Puede infectar su equipo cuando abre un email o guarda un archivo adjunto

Vulnerabilidades de software. Explotación de vulnerabilidades de software instalado en el sistema es el método preferido por los hackers. Las vulnerabilidades permiten a un hacker establecer una conexión remota a su equipo, y consecuentemente a sus datos, los datos de su red, 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.

Originalmente las computadoras tenían que ser booteadas con un diskette, y hasta hace poco tiempo era común que fuera el dispositivo de arranque por defecto. Esto significaba que un diskette contaminado podía dañar la computadora durante el arranque, e igual se aplica a CD y memorias USB. Aunque eso es menos común ahora, sigue siendo posible olvidarse de que el equipo se inicia por defecto en un medio removible, y por seguridad normalmente no debería haber ningún diskette, CD, etc, al encender la computadora. Para solucionar este problema de seguridad basta con entrar en la BIOS del ordenador y cambiar el modo de arranque del ordenador.

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.

Por un archivo malicioso: Esta es la forma que tienen gran cantidad de troyanos de llegar al equipo. El archivo malicioso puede llegar como adjunto de un mensaje, por redes P2P, como enlace a un fichero que se encuentre en Internet, a través de carpetas compartidas en las que el gusano haya dejado una copia de sí mismo…La mejor forma de prevenir la infección es analizar con un antivirus actualizado todos los archivos antes de ejecutarlos, a parte de no descargar archivos de fuentes que no sean fiables.

Muchos gusanos suelen dejar copias de sí mismos en dispositivos extraíbles para que automáticamente, cuando el dispositivo se conecte a un ordenador, ejecutarse e infectar el nuevo equipo. La mejor forma de evitar quedarse infectados de esta manera, es deshabilitar el autoarranque de los dispositivos que se conecten al ordenador Algunos ejemplos de malware que se diseminan aprovechándose de estos dispositivos son:

• **RJUMP:** este gusano posee características de troyano y abre una puerta trasera en el sistema infectado. Entre los medios de almacenamiento masivo que puede infectar se encuentran discos rígidos extraíbles, cámaras digitales y memorias USB.

Fujacks: esta familia de gusanos no sólo se propaga a través de dispositivos de almacenamiento masivo sino que también infecta archivos ejecutables y recursos compartidos que existen en la red configurados con contraseñas débiles (o sin ellas).

AutoRun.C (también conocido como Zayle): es un gusano de Internet que aprovecha la conexión a los dispositivos USB para propagarse e infectar las computadoras. Para lograr ejecutarse en forma automática, se vale de un archivo “autorun.inf”. Además posee la capacidad de deshabilitar la opción de abrir las unidades con doble clic.

Tanto los códigos maliciosos mencionados como la mayoría del malware en general, utilizan formas comunes de infección; como por ejemplo, copiarse a sí mismo a un determinado sector del disco, manipular el registro de Windows, etc.

Cookies

Las **cookies** son ficheros de texto que se crean al visitar una página web, y que sirven para almacenar información de diversos tipos que no debería afectar a tu privacidad. Algunas páginas web utilizan la información recogida en estas cookies para recopilar información del usuario y seguidamente enviarle publicidad, por lo que se consideran un tipo de spyware.

Saber si estamos infectado por cookies. 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.

4. Herramientas paliativas. Instalación y configuración.

Software anti-malware

Como los ataques con malware son cada vez más frecuentes, el interés ha empezado a cambiar de protección frente a virus y spyware, a protección frente al malware, y los programas han sido específicamente desarrollados para combatirlos. Los programas anti-malware pueden combatir el malware de dos formas:

1. Proporcionando protección en tiempo real (real-time protection) contra la instalación de malware en una computadora. El software anti-malware escanea todos los datos procedentes de la red en busca de malware y bloquea todo lo que suponga una amenaza.

2. Detectando y eliminando malware que ya ha sido instalado en una computadora. Este tipo de protección frente al malware es normalmente mucho más fácil de usar y más popular. Este tipo de programas anti-malware escanean el contenido del registro de Windows, los archivos del sistema operativo, la memoria y los programas instalados en la computadora. Al terminar el escaneo muestran al usuario una lista con todas las amenazas encontradas y permiten escoger cuales eliminar.

La protección en tiempo real funciona idénticamente a la protección de los antivirus: el software escanea los archivos al ser descargados de Internet y bloquea la actividad de los componentes identificados como malware. En algunos casos, también pueden interceptar intentos de ejecutarse automáticamente al arrancar el sistema o modificaciones en el navegador web. Debido a que muchas

veces el malware es instalado como resultado de exploits para un navegador web o errores del usuario, usar un software de seguridad para proteger el navegador web puede ser una ayuda efectiva para restringir los daños que el malware puede causar.

Antivirus

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.

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 normalme intalado en un cd que nos sirve para analizar el equipo sin necesidad de cargar el SO evitando asi el camuflamiento de algunos virus.

Antispyware

Tipo de aplicación que se encarga de buscar, detectar y eliminar spywares o espías en el sistema.

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. Sin embargo, a diferencia de los virus, no se intenta replicar en otros ordenadores, por lo que funciona como un parásito.

HERRAMIENTAS DE BLOQUEO WEB.

Estas herramientas pueden ser automatizadas o no. Las herramientas automátizadas son aplicaciones para la computadora que permiten trabajar en dos niveles de seguridad: la prevención y el control. Ninguna de estas herramientas es 100% efectiva por lo que debemos ser conscientes de la importancia de las herramientas no automátizadas: la educación y la concientización. El diálogo con los menores es la mejor herramienta de prevención para los riesgos que existen en la web. Todas las herramientas indicadas en la presente sección deben ser aplicadas con el compromiso de la familia, siendo conscientes de cuáles son las configuraciones que se realizan y tomando la responsabilidad sobre cuáles son los contenidos a los que se podrá acceder y a cuáles no.

Existen diferentes controles que se pueden aplicar:

 Herramientas de control de navegación: permite controlar a qué sitios es posible acceder y a qué sitios no. Este es el principal control utilizado y para ello, se utilizan diferentes técnicas de prevención:

Listas blancas/negras: en estos casos se utiliza una lista de sitos a los que el menor tiene permitido acceder (lista blanca) o bien permitir la navegación exceptuando los sitios explícitamente denegados (listas negras).

-Bloqueo por palabras clave: en estos casos la aplicación verifica el contenido del sitio web y bloquea el acceso a aquellos que tengan ciertas palabras (lease "porno", "sexo", "drogas", "matar", "xxx", etc.). Muchas aplicaciones, permiten personalizar los criterios de severidad (¿cuántas veces debe aparecer una palabra para considerar el sitio como no apto?) e incluso seleccionar las palabras por categorías y agregando palabras específicamente indicadas por el usuario.

-Bloqueo de aplicaciones: son herramientas que permiten directamente bloquear ciertas aplicaciones como acceso web (www), mensajería instantánea o chat, o correo electrónico.

-Control de tiempo: estas herramientas limitan el tiempo que un menor puede estar utilizando computadora o conectado a Internet. En su mayoría también permiten controlar a qué horas es posible conectarse. Son útiles para controlar que los horarios y la cantidad de uso sea razonable, acorde a los criterios de cada familia.

-Navegadores infantiles: Son herramientas que dan acceso a páginas adecuadas para los niños y adolescentes. Tienen un diseño y características apropiadas al público menor y permiten el uso de diferentes perfiles, en función de la edad del usuario. También existen buscadores infantiles con características similares. Algunos navegadores infantiles son Kidsui, Kidrocket, MyKidBrowser y BuddyBrowser.

-Herramientas que bloquean la información que sale del Pc: son aplicaciones que impiden revelar información personal. Esto es especialmente útil con respecto a llenar formularios y hojas de registro en línea o comprar a través de la tarjeta de crédito. Puede ser utilizado tanto para la red, como para el correo electrónico, como para los chats, etc.

-**Monitorización**: son herramientas que realizan un monitoreo del sistema. Por ejemplo, registran todas las páginas web visitadas para posteriormente poder supervisar los hábitos de navegación de los menores. No son las herramientas más óptimas ya que implican una mayor invasión a la privacidad de los menores y a la vez no son preventivas, sino solo de monitoreo.

Herramientas preventivas. Instalación y configuración.

Gran parte de los problemas que se presentan en los sistemas de nuestros equipos se pueden evitar o prevenir si se realiza un mantenimiento periódico de cada uno de sus componentes. Se explicará como realizar paso a paso el mantenimiento preventivo a cada uno de los componentes del sistema de cómputo incluyendo periféricos comunes. Se explicarán también las prevenciones y cuidados que se deben tener con cada tipo. En las computadoras nos referiremos a las genéricas (clones). Algunos ejemplos de herramientas administrativas a nivel software son:

-SpywareBlaster bloquea la entrada de spyware en tu sistema preveniendo que se instalen en el mismo elementos de spyware al deshabilitar los controles active X de los mismo sin interferir en aquellos controles active X inofensivos y de esa forma es posible navegar sin interrupciones de ningún tipo.
El programa actualiza periódicamente la lista de spyware y también permite deshacer los cambios llevados a efecto por los programas spyware en tu sistema. Se trata de un programa gratuito en inglés.

Spyware Guard proporciona protección contra el denominado spyware, pequeños programas
que se instalan sin tu conocimiento en tu sistema envíando información sobre tus preferencias a la hora de navegar. Funciona de manera similar a un antivirus, analizando los ficheros EXE y CAB cuando accedes a los mismos y te advierte si detecta algún tipo de spyware bloqueando el acceso al fichero y ofreciéndote la opción de tomar las acciones que consideres oportunas. Es sencillo de manejar siendo eficaz contra un gran número de spyware, de lo que se descatan CommonName, Brilliant Digital, HotBar y otros que a continuación ennumero:
AdBreak, AdultLinks/LinkZZ, CommonName,
Cytron, DV, FriendGreetings, Gator, HaczYK Dialer,
HighTraffic, HotBar IE Installer, HotBar
Netscape Installer, IEAccess2, IEDisco,
MasterDialer, MoneyTree Dialer, MS7531 Browser Hijacker Trojan, NetZany,
NewtonKnows, SubSearch, TGDC Plugin, UCmore, UKVideo2, VLoading, WinAD,
WorkPlaceCrush, Xupiter, etc.

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)
El control de acceso lógico es la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a personas autorizadas.
El principio más elemental de seguridad lógica es: Todo lo que no está permitido debe estar prohibido
Un control de acceso lógico conlleva a 2 procesos:

-**Identificación:** usuario se da a conocer en el sistema
-**Autentificación:** verificación que realiza el sistema sobre esta identificación.

Existen varios niveles de seguridad lógica dependiendo de la complejidad:
1º Nivel: arranque (bios y gestor de arranque)
2ºNivel: Sistema operativo y servidor de autentificación
3º Nivel: Datos, aplicaciones y comunicaciones

Política de contraseñas seguras

Para realizar un correcta política de contraseñas seguras, debemos de seguir los siguientes pasos:
-No incluir secuencias, palabras o nombres de usuario conocidos
-No dejar en blanco
-Variar entre servicios
-No revelarla, ni usarla en entornos poco seguros o públicos
-Modificarla con periodicidad

A nivel del administrador además de las anteriores, debemos añadir otras variables:
-No dejar la seguridad en manos de usuarios.
Disponer configuraciones que controle la configuración de contraseñas seguras.

Por otro lado existen configuraciones a nivel SO:

Windows

-Directivas de seguridad local/Directivas de cuenta
Visor de sucesos. Activar previamente auditorias

Gnu/Linux

Modulo PAM_cracklib
-Control de intentos de login: /var/login/auth.log
Control de acceso en la BIOS y gestor de arranque
El control de acceso a través de la BIOS nos supone un peligro ya que si esa contraseña es descubierta, tendrán acceso total a nuestro equipo.
En caso de la contraseña sea olvidada o este dañada, se utiliza un arranque con distribución live o un gestor de arranque vulnerable.

La configuración básica de una bios sera:
-Proteccion de acceso físico a la placa base
-Añadir una contraseña
-Poner como 1º dispositivio de arranque del disco duro al sistema de ficheros del SO Principal.

Control de acceso en el sistema operativo

Su objetivo es evitar el acceso no autorizado a los sistemas operativos. Se recomienda utilizar medios de seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos. Tales medios deberían tener la capacidad para:
-Autentificar usuarios autorizados, de acuerdo con una política definida de control de acceso.
-Registrar intensos exitosos y fallidos de autentificacion del sistema
-Registrar el uso de privilegios especiales del sistema.
-Emitir alarmas cuando se violan las políticas de seguridad del sistema
-Suministrar medios adecuados para la autenticación
-Cuando sea apropiado, restringir el tiempo de conexión de los usuarios

Política de usuarios y grupos
Las políticas de usuarios y grupos de un administrador de sistemas sera la siguiente:
-Determinar el nivel de seguridad de los datos y aplicaciones (clasificar la información, determinar el riesgo)
-Diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.
-Definicion de cuentas y su asignación a perfiles determinados, grupos o roles, así como asignación de privilegios sobre los objetos del sistema.
-Permisos de acceso a cada objeto del sistema. **Gestion en red LDAP/ Active Directory**,
dependerá del sistema operativo:
Windows: Directivas de seguridad local, Directivas de auditoria, Asignacion de derechos de
usuario y opciones de seguridad
GNU/LINUX: chmod (modificar), chown(propietario), chgrp (grupo) permisos sobre archivos.
-Listas de control de acceso (ACL): permite asignar permisos a un usuario, sin tener en cuenta el grupo al que pertenece.

Actualización de sistemas y aplicaciones
Mientras hacemos uso de Internet y sus servicios, los ciberdelincuentes- de forma análoga
a como haría un ladrón al intentar entrar a robar a una casa– desarrollan software malicioso.

para aprovechar cualquier vulnerabilidad en el sistema a través del cual infectarlo. Suelen
aprovechar las vulnerabilidades más recientes que tienen tanto el sistema operativo como
los demás programas, y que requieren una actualización inmediata de los sistemas.
Hay que tener en cuenta que cuanto más tiempo tardemos en actualizar nuestros equipos más tiempo estaremos expuestos a que cualquier tipo de malware pueda explotar alguna vulnerabilidad y nuestro equipo quede bajo el control del atacante.

Estas actualizaciones de software vienen justificadas por diferentes motivos:
• Corregir las vulnerabilidades detectadas.
• Proporcionar nuevas funcionalidades o mejoras respecto a las versiones anteriores.

6. Seguridad en la conexión con redes públicas:
Pautas y prácticas seguras:

Técnicas de Cifrado:
El cifrado es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo. Por ejemplo, si realiza una compra a través de Internet, la información de la transacción (como su dirección, número de teléfono y número de tarjeta de crédito) suele cifrarse a fin de mantenerla a salvo.
A continuación algunas de las técnicas de cifrado más utilizadas.

2.2.1.1.1-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.
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.

Criptografía asimétrica.
La criptografía asimétrica es el método criptográfico que usa 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.

La mayor ventaja de la criptografía asimétrica es que se puede cifrar con una clave y descifrar con la otra, pero este sistema tiene bastantes desventajas:
Para una misma longitud de clave y mensaje se necesita mayor tiempo de proceso.
Las claves deben ser de mayor tamaño que las simétricas.

-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 a clave y enviándolo al destinatario. Ya que compartir una clave simétrica no es seguro, la clave usada es diferente para cada sesión.
Tanto PGP como GnuPG usan sistemas de cifrado híbridos. La clave de sesión es cifrada con la clave pública, y el mensaje saliente es cifrado con la clave simétrica, todo combinado automáticamente en un sólo paquete.

-**Identificación Digital:**
Es la verificación de la identidad en línea. Se encuentra dentro de la teoría de la Web 2.0 y se trata de ofrecer la autenticación y la confidencialidad, protegiendo documentos de falsificaciones y manipulaciones.
Este sistema ya está operativo con diversas aplicaciones en funcionamiento y numerosos organismos en fase de incorporación al sistema.

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.

Firma Electrónica y Firma Digital.
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.

-Certificado Digital, Autoridad certificadora (CA).
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.

Documento Nacional de Identidad Electrónico (DNIe)
El desarrollo de la Sociedad de la Información y la difusión de los efectos positivos que de ella se derivan exigen la generalización de la confianza de los ciudadanos en las comunicaciones telemáticas.
Como respuesta a esta necesidad, y en el marco de las directivas de la Unión Europea, el Estado español ha aprobado un conjunto de medidas legislativas, como la Ley de Firma.

Electrónica y el RD sobre el Documento Nacional de Identidad electrónico, para la creación de instrumentos capaces de acreditar la identidad de los intervinientes en las comunicaciones electrónicas y asegurar la procedencia y la integridad de los mensajes intercambiados.

El nacimiento del Documento Nacional de Identidad electrónico (DNIe) responde, por tanto, a la necesidad de otorgar identidad personal a los ciudadanos para su uso en la nueva Sociedad de la Información, además de servir de impulsor de la misma. Así, el DNIe es la adaptación del tradicional documento de identidad a la nueva realidad de una sociedad interconectada por redes de comunicaciones.

Buenas prácticas en el uso del certificado digital y DNIe.
Tal y como recoge la Declaración de Prácticas de Certificación del DNI electrónico, los certificados electrónicos podrán utilizarse:

• **Como medio de Autenticación de la Identidad.**

El Certificado de Autenticación (Digital Signature) asegura que la comunicación electrónica se realiza con la persona que dice que es. El titular podrá, a través de su certificado, acreditar su identidad frente a cualquiera, ya que se encuentra en posesión del certificado de identidad y de la clave privada asociada al mismo.

• **Como medio de firma electrónica de documentos.**

Mediante la utilización del Certificado de Firma (nonRepudition), el receptor de un mensaje firmado electrónicamente puede verificar la autenticidad de esa firma, pudiendo de esta forma demostrar la identidad del firmante sin que éste pueda repudiarlo.

• **Como medio de certificación de Integridad de un documento.**

Permite comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación. La garantía de la integridad del documento se lleva a cabo mediante la utilización de funciones resumen (hash), utilizadas en combinación con la firma electrónica. Este esquema permite comprobar si un mensaje firmado ha sido alterado posteriormente a su envío.

Seguridad en la red corporativa:

Amenazas y ataques en redes corporativas:
Amenaza interna o corporativa y Amenaza externa o de acceso remoto.

El objetivo de estas amenazas es la violación de los sistemas, provocando la pérdida o modificación de los datos sensibles de la organización.
En cuanto a tipos de amenazas hay dos claros tipos:

Amenaza externa o de acceso remoto.

Son aquellas amenazas que se originan desde el exterior de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla, como son la localización, violación de la seguridad y evadir las pruebas. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos.

Amenaza interna o corporativa

Generalmente estas amenazas son más serias que las externas y pueden dañar seriamente al sistema, algunas amenazas pueden ser la paralización del sistema por daños físicos o la intrusión en la red internamente. Estas amenazas son potencialmente peligrosas por estos motivos:

- Los usuarios conocen la red y saben cómo es su funcionamiento.
- Pueden tener algún nivel de acceso a la red por las mismas necesidades de su trabajo.
- Los Firewalls son mecanismos no efectivos en amenazas internas.

Esta situación se presenta gracias a los esquemas ineficientes de seguridad con los que cuentan la mayoría de las compañías a nivel mundial, y porque no existe conocimiento relacionado con la planeación de un esquema de seguridad eficiente que proteja los recursos informáticos de las actuales amenazas combinadas.

Amenazas: Interrupción, Intercepción, Modificación y Fabricación.
Hay varios tipos de amenazas a los sistemas informáticos, que se pueden catalogar en:

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 (DOS)

Su objetivo es degradar considerablemente o detener el funcionamiento de un servicio ofrecido por un sistema o dispositivo de red.
Existen diferentes técnicas para la
explotación de este tipo de ataques:
Envío de paquetes de información mal conformados de manera de que la aplicación que debe interpretarlo no puede hacerlo y colapsa.
Inundación de la red con paquetes (como ser ICMP - ping, TCP – SYN, IP origen igual a IP destino, etc.)
que no permiten que circulen los paquetes de información de usuarios.
Bloqueo de cuentas por excesivos intentos de login fallidos.
Impedimento de logueo del administrador.

MAN-IN-THE-MIDDLE

El atacante se interpone entre el origen y el destino en una comunicación pudiendo conocer y/o modificar el contenido de los paquetes de información, sin esto ser advertido por las víctimas. Esto puede ocurrir en diversos ambientes, como por ejemplo, en comunicaciones por e-mail, navegación en Internet, dentro de una red LAN, etc.

IP SPOOFING - MAC ADDRESS SPOOFING

El atacante modifica la dirección IP o la dirección MAC de origen de los paquetes de información que envía a la red, falsificando su identificación para hacerse pasar por otro usuario. De esta manera, el atacante puede asumir la identificación de un usuario válido de la red, obteniendo sus privilegios.

PHARMING

Es la manipulación del mecanismo de resolución de nombres de dominio en Internet, llevada a cabo mediante la introducción de código malicioso en los servidores conectados a la red. Cuando un usuario ingresa una dirección en su navegador, ésta debe ser convertida a una dirección de IP numérica. Este proceso, que se denomina resolución de nombres, es llevado a cabo por servidores.

DNS (Domain Name Servers). En ellos se almacenan tablas con las direcciones de IP de cada nombre de dominio. El pharming consiste en adulterar este sistema, de manera que cuando el usuario cree que está accediendo a su entidad financiera en Internet, en realidad esta ingresado a una página Web falsa.

AIRsniffing

Consiste en capturar paquetes de información que circulan por redes inalámbricas. Para ello es necesario contar con una placa de red "wireless" configurada en modo promiscuo y una antena.

War Driving y Netstumbling

estas técnicas se valen del AIRsniffing, ya que consisten en circular (generalmente en un vehículo) por un vecindario o zona urbana, con el objeto de capturar información transmitida a través de redes inalámbricas. Esto es posible debido a que generalmente las ondas de transmisión de información en redes inalámbricas se expanden fuera del área donde se ubican los usuarios legítimos de la red, pudiendo ser alcanzadas por atacantes. Lo que en ocasiones las hace más vulnerables es la falta de seguridad con que se encuentran implementadas.

Riesgos potenciales en los servicios de red.

2.3.2.1-**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:

a) Conocimientos del sistema
b) Verificación de la integridad
c) Protocolos cifrados
d) Revisión de los registros
e) Paranoia (evitar ejecución de código externo. Aplicaciones “seguras”)
f) Eliminación de servicios innecesarios
g) Reglas de acceso (cotafuegos) TÍTULO

Ventajas

a) Control de acceso
b) Limita el alcance de los problemas de seguridad en redes locales

c) Limita la posibilidad de utilizar sistemas comprometidos para atacar a terceros
d) Limita la posibilidad de extraer información

Inconvenientes
a) Dificultad a la hora de configurarlos
b) Dificultad a la hora de instalar nuevos servicios
c) Dificultad con protocolos que usan puertos aleatorios
d) Ralentización
e) Importancia relativa en maquinas sin servicios y con accesos controlados
f) Mantener el sistema actualizado

g) **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

Seguridad en los servicios de red por niveles:

El modelo OSI está pensado para que cada capa opere independiente de las demás.
Esto significa que una capa puede ser comprometida sin que las demás lo noten.

Ataque en la Capa Enlace de datos
Mitos de la capa de enlace de datos
• Las direcciones MAC no pueden ser falsificadas.
• Un switch no permite hacer sniffing.
• Las VLANs están completamente aisladas unas de otras.

Ataques basados en MAC y ARP:
CAM Table Overflow
• Los switchs guardan las asociaciones MACPuerto e información de VLAN a medida que las “aprenden” en un tabla llamada tabla CAM.

• La tabla CAM de un switch tiene un tamaño fijo y finito.
• Cuando la tabla CAM no tiene espacio para almacenar más asociaciones MAC-Puerto envía a todos los puertos las tramas que tengan una dirección MAC destino no almacenada en la tabla CAM. (Actúa como un HUB para cualquier MAC que no haya aprendido)

• Se basa en el tamaño limitado de la tabla CAM.
• Para realizar el ataque sólo hace falta enviar gran número de tramas con direcciones MAC distintas (usualmente generadas al azar) a cualquier puerto del switch hasta que se llene la tabla CAM.
• Se desarrolló una herramienta para tal fin llamada macof.

Actualmente es parte del paquete Dsniff (GNU/Linux).
Address Resolution Protocol(ARP)
La solicitud ARP se coloca en una trama broadcast y se envía.
Todas las estaciones reciben la trama y examinan el pedido.
La estación mencionada en el pedido contesta y todas las demás estaciones

procesan la misma.

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 extranets. Los controles de acceso de usuarios basados en contraseñas no protegen por sí solos los datos transmitidos a través de una red.

Tipos comunes de ataques a redes

Si no se toman medidas de seguridad ni se aplican controles, los datos pueden ser objeto de un ataque. Algunos ataques son pasivos, en el sentido de que sólo se observa la información. Otros ataques son activos y se modifica la información con intención de dañar o destruir los datos o la propia red. Cuando no se tiene un plan de seguridad, las redes y los datos son vulnerables a todos los tipos de ataques siguientes.

Espionaje

En general, la mayoría de las comunicaciones por red tienen lugar en formato de texto simple (sin cifrar), lo que permite al atacante que haya logrado el acceso a las rutas de datos de una red observar e interpretar (leer) el tráfico. El espionaje de las comunicaciones por parte de un atacante se conoce como husmear. La capacidad de los espías para observar la red suele ser el mayor problema de seguridad que afrontan los administradores de las compañías. Sin unos servicios de cifrado eficaces basados en criptografía, mientras los datos atraviesan la red pueden ser observados por terceros.

Modificación de datos

Cuando un atacante ha leído los datos, a menudo el siguiente paso lógico consiste en modificarlos. Un atacante puede modificar los datos de un paquete sin que el remitente ni el receptor lo adviertan. Incluso cuando no se requiera confidencialidad en todas las comunicaciones, no se desea que los mensajes se modifiquen en su camino. Por ejemplo, si intercambia solicitudes de compra, no desea que se modifique la información relativa a los artículos, los importes ni la facturación.

Ataques basados en contraseñas

Un procedimiento común en la mayoría de los sistemas operativos y planes de seguridad de redes es el control de acceso basado en contraseñas. El acceso tanto a un equipo como a los recursos de la red está determinado por un nombre de usuario y una contraseña.

Históricamente, muchas versiones de componentes de sistemas operativos no siempre protegían la información de identidad cuando ésta pasaba por la red para su validación. Ello podría permitir a un espía detectar un nombre de usuario y una contraseña válidos, y utilizarlos para lograr acceso a la red haciéndose pasar por un usuario autorizado.

Cuando un atacante encuentra una cuenta de usuario válida y la utiliza para el acceso, obtendrá los mismos derechos que el usuario real. Por ejemplo, si el usuario tiene derechos administrativos, el atacante puede crear cuentas adicionales para tener acceso posteriormente.

Una vez obtenido el acceso a una red con una cuenta válida, el atacante puede hacer lo siguiente:

-Obtener listas de nombres de usuarios y equipos válidos e información de la red.
-Modificar las configuraciones de los servidores y de la red, incluidos los controles de acceso y las tablas de enrutamiento.
-Modificar, desviar o eliminar datos.

Ataque de rechazo de servicio
A diferencia de un ataque basado en contraseñas, el ataque de rechazo de servicio impide el uso normal de un equipo o de una red por parte de los usuarios autorizados.
Una vez obtenido el acceso a una red, el atacante puede hacer lo siguiente:
-Distraer al personal de sistemas de información para que no detecte inmediatamente la intrusión. Esto da al atacante la oportunidad de llevar a cabo ataques adicionales.
-Enviar datos no válidos a aplicaciones o servicios de red para provocar su cierre o su funcionamiento de forma anormal.
-Generar tráfico masivamente hasta provocar el colapso de un equipo o de toda la red.

Ataque por usuario interpuesto
Como su nombre indica, un ataque por usuario interpuesto se produce cuando alguien situado entre dos usuarios que se están comunicando observa activamente, captura y controla la comunicación sin que los usuarios lo adviertan. Por ejemplo, un atacante puede negociar claves de cifrado con ambos usuarios. A continuación, cada usuario enviará datos cifrados al atacante, quien podrá descifrarlos. Cuando los equipos se comunican en niveles bajos de la capa de red, quizás no puedan determinar con qué equipos están intercambiando datos.
Ataque de clave comprometida
Una clave es un código o un número secreto necesario para cifrar, descifrar o validar información protegida. Averiguar una clave es un proceso difícil y que requiere grandes recursos por parte del atacante, pero no deja de ser posible. Cuando un atacante averigua una clave, ésta se denomina clave comprometida.

El atacante puede utilizar la clave comprometida para obtener acceso a una comunicación protegida sin que el remitente ni el receptor lo perciban. La clave comprometida permite al atacante descifrar o modificar los datos. El atacante también puede intentar utilizar la clave comprometida para calcular otras claves que podrían suponer el acceso a otras comunicaciones protegidas.

Monitorización del Tráfico en redes
El monitoreo es saber la disponibilidad de la maquina, tiempos de respuesta por medio del ping. Saber que servicios de red se encuentran habilitados, si están en funcionamiento o han dejado de funcionar y ver los paquetes que se envían y reciben con información. Se usan unas herramientas para realizar el monitoreo.

Wireshark

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.

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.

10. Intentos de Penetración.

Un intento de Penetración es un análisis que permite detectar vulnerabilidades en un entorno informatizado mediante la búsqueda, la identificación y explotación de vulnerabilidades. Su alcance se extiende a:
-Equipos de comunicaciones;
-Servidores;
-Estaciones de trabajo;
-Aplicaciones;
-Bases de Datos;
-Servicios Informáticos;
-Casillas de Correo Electrónico;

-Portales de Internet;
-Intranet corporativa;
-Acceso físico a recursos y documentación;
-Ingeniería social (La ingeniería social es la técnica por la cual se obtiene información convenciendo al usuario que otorgue información confidencial, haciéndose pasar por usuarios con altos privilegios como administradores y técnicos).

Para realizar un Intento de Penetración es necesario realizar las siguientes tareas:
-Reconocimiento de los recursos disponibles mediante el empleo de herramientas automáticas.
-Identificación de las vulnerabilidades existentes mediante herramientas automáticas.
-Explotación manual y automática de las vulnerabilidades para determinar su alcance.
-Análisis de los resultados.

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 claras familias importantes 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.

Reconocimiento de ataques de "comparación de patrones": Esta técnica de reconocimiento de intrusión es el método más antiguo de análisis N-IDS y todavía es de uso frecuente.

Consiste en la identificación de una intrusión al examinar un paquete y reconocer, dentro de una serie de bytes, la secuencia que corresponde a una firma específica.

Esta táctica está difundida por los grupos N-IDS "Network Grep", que se basan en la captura de paquetes originales dentro de una conexión supervisada y en su posterior comparación al utilizar un analizador de "expresiones regulares". Éste intentará hacer coincidir las secuencias en la base de firmas byte por byte con el contenido del paquete capturado.
Existen otros métodos para detectar e informar sobre intrusiones, como el método Pattern Matching Stateful, y/o para controlar el tráfico peligroso o anormal en la red.

Tipos de IDS: (Host IDS, Net IDS).
Existen dos tipos de sistemas de detección de intrusos:
1) **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.
2) **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 commercial

El software libre (en inglés free software, aunque esta denominación también se confunde a veces con "gratis" por la ambigüedad del término "free" en el idioma inglés, por lo que también se usa "libre software") 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.
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:

-La libertad de usar el programa, con cualquier propósito (libertad 0).
-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.
-La libertad de distribuir copias, con lo que puedes ayudar a tu

vecino (libertad 2).
-La libertad de mejorar el programa y hacer públicas las mejoras a los demás, de modo que toda la comunidad se beneficie. (libertad 3). El acceso al código fuente es un requisito previo para esto.

El software comercial
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:
-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.
-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).
-En el software comercial se suele esconder y mezquinar los avances y descubrimientos tecnológicos entre las empresas que lo desarrollan.

-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.

Existen además tipos de software intermedios.
Software semilibre
Es aquel que mantiene las mismas características que el software libre para los usuarios individuales, entidades educativas o sin ánimo de lucro, sin embargo prohibe esas libertades para su uso comercial o empresarial.
Software propietario
Es aquel que no es libre ni semilibre; por lo tanto, su redistribución, modificación y copia están prohibidas o, al menos, tan restringidas que es imposible hacerlas efectivas.

Freeware
No tiene una definición clara y precisa, sin embargo suele usarse para clasificar al software que puede redistribuirse libremente pero no modificarse, entre otras cosas, porque no está disponible su código fuente. El freeware no es software libre.
Shareware
Es un software que permite su redistribución, sin embargo no viene acompañado de su código fuente y, por tanto, no puede ser modificado.
Además, pasado un periodo de tiempo, normalmente es necesario pagar una licencia para continuar usándolo, luego tampoco es software libre.

Sistemas de seguridad en WLAN.
Los paquetes de información en las redes inalámbricas viajan en forma de ondas de radio. Las ondas de radio -en principio- pueden viajar más allá de las paredes y filtrarse en habitaciones/casas/oficinas contiguas o llegar hasta la calle. Si nuestra instalación está abierta, una persona con el equipo adecuado y conocimientos básicos podría no sólo utilizar nuestra conexión a Internet, sino

también acceder a nuestra red interna o a nuestro equipo -donde podríamos tener carpetas compartidas- o analizar toda la información que viaja por nuestra red -mediante sniffers- y obtener así contraseñas de nuestras cuentas de correo, el contenido de nuestras conversaciones por MSN, etc.Si la infiltración no autorizada en redes inalámbricas de por sí ya es grave en una instalación residencial (en casa), mucho más peligroso es en una instalación corporativa. Y desgraciadamente, cuando analizamos el entorno corporativo nos damos cuenta de que las redes cerradas son más bien escasas.

Sin pretender invitaros a hacer nada ilegal, podéis comprobar la cantidad de redes abiertas que podéis encontrar sin más que utilizar el programa Network Stumbler o la función Site Survey o escaneo de redes de vuestro PDA con WiFi o de vuestro portátil mientras dáis un paseo por vuestro barrio o por vuestra zona de trabajo.

Para que una red inalámbrica sea segura ahí que tener en cuenta:
-**Cambiar la contraseña que trae por defecto**. Un fabricante usa la misma contraseña para todos sus equipos.
-**Usar encriptación WEP/WPA**. Activar en el Punto de Acceso la encriptación WEP, mejor 128 bits que de 64 bits… cuanto mayor sea el número de bits mejor. Cuidar la frase para generar las claves, que no sean palabras del diccionario, mezclar mayúsculas, números, que no sean letras seguidas de las teclas del ordenador etc.
-**Cambiar el SSID por defecto.** No usar palabras atractivas sino más bien "Broken", "Down" o "Desconectado". El SSID (Service Set IDentifier) es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.
-**Desactivar el broadcasting SSID**. Es uno de los métodos más básicos de proteger una red inalámbrica, desactivar el broadcast del SSID, ya que para el usuario medio no aparecerá como una red en uso.
-**Activar el filtrado de direcciones MAC.** Activa en el AP el filtrado de direcciones MAC de los dispositivos Wi-Fi que actualmente tengas funcionando. Al activar el filtrado MAC dejarás que sólo los dispositivos con las direcciones MAC especificadas se conecten a tu red Wi-Fi.
-**Establecer el número máximo de dispositivos que pueden Conectarse.**

11. 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.
La mayoría de los puntos de acceso o routers sin cable funcionan nada más conectarlos, o vienen configurados por el operador. Pero si se quiere modificar algo, como la seguridad, conviene conocer algunos de los parámetros de la conexión:

-**El identificador SSID:** es el nombre de la red WiFi que crea el punto de acceso. Por defecto suele ser el nombre del fabricante ("3Com" o "Linksys"), pero se puede cambiar y poner "PerezWiFi", por ejemplo.
-**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).

12.Recomendaciones de seguridad en WLAN.

Consejos finales para mejorar la seguridad.
- 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 inalambrico:** en general, el nombre de usuario es admin y la contraseña también es admin.

- Cambie el SSID por default del router inalambrico 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 esten 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.

-Establecer el uso obligatorio de una VPN corporativa y el cifrado cuando se hacen conexiones e intercambio de datos. Mejor aún, instalar computadoras y otros dispositivos móviles para que se conecten automáticamente a los datos cifrados de la VPN, de esta forma se pueden determinar sí el dispositivo no ha sido extraviado o robado.

-Establecer y hacer cumplir las políticas de fuerte autenticación para los dispositivos que intentan acceder a redes corporativas.
-Cerciorarse de que todos los dispositivos y aplicaciones de software están configurados correctamente y tienen los últimos parches.
-Asegurarse que las políticas de seguridad corporativa prohíban a las personas la transferencia de datos sensibles a dispositivos móviles o equipos no autorizados.
-Proporcionar a los trabajadores tarjetas de acceso a la banda ancha que requieren un plan de servicio, para que los empleados no tengan que usar los puntos de acceso públicos para conexiones inalámbricas.