SEGURIDAD EN REDES Y SISTEMAS INFORMÁTICOS

1
Ada_lovelance

UNIDAD 1.
INTRODUCCIÓN
Parte Práctica

Medidas prácticas para cada punto de la seguridad.

Disponibilidad

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

Los ejemplos y prácticas a continuación se harán tanto en Linux como en Windows pero nos centraremos más en Linux, ya que, 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 ahí, 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]
```

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 esta información ampliada para diferentes versiones de Windows 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
```

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`
```

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 instalar cualquiera de estas herramientas de backup:

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

Aunque si nos encontramos en un entorno con varios servidores de los cuales hacer backup, quizás queramos usar Bácula:

http://crysol.org/node/400

Pero no sólo de copias de seguridad vive el sys-admin, debemos de procurar tener servicios de red redundantes, esto quiere decir si lo trasladamos al ámbito doméstico, 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 maquina que no esta correctamente refrigerada se apaga en el mejor de los casos.

Por último debemos de ser conscientes de la carga de trabajo que nuestra máquina 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 un servidor tienen que estar contemplados el número de usuarios previstos más un tercio mínimo adicional para que no se produzca un DoS natural.

Pero a pesar de nuestras previsiones, hemos de ser muy conscientes de que nunca estamos exentos de riesgos, por lo que auditar nuestras máquinas con cierta periodicidad es una buena práctica que no debemos dejar de lado.

Para ello contamos con diferentes scaners de vulnerabilidades:

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

Nessus:

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

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

o su alternativa libre Openvass:

http://www.openvas.org/

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

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

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:

```
aptitude install perl libnet-ssleay-perl openssl libauthen-pam-perl
libpam-runtime
libio-pty-perl apt-show-versions python
```

apt-get install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime

libio-pty-perl apt-show-versions python

-2. Añadir Webmin a nuestros repositorios para que se actualice automáticamente:

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

desde root:

```
root@localhost -# nano /etc/apt/sources.list
```

root@localhost -# 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
```

#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
```

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:

Dentro de la página desde donde nos estemos descargando el paquete veremos algo como lo siguiente:

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 máquina, 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,

Aun que 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)

iQEcBAEBAgAGBQJQBxEIAAoJEHvKqayQpKwUl7AIAKwKFRwxb1a48qg0oEaOb3c6UvdBloGKkKWoCFVWz2aJ7B9YFiNrqsZWffKnyKqiy1PwFXO9DU0+NkN6v/KfB7br4KmbnGrkgnsaJyBCU33M2E9Jwe9odJYKXcJfbxLnv34/U1yK86UapLArcXyzofjvNIWGxnHIY72LJei+HSCjOs2Som5+QSgEXYM6B7AUk+w92rU1WA6knGalOTp3dJv57a/7FmrPFWrRL1SstzdZB+YDMhia

LuvZwgqWQ7y+h3pxDsTMsj81hiZ7ERxx29hnqWpOwtiM4ZBHvAVSGT
7LcvVxjJMjVnZc9+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 línea 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>
```

$ 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.