Curso de Seguridad Infórmatica

Creada por V. Ana González Hernández

PRESENTACIÓN

Este curso ha sido desarrollado para acercar a los profesionales del mundo de telecomunicaciones a la seguridad informática.

No se presuponen ningún conocimiento previo del alumno en la materia, sí se entiende que el alumno está familiarizado con la informática en general.

A lo largo del curso iremos planteando ciertos temas de los cuales se pretende fijar conceptos básicos. Los temas irán acompañados de una parte práctica y autoevaluaciones disponibles en el portal .

Dentro de los pdf's hay enlaces externos que es importante seguir para poder adquirir un conocimiento completo. El contenido de estos enlaces no ha sido incluido de forma propia para evitar alargar en exceso los temas, sigue los enlaces de la distribución que te interese, el resto siempre estarán disponibles en el pdf a modo de consulta.

Decir que con este curso no tengo en mente “inventar la rueda”, porque ya está inventada y sigue rodando, si no proveer al alumno de una base en materia de seguridad, con lo cual utilizaré todos los recursos posibles para volver el contenido ameno y completo.

Creada por V. Ana González Hernández

Índice

Creada por V. Ana González Hernández

Curso de Seguridad Informática

Tema 1 Introducción a la Seguridad informática

Introducción

En nuestra vida cotidiana, en nuestra relación diaria con el mundo de la información, no solemos preocuparnos por el tema de la seguridad informática, ya que hemos adquirido una falsa sensación de confianza hacia un mundo que sabemos que existe pero nos es ajeno, o nos lo era, si podemos permitirnos este lujo y aún así surgen problemas ocasionales, es porque hay otros profesionales que dedican su vida a preservar nuestra seguridad.

A lo largo de este curso aprenderás cómo es el mundo de la seguridad informática, que profesionales componen este mundo e incluso abordaremos aunque muy brevemente algunas medidas de pentesting.

Bienvenid@ , esperamos que lo disfrutes y sea lo que estabas buscando.

-La Autora-

Creada por V. Ana González Hernández

¿QUÉ ES SEGURIDAD?

Podemos entender como seguridad algo que es libre y exento de todo peligro daño o riesgo, cierto, indubitable y en cierta manera infalible, firme constante y que no está en peligro de faltar o caerse, algo que no es sospechoso,.

Según la RAE Seguridad es definido como cualidad de seguro y seguro queda definido como:

seguro, ra.

(Del lat. *secūrus*).

1. adj.Libre y exento de todo peligro, daño o riesgo.

2. adj. Cierto, indubitable y en cierta manera infalible.

3. adj. Firme, constante y que no está en peligro de faltar o caerse.

4. adj. No sospechoso.

Pero, **¿son estas definiciones aplicables a la seguridad informática?**.

¿Podemos conseguir un sistema Libre y exento de todo peligro, daño o riesgo ?

Si nos vamos haciendo esta misma pregunta con cada una de las definiciones dadas por la Rae vamos llegando a la misma respuesta:

No podemos garantizar que nuestro sistema va a estar en todo momento libre o exento de todo riesgo, que valla a ser cierto, indubitable y en cierta manera infalible o que valla a mantenerse Firme y constante.

¿Por qué no podemos garantizarlo?

Porque existen una serie de amenazas constantes clasificadas en Amenazas Lógicas, Físicas ,y Ambientales que de paliarse de forma completa afectarían a la disponibilidad de nuestro sistema lo que hace que su implementación no sea viable.

De hecho me voy a permitir citar al experto en seguridad Eugene H. Spafford citado también en otros libros sobre la materia:

"EL único sistema que es totalmente seguro es uno que se encuentra apagado y desconectado, metido en una caja fuerte de titanio que está enterrada en cemento, rodeada de gas nervioso y de un grupo de guardias fuertemente armado, ¡Y aún así no apostaría mi vida por ello!"

Creada por V. Ana González Hernández

Todo las posibles amenazas, y terminología que nos os resulte familiar, la vamos a ir aclarando poco a poco, por tanto volvamos a a nuestra pregunta inicial.

¿Qué es la seguridad informática?

Pues ya que existen innumerables definiciones para esta materia, nosotros diremos que:

La seguridad informática es una rama dentro de la ingeniera informática que **se encarga del estudio y la puesta en funcionamiento de los diferentes métodos, herramientas y procesos para garantizar la Confidencialidad, Integridad, Disponibilidad , Autenticidad y no repudio** de un sistema informático entendiéndose sistema informático como**:**

- "El conjunto de partes interrelacionadas, hardware, software y de recurso humanos que permite almacenar y procesar información." (Definición de sistema sacada de la Wikipedia).

La seguridad no es un conjunto de medidas que se toman por única vez, sino un proceso dinámico en el que todos los actores juegan un rol permanente y debe de abarcar tres áreas de incumbencia: Personas , Procesos y Tecnología.

Existen varias ramas y profesionales dentro de esta materia o estrechamente relacionados con ella, algunos de ellas son:

Analistas de sistemas: Definen las pautas del sistema, deciden la función y utilidad de ese sistema. Deben crear las políticas adecuadas para el uso del sistema. Elaboran los planes de seguridad de la información, de los equipos y crean los entornos de pruebas

Pentesters: Se encargan de probar o intentar comprometer la seguridad de un sistema o de parte del mismo con el consentimiento de la empresa y a petición de la misma para elaborar un informe detallado de las vulnerabilidades encontradas y como subsanarlas. Auditan el sistema a petición del cliente. Pueden ser personal propio de la organización y dependiendo de ello hablaremos de diferentes tipos de auditorías, las cuales veremos con más detalle más adelante

Hackers: Son profesionales expertos en una o varias materias relacionadas con la seguridad, en algunos casos son contratados por las empresas o organizaciones para hacer auditorías expertas desde el exterior o para resolver problemas que no entran dentro de las competencias de los profesionales de la empresa. Hay varios tipos de hackers que también veremos con más detalle.

Forenses: Se encargan de la recopilación de pruebas y evidencias una vez el sistema ha sido alterado. Definen como debe tratarse el sistema y su información para poder recopilar evidencias de la intrusión o manipulación del mismo.

Criptólogos y Criptoanalistas: la criptografía es una rama de las matemáticas y actualmente de la informática que se encarga del estudio de métodos, algoritmos y técnicas de cifrado para proteger un mensaje o sistema granizando así su integridad confidencialidad y no repudio

Legalistas: Son los encargados de que la organización cumpla con las normativas vigentes en materia de de seguridad, informan a la organización de dichas normativas y de los requisitos necesarios para su cumplimiento

Los principales objetivos de la seguridad informática por tanto son:

- **Analizar los riesgos de seguridad adecuadamente para hacer posible la detección de problemas y amenazas minimizando así los riesgos**
- **Garantizar la adecuada utilización de los recursos, de las aplicaciones, y de los sistemas**
- **Limitar el impacto de la las perdidas, en el caso de producirse, y conseguir la adecuada recuperación del sistema después de un incidente de seguridad**
- **Cumplir el marco legal y con los requisitos impuestos a nivel organizativo**

Bien, veamos a qué nos referimos en cada uno de los puntos de nuestra definición:

- **Disponibilidad**: Se refiere a la capacidad de que las aplicaciones, los dato y el sistema se encuentre accesible a los usuarios autorizados en todo momento o el tiempo previsto al incluir las suspensiones programadas debidas a actualizaciones o mejoras programadas.

- **Confidencialidad:** La confidencialidad consiste en procurar un acceso confidencial al mensaje, la comunicación, los datos o al sistema en si. Quiere decir que sólo tendrán acceso personas o sistemas que hayan sido autorizados para ello y que estos no van a compartir esta información con terceros, haciendo de este modo que los datos resulten ajenos a quien no haya sido autorizado y por tanto confidenciales.

  Integridad de la información: Es la característica que hace que un sistema permanezca inalterado a no ser que estas modificaciones sean hechas por personal autorizado y queden registradas y documentadas.

  Un sistema integro es aquel que permite comprobar ni el propio sistema ni ninguna de sus partes ha sido manipulada en su forma original, es decir, es un sistema que no ha sido alterado.

- **Autenticidad:** Asegurar la identidad con certeza respeto al origen y procedencia del los datos , la información o el sistema. El objetivo que se pretende es la comprobación de que dichos datos o información provienen realmente de la fuente que dice ser.

- **No repudio:** No repudio quiere decir que ni el emisor ni el receptor de los datos pueden alegar que esa información no proviene de su fuente.

Una vez aclarados todos estos conceptos veamos como se relacionan entre si.

Si no existe la disponibilidad ya que el sistema se encuentra caído o sin servicio, el resto de los factores no son verificables, ya que los usuarios autorizados no tienen acceso así que no es posible procurarles un acceso confidencial ni verificar si los datos trasmitidos son íntegros y ya que no hay datos no hay origen ni destino del cual asegurar su certeza.

¿Se te ocurre algún ataque que afecte a la disponibilidad?

Creada por V. Ana González Hernández

Los ataques los vamos a ver más adelante, pero aún así, puedes haber encontrado en algún momento una página pública a la que no fuese posible acceder.

Esto puede ser debido a una falta de previsión por parte de los administradores ya que están recibiendo más tráfico del esperado, o debido a un ataque que está generando más tráfico del soportado para bloquear el servicio.
Este tipo de ataque se conoce comúnmente como Dos, Deniegal of Service o denegación de servicio.

Lo mismo nos ocurre con el resto de las capas de la seguridad, están íntimamente relacionadas, sin la confidencialidad no podemos garantizar la integridad ya que si la información ha sido divulgada es probable que también haya podido ser modificada o nuestras claves sean conocidas por lo que exista la posibilidad de que un intruso esté actuando con nuestra identidad dentro del sistema.

1.1.2 Amenazas de la seguridad

Al principio decíamos que existen una serie de amenazas físicas, lógicas y ambientales que deben ser medidas para proveer de seguridad a nuestro sistema.
Con amenaza nos estamos refiriendo a cualquier elemento que comprometa el sistema.

Veamos un poco cuales son los actores y sus roles:

Creada por V. Ana González Hernández

Amenazas Físicas:
Pueden ser desastres o catástrofes naturales.
Por ejemplo una inundación por exceso de lluvia, un incendio en el edificio.

Ante este tipo de situación poco podemos hacer excepto planificar desde un principio una red redundante tanto en la conexión como en los datos.

Pueden ser provocas por el factor humano:
- La excavadora que corta un tendido de fibra óptica y acaba con la conexión de todos nuestros servidores.
-El vaso de agua que se cae en el lugar menos oportuno...
-Pero también puede ser un trabajador descontento que desee llevase datos de la empresa y saque varios discos duros de algunos equipos.

Por esto nuestras maquinas siempre deben encontrarse en un lugar seguro, protegidas por cámaras de seguridad y otro tipo de medidas que veremos en un capitulo de este mismo curso.

Creada por V. Ana González Hernández

Amenazas lógicas:

La amenazas lógicas son aquellas que afectan o comprometen los datos y/o la información del sistema bien sea por un error del software, debido a la falta de actualizaciones oportunas, por una gestión incorrecta de los permisos de seguridad, no haber realizado los backups correspondientes cuando se debía, o por una intrusión ajena.
Por tanto cuando hablamos de seguridad lógica en un sistema hablamos de las barreras y procedimientos que protejan el acceso a los datos e información que contiene.

“”””
Las amenazas pueden ser analizadas en tres momentos: antes del ataque durante y después del mismo.

Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

a. La Prevención (antes): mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.

b. La Detección (durante): mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.

c. La Recuperación (después): mecanismos que se aplican, cuando la violación del

sistema ya se ha detectado, para retornar éste a su funcionamiento normal.
Por ejemplo recuperación desde las copias de seguridad (backup) realizadas.

Las preguntas que se hace un técnico en sistemas de información ante un problema de seguridad, normalmente, están relacionadas con medidas defensivas que no solucionan un problema dado, sólo lo transforma o retrasa. La amenaza o riesgo sigue allí y las preguntas que este técnico debería hacerse son:

¿Cuánto tardará la amenaza en superar la “solución” planteada?
¿Cómo se hace para detectarla e identificarla a tiempo?
¿Cómo se hace para neutralizarla?

Ya se trate de actos naturales, errores u omisiones humanas y actos intencionales, cada riesgo debería ser atacado de las siguientes maneras:

1. Minimizando la posibilidad de su ocurrencia.
2. Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
3. Diseño de métodos para la más rápida recuperación de los daños experimentados.
4. Corrección de las medidas de seguridad en función de la experiencia recogida.

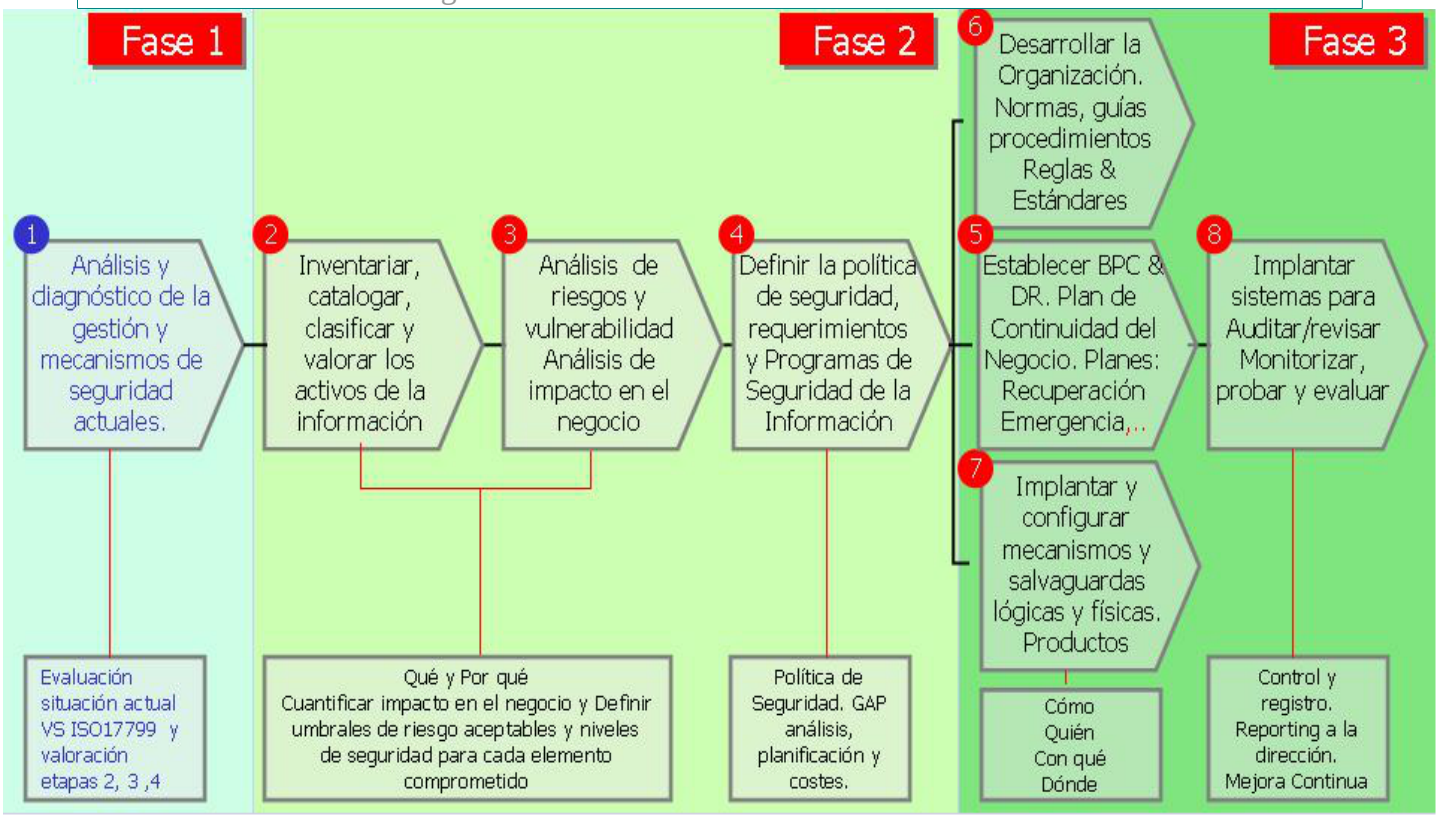
Luego, el Daño es el resultado de la amenaza; aunque esto es sólo la mitad del axioma. El daño también es el resultado de la no–acción, o acción defectuosa, del protector. El daño puede producirse porque el protector no supo identificar adecuadamente la amenaza y, si lo hizo, se impusieron criterios comerciales por encima de los de seguridad.
De allí que se deriven responsabilidades para la amenaza (por supuesto) pero también para la figura del protector.
Luego, el protector será el encargado de detectar cada una de las Vulnerabilidades (debilidades) del sistema que pueden ser explotadas y empleadas, por la amenaza, para comprometerlo.
También será el encargado de aplicar las contra-medidas (técnicas de protección) adecuadas. """ AUTOR: A.S.S. BORGHELLO, CRISTIAN FABIAN En su tesis de licenciatura.

Por supuesto si tenemos una caseta de perro en el jardín no le compramos una alarma antirrobo ni le ponemos puertas blindadas ya que sería un gasto innecesario comparado con el bien a proteger, pero seguramente a la casa donde esté esa caseta si nos parezca adecuado comprar dicha alarma.

En la seguridad informática pasa exactamente lo mismo, las medidas que se tomen deben de ser acordes a la información a proteger.

Pero la seguridad no va a ser la suma de las medidas del sistema, la seguridad del sistema será igual a su parte más débil.
Un administrador de sistemas tiene que administrar cada una de las maquinas, personas, redes, servidores y servicios de sus sistema. Un atacante sólo necesita encontrar un fallo para poder realizar la intrusión.

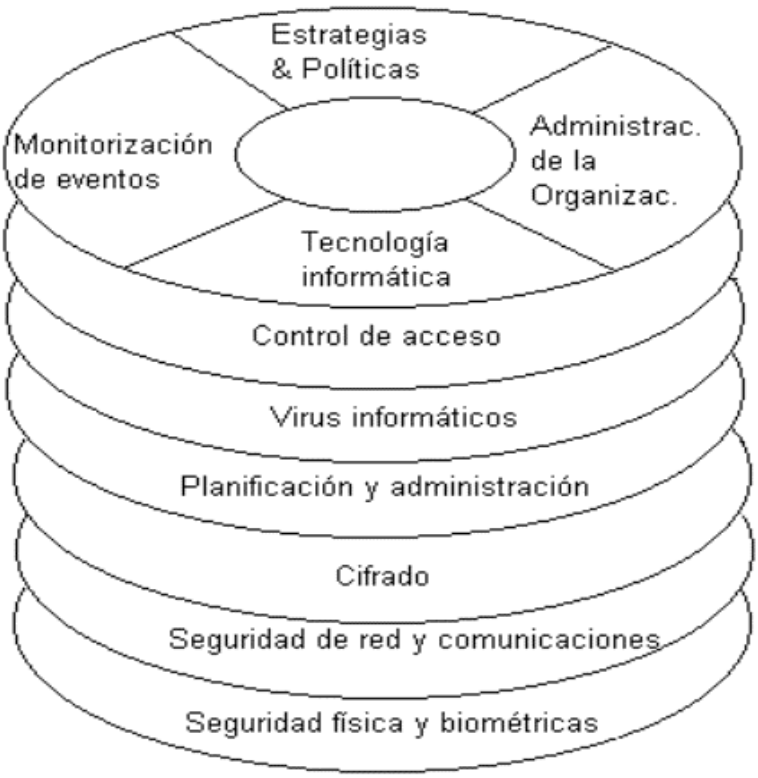
Veamóslo en las imágenes a continuación:



En primer lugar debemos de analizar la situación en la que nos encontramos siempre teniendo presente el tipo de medidas que se pueden implantar que son las mostradas en la imagen de la derecha.

Una vez estén inventariados y catalogados los activos hemos de analizar los riesgos existentes, estos riesgos pueden llegar a ser tolerables si el valor de nuestros activos es inferior al coste de implantación de las medidas de seguridad.

Cuando esto haya sido valorado estipularemos las políticas de seguridad adecuadas para nuestra organización.



PARTE PRACTICA

Creada por V. Ana González Hernández

Medidas prácticas para cada punto de la seguridad.

Disponibilidad

Para garantizar la disponibilidad de nuestro sistema programaremos copias de seguridad automáticas.

Los ejemplos y practicas a continuación se harán tanto en linux como en windows pero en los vídeos nos centraremos en linux únicamente, consideramos que windows al ser un sistema propietario y de pago debe de ofrecer este soporte al usuario.

Si nos hallamos en Windows Server podemos utilizar la herramienta incluida en sistema para este propósito

Nos vamos a Inicio buscamos el Command Prompt y lo ejecutamos como administrador:

A partir de hay la sintaxis es la siguiente:

wbadmin enable backup
[-addtarget:<BackupTarget>]
[-removetarget:<BackupTarget>]
[-schedule:<TimeToRunBackup>]
[-include:<VolumesToInclude>]
[-nonRecurseInclude:<ItemsToInclude>]
[-exclude:<ItemsToExclude>]
[-nonRecurseExclude:<ItemsToExclude>][-systemState]
[-allCritical]
[-vssFull | -vssCopy]
[-user:<UserName>]
[-password:<Password>]
[-quiet]

Podemos encontrar información en

http://technet.microsoft.com/en-us/library/c0e57f8a-70fa-4c60-9754-e762e8ad8772

http://technet.microsoft.com/es-es/library/cc731517(v=ws.10).aspx

O podemos instalar un programa para copias de seguridad.

Si nos encontramos en GNU/Linux :

Desde Sistema>Administración>Herramienta de copias de seguridad podremos programar nuestros backups.

También podemos hacerlo mediante cron.

Cron es un servicio que nos permite lanzar comandos automáticamente los días y a las horas que deseemos.
Cada usuario tiene su propio cron en el que puede configurar sus tareas programadas mediante el comando 'crontab -e' o con alguna aplicación gráfica como gnome-schedule.
En nuestro caso, como realizamos copia de seguridad de carpetas que solamente tiene acceso el usuario root, debemos programar la copia mediante el cron de root.

Supongamos que deseamos crear una copia de seguridad total los días 1 de cada mes y una copia de seguridad diferencial el resto de días en la carpeta /tmp (temporal), de las carpetas /home y /etc.

El comando que ejecutaremos el día 1 de cada mes será:

tar -jcvf /tmp/CopiaTotal_etc-home_`date +%d%b%y`.tar.bz2 /home /etc

Como puede verse, utilizamos `date +%d%b%y` que si hoy es 1 de febrero de 2012 se sustituirá por 1feb12. De esta forma nos sirve el mismo comando para todos los meses.

El comando que ejecutaremos todos los días para realizar la copia diferencial, será:

// Comando a ejecutar los días para hacer copia diferencial respecto al día 1

tar -jcvf /tmp/CopiaDiferencial_etc-home_01`date +%b%y`-`date +%d%b%y`.tar.bz2 /home /etc -N 01`date +%b%y`

Pero si no nos apetece utilizar cron podemos intalar cualquiera de estas herramientas de backup:

http://lamaquinadiferencial.wordpress.com/2010/02/11/aplicaciones-para-copias-de-seguridad-en-linux/

Pero no sólo de copias de seguridad vive el informático, debemos de procurar tener servicios de red redundantes, esto quiere decir si lo trasladamos al ámbito domestico que no nos cuesta nada tener un moden 3G de prepago guardado en un cajón si estar conectados a internet es de vital importancia para nuestro funcionamiento.

Si lo trasladamos al ámbito empresarial no debemos de confiar todo nuestro tráfico a una mismo punto de acceso, si no que nuestra red debe de tener también al menos otra red de backup.

Por supuesto tendremos que tener en cuenta las condiciones físicas de nuestras máquinas, sobretodo la temperatura, una maquinad que no esta correctamente refrigerada se apaga en el de los casos.

Por último debemos de ser conscientes de la carga de trabajo que nuestra maquina puede soportar y en caso de que sea mayor a la soporta ampliar sus capacidades.

Sirva como ejemplo el diseñador gráfico que se pone a trabajar con insuficiente memoria lo cual le causa que su equipo se bloquee debido a la carga en procesos de la memoria y este pierda todo su trabajo.

Nuestro hardware debe de ser adecuado a nuestros requerimientos.

Del mismo modo en caso de ser ser un servidor tienen que estar contemplados el número de usuarios previstos más un tercio mínimo adicional para que no se produzca un DoS natural.

Otra herramienta que podemos utilizar para descubrir vulnerabilidades en nuestro sistema tanto en windows como en gnu/linux, es nessus.

Nessus es un escaner de vulnerabilidades que nos será muy útil a la hora de hacer auditorias internas, podemos descargarlo de :

http://www.tenable.com/products/nessus

Confidencialidad
Para garantizar la confidencialidad de un sistema debemos implantar unas buenas políticas de gestión de usuarios, cifrado de unidades lógicas y encriptado de ficheros.

Gestión de usuarios.

Todos los usuarios deberán de tener una contraseña propia de acceso al sistema que deberá renovarse habitualmente, estas contraseñas no deben tener relación con sus contraseñas habituales, gustos o vida privada, la mejor forma de gestionarlo es que sean aleatorias generadas por un generador de contraseñas.

Ningún usuario debe de tener acceso a una carpeta o recurso que no necesite de forma

específica para realizar su labor habitual.

Todos los usuarios deberán de encriptar sus archivos y recursos, existen herramientas muy sencillas para ello en todos los sistemas operativos del mercado.

Desde Windows Server:

Tenemos la consola de administración de directivas de grupo (GPMC) podemos ver una documentación detallada al respecto en:

http://technet.microsoft.com/es-es/library/cc753298(v=ws.10).aspx

y contamos con dos herramientas útiles para verificar la salud de nuestro Directorio activo que podemos ver con detalle en el siguiente enlace:

http://blogs.technet.com/b/davidcervigon/archive/2007/09/10/dos-buenas-herramientas-para-el-directorio-activo.aspx

Para entender el funcionamiento de la gestión de políticas de contraseñas os dejo con el siguiente vídeo:

http://www.youtube.com/watch?v=0NPR6ngT2tg

Desde GNU/linux:

Podemos hacerlo de forma manual con el siguiente tutorial:

http://emslinux.com/usuarios-en-ubuntu-server/

O podemos instalarnos el Webmin, es una herramienta de gestión integral, que nos va a ser de bastante utilidad, ya que nos permite ver los logs de nuestro sistema y nos da información detalla del mismo a parte de permitirnos gestionar los grupos de usuarios.

Para instalarnos el Webmin podemos hacerlo de varias formas:

1 Descargar el paquete directamente con wget:

wget http://prdownloads.sourceforge.net/webadmin/webmin_1.630_all.deb
sudo aptitude install webmin

después ejecutamos

dpkg --install webmin_1.630_all.deb (necesitamos permisos de root)

La instalación se hará de forma automática en /usr/share/webmin.
Una vez haya acabado podremos loguearnos en http://localhost:10000/ con user root y nuestro password de root.
Si queremos acceder de forma remota debemos de reemplazar localhost por por la ip que corresponda.

Si durante la instalación nos dice que le faltan dependencias debemos instalar los siguientes paquetes:
apt-get install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime libio-pty-perl apt-show-versions python

2 Añadir Webmin a nuestro repositorios para que se actualice automáticamente:

Editamos /etc/apt/sources.list con nuestro editor favorito (nano, gedit, pluma, vim...):

Desde root: -# nano /etc/apt/sources.list
Y añadimos:

#webmin
#wget http://www.webmin.com/jcameron-key.asc **(estas son las claves, las dejo comentadas en los repos para no tener que buscarlas más)**
#apt-key add jcameron-key.asc
deb http://download.webmin.com/download/repository sarge contrib
deb http://webmin.mirror.somersettechsolutions.co.uk/repository sarge contrib

Cerramos guardando los cambios y ejecutamos:

cd /root
wget http://www.webmin.com/jcameron-key.asc
apt-key add jcameron-key.asc

apt-get update
apt-get install webmin

Todas las dependencias se resolverán de forma automática.
Una vez haya acabado podremos loguearnos en http://localhost:10000/ con user root y nuestro password de root.

Tenemos un tutorial completo en http://doxfer.webmin.com/Webmin/Tutorials.

Cifrado de unidades lógicas:
Para no entrar en detalle sobre el tipo de unidades y sistemas de ficheros, lo que nos podría llevar un capítulo entero os voy a presentar una herramienta útil tanto para windows como para linux.

TrueCypt
Nos permite cifrar archivos carpetas ficheros o el sistema entero.
http://www.kriptopolis.org/book/export/html/3729

Con esta herramienta acabamos la parte de confidencialidad.

Integridad autenticidad y no repudio
Debemos comprobar que la integridad de nuestro sistema no haya sido alterada por terceros, sin nuestro conocimiento.

¿Cómo puede ser alterar la integridad?

Por medio de rootkits (“”””Un **rootkit** es un programa que permite un acceso de privilegio continuo a una computadora pero que mantiene su presencia activamente oculta al control de los administradores al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones “”” fuente Wikipedia) y actualizaciones de procedencia dudosa o no verificada, pero incluso las actualizaciones que son de procedencia confiable pueden haber sido adulteradas en origen.

¿Cómo comprobamos esto sin abrir código por código de cada programa instalado e irlo revisando?

Pues se hace con funciones hash, con firmas digitales, con los certificados digitales y buscando en bases de datos como virus total.

Breve explicación de cada una de ellas, vamos a hablar en detalle en un capitulo más adelante:

Funciones hash:
Nos dan una garantía de que el archivo no ha cambiado. Fuente definición Inteco
Son el resultado del calculo de un algoritmo matemático que sirve para comprobar que los datos no han sido modificados ya que de haberlo sido el algoritmo daría como resultado una función distinta.
Por tanto si nos descargamos un archivo y en la página de descarga nos dan un hash, con este aspecto:

EJEMPLO:

Package-List:
```
 mate-core deb mate optional
 mate-desktop-environment deb mate optional
Checksums-Sha1:
 d980c6a21a2a58bf723307fc6f668ac75459e1b7 2225
mate-desktop-environment_1.4.0.tar.gz
Checksums-Sha256:
 972cd1030bd10f26ceb68d589d393e1a337ac21207814a452da43ae4c699346d 2225
mate-desktop-environment_1.4.0.tar.gz
Files:
 0a6f40a0a86baa4d78b5a1c368e36f76 2225 mate-desktop-environment_1.4.0.tar.gz
```

una vez descargado en nuestra maquina, cuando calculemos el hash debe de ser igual, si no lo es el archivo o descarga puede haber sido modificado.

Firmas Digitales

“”””Garantía de que el archivo no ha cambiado y proviene de una firma digital concreta, aunque nada garantiza que pertenezca a esa persona física determinada. ””””” Fuente definición Inteco

Tienen este aspecto:

```
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.11 (GNU/Linux)

iQEcBAEBAgAGBQJQBxEIAAoJEHvKqayQpKwUl7AIAKwKFRwxb1a48qg0oEaOb3c6
UvdBloGKkKWoCFVWz2aJ7B9YFiNrqsZWffKnyKqiy1PwFXO9DU0+NkN6v/KQfB7b
r4KmbnGrkgnsaJyBCU33M2E9Jwe9odJYKXcJfbxLnv34/U1yK86UapLArcXyzofj
vNIWGxnHIY72LJei+HSCjOs2Som5+QSgEXYM6B7AUk+w92rU1WA6knGalOTp3dJv
57a/7FmrPFWrRL1SstzdZB+YDMhiaLuvZwgqWQ7y+h3pxDsTMsj81hiZ7ERxx29h
nqWpOwtiM4ZBHvAVSGT7LcvVxjJMjVnZc9+LyznMU20hI3mGySciD/DPRVdo/IE=
=MPuC
-----END PGP SIGNATURE-----
```

Y son por ahora solamente diremos que son la forma de identificar el origen del del archivo.

Certificados Digitales

“”””Garantía de que el archivo no ha cambiado y proviene de una firma concreta, garantizada su identidad por una tercera parte confiable (Autoridad Certificadora) ”””Fuente definición Inteco

Pues también para resumir diremos que hay entidades oficiales que emiten estos

certificados para decir que la persona o entidad es quien dice ser.

Virustotal :
https://www.virustotal.com/es/

Y ya con estas nociones claras voy a presentaros las herramientas de rigor de momento sólo para poder comprobar que lo que descargamos es lo que realmente creemos y nos lo estamos descargando de quien realmente dice ser.

En Windows:

Herramientas de comprobación de hash:

- md5sum.exe, disponible desde
http://www.etree.org/cgi-bin/counter.cgi/software/md5sum.exe

-md5.exe disponible desde
http://www.fourmilab.ch/md5/

Y desde linea de comandos fciv, (File Checksum Integrity Verifier)
http://support.microsoft.com/kb/841290/en-us

Linux

Linux viene con herramientas ya instaladas, sólo tendremos que teclear lo siguiente:

$ md5sum <nombre del archivo ISO>
$ sha1sum <nombre del archivo ISO>

Firmas digitales:
Para comprobar las firmas digitales tanto en windows como en linux podemos hacerlo con gpg.
Si estamos en linux lo descargaremos e instalaremos desde los repositorios, para windows nos iremos a la página oficial: http://www.gnupg.org/download/

En ambos:

gpg --import KEYS
gpg --verify d:\httpd-2.2.3-win32-src.zip.asc

Y por último veamos cómo verificar que nuestro sistema no tiene rootkits:

Windows

SFC examina la integridad de todos los archivos del sistema, remplaza los que están corruptos o dañados y su sintaxis es bastante sencilla:

Sintaxis

sfc[/scannow] [/scanonce] [/scanboot] [/revert] [/purgecache] [/cachesize=x]

Parámetros
/scannow: Explora de inmediato todos los archivos del sistema protegidos.
/scanonce: Explora todos los archivos del sistema protegidos una vez.
/scanboot: Explora todos los archivos del sistema protegidos cada vez que se reinicia el equipo.
/revert: Devuelve la digitalización a su operación predeterminada.
/purgecache: Purga la caché de archivo de Protección de archivos de Windows y explora de inmediato todos los archivos del sistema protegidos.
/cachesize=x: Establece el tamaño, en MB, de la caché de Protección de archivos de Windows.
/?: Muestra la Ayuda en el símbolo del sistema.
Observaciones
Para ejecutar sfc, debe haber iniciado la sesión como miembro del grupo Administradores.
Si sfc descubre que un archivo protegido se ha sobrescrito, recupera la versión correcta del archivo de la carpeta raízDelSistema\system32\dllcache y luego reemplaza el archivo incorrecto.
Si la carpeta raízDelSistema\system32\dllcache está dañada o es inservible, utilice sfc /scannow, sfc /scanonce o sfc /scanboot para reparar el contenido del directorio Dllcache.

Linux

En linux tenemos otra gran herramienta que podemos instalar desde la terminal, se llama RootkitHunter

sudo aptidute install rkhunter

Con man rkhunter ó rkhunter --help podemos ver como utilizarlo en profundidad pero basta con tipear

rkhunter –checkall

Y con esto finalizamos el tema 1.

Creada por V. Ana González Hernández