Universidad del Azuay

Facultad de Administración de Empresas

Escuela de Ingeniería de Sistemas

Seguridad Aplicada a Servidores SAMBA

Trabajo de Graduación previo a la obtención del Título de Ingeniero de Sistemas

Autores:
Peñaherrera Ramón Carlos Santiago
Alvarado Zenteno William Adrián

Director: Ing. Fernando Balarezo

Cuenca, Ecuador

2006

Dedicatoria:

Dedico esta tesis a todas
Las personas por las que vivo,
mi esposa, mi hija, mis hermanos y
en especial a mi madre y padre que
fueron quienes se aferraron a este
sueño, muchas gracias por todo
william

Agradezco a Dios por darme la oportunidad
de cumplir con este objetivo y a mi familia
por darme la fuerza y el valor para
hacerlo especialmente
a mis padres.
Gracias.
Santiago

Agradecimientos:

Queremos agradecer en primer lugar a Dios
por la oportunidad que nos dio de estudiar,
a la Universidad del Azuay
y sus profesores que permitieron que
nuestro proyecto se cumpla.

Índice de Contenidos

Índice de Ilustración y Cuadros

Cuadros. -

Gráficos. -

Índice de Anexos

Resumen y Abstract

El proyecto mencionado se orienta a la configuración de los diferentes niveles de seguridad que se pueden implementar en un servidor Samba, para la realización del mismo se utilizará el sistema operativo Linux CentOS versión 4.2 en el servidor y Windows XP en los diferentes terminales.

El objetivo del proyecto se orienta a establecer una eficaz y eficiente administración de los diferentes recursos existentes en el ámbito empresarial, los mismos que podrán ser software y hardware, teniendo en cuenta como software a los diferentes sistemas de administración, ya sean sistemas privados, bases de datos o ficheros compartidos de usuarios; y como hardware impresoras, fax, scanner, usb, cdrom, floppy etc.

El proyecto mencionado inicia desde la configuración del servidor Samba a manera de introducción, teniendo como puntos centrales los distintos Modos de Seguridad aplicables a una necesidad determinada.

Summary and Abstract

The project mentioned is oriented to the configuration of the different levels of security that are implemented in a server Samba, for the realization itself, utilized in the operative system Linux CentOS version 4.2, in the server and Windows XP in the different terminals.

The object of the project is oriented to established an efficient and effective administration of the different existing resources in the business field, the same that can be software and hardware, taking in account the data base or card indexes of shared users; and like hardware printers, fax, scanner, USB, cdrom, floppy etc.

The project mentioned starts from the configuration of the server Samba as a way of introduction, having like central points the distinct Modes of Security applicable to a necessity determined.

Introducción

Las razones principales que motivaron la realización del proyecto de tesis son el obtener un conocimiento global del servicio que ofrece los servidores Samba en un entorno de red, cualquiera que este fuere a la vez de controlar y administrar los recursos de una manera eficaz y eficiente de forma que sean útiles para el desarrollo empresarial a nivel de usuarios, administradores e invitados.

Así también, generar una conectividad entre dos plataformas distanciadas como son Windows y Linux, esta tarea se vuelve cada día mas trascendental ya que en la actualidad se utiliza mucho o casi siempre el sistema Linux como servidor de datos, correo y recursos, y el sistema Windows para usuarios finales y aplicaciones, Samba nos permite realizar esta tarea pero no seria completa sin su debida administración y seguridad con relación a sus recursos.

Tenemos la seguridad que este proyecto será de gran aporte para lograr un verdadero conocimiento de lo que podemos mejorar en el ámbito de seguridad dentro de una organización, teniendo en cuenta que el mayor ataque a la información y recursos de las mismas proceden dentro de la empresa, una ventaja adicional para este servicio es que Samba es uno de los proyectos de Software Libre mas importantes en la actualidad, razón por la cuál los diferentes Gerentes de Sistemas podrán instalar el software con todas sus opciones sin ningún costo.

Los niveles de seguridad son el conjunto de medidas de carácter técnico y organizativo que se deben tener en cuenta el momento de configurar un servidor en un entorno de red empresarial, es por esto que como objetivos hemos precisado el logro de un completo nivel de seguridad en cada escalafón de las empresas como pueden ser usuarios administradores, generales o simplemente invitados.

Para la realización del proyecto mencionado se utilizará tanto investigación bibliográfica como práctica mediante la realización de pruebas e instalación, valiéndonos de un entorno de red con sistemas Windows XP funcionando como terminales.

Capítulo 1

Visión Global de Samba

Objetivo -

La conectividad entre un equipo instalado con el Sistema Operativo Linux y equipos instalados con el sistema operativo Windows es primordial, ya que esto nos permitirá compartir recursos a mas de poder administrarlos; esta tarea podemos realizarla a través de la configuración de un servidor SAMBA.

"Samba es una suite de aplicaciones Unix que habla el protocolo SMB (Server Message Block). Muchos sistemas operativos, incluidos Windows y OS/2, usan SMB para operaciones de red cliente-servidor. Mediante el soporte de este protocolo, Samba permite a los servidores Unix entrar en acción, comunicando con el mismo protocolo de red que los productos de Microsoft Windows. De este modo, una máquina Unix con Samba puede enmascararse como servidor en tu red Microsoft y ofrecer los siguientes servicios:

- Compartir uno o más sistemas de archivos.
- Compartir impresoras, instaladas tanto en el servidor como en los clientes.
- Ayudar a los clientes, con visualizador de Clientes de Red.
- Autentificar clientes logeándose contra un dominio Windows.
- Proporcionar o asistir con un servidor de resolución de nombres WINS

"

Fuente:http://es.tldp.org/Manuales-LuCAS/USANDO-SAMBA/usando-samba-html/node3.html

Samba. -

Samba es un proyecto de software libre con la intención de llegar a conectar redes heterogéneas, generalmente Linux y Windows aunque soporta también conectividad con Mac OS, la estructuración del archivo principal de configuración smb.conf, cuenta con comentarios útiles el momento de configurar el servidor, razón por la cuál Samba se vuelve manejable y relativamente sencillo de implementar a la ves que provee un servicio eficiente dentro de un entorno de red, a mas de esto muchos técnicos y programadores han desarrollado herramientas para facilitar el trabajo de configuración, como por ejemplo web-min, que es una herramienta totalmente grafica y amigable, en la cuál se puede administrar al detalle los recursos a compartir, es por esto que Samba se ha vuelto muy popular y es usado por una gran cantidad de usuarios en el mundo.

Anexo 1.1: Roles de Samba (desde 2.0.4b).

1.1 Herramientas necesarias. -

Paquetes a instalar. -

Los paquetes de Samba por lo general suelen ser tres:

1. - samba-common
2. - samba
3. - samba-client

Samba-Common. -

Es el primer paquete, se encarga de que los dos paquetes siguientes funcionen correctamente, maneja las herramientas de conversión de tablas de caracteres Windows, los ficheros de configuración y la documentación.

Samba. -

En este paquete se encuentran localizados todos los archivos de configuración tales como el smb.conf que es el principal, a más de smbuser y lmhosts, los cuáles proveen de parámetros necesarios para la implementación de recursos compartidos**,** en este directorio también se encuentra la documentación de Samba.

Samba-Client. -

Es el último paquete, permite conectarse con los recursos compartidos de clientes Windows y Linux, maneja un ambiente Gráfico parecido al ftp caractérico.

Cuadro1.1: Herramientas de configuración samba:

- **smbclient**. Un cliente SMB para Unix con interfaz similar a FTP.
- **smbtar**. Un utilitario para respaldar datos compartidos a través de la red.
- **nmblookup**. Un utilitario para consultar nombres NetBIOS sobre TCP/IP.
- **smbpasswd**. Un utilitario administrativo para los passwords de Samba.
- **smbstatus**. Un utilitario para listar las conexiones al servidor Samba.
- **testparm**. Un utilitario para validar la configuración de Samba.
- **testprn**. Un utilitario para validar las impresoras de Samba.

Fuente.- http://bulma.net/body.phtml?nIdNoticia=615

1.2 Demonios.-

Dos demonios se encargan de ofrecer los servicios del conjunto de aplicaciones samba. El primero es el **smbd** y el segundo de ellos es el **nmbd.**

Smbd: es el demonio que se encarga de la compartición de recursos, ficheros, impresoras, etc, y al mismo tiempo del control del acceso a los recursos; gestiona los permisos de los diferentes clientes una vez que estos han sido identificados.

Nmbd: El demonio **nmbd** se ocupa de anunciar los servicios, es decir, se encarga de informar a las máquinas presentes en la red sobre cuáles son los recursos disponibles. Este demonio maneja también la resolución de nombres de NetBios; o sea permite que el host UNIX pueda verse desde la red Windows ya sea por Entorno de Red o Mis Sitios de Red, y de esta manera acceder al servidor SMB.

1.3 Principales ficheros para la configuración samba. -

Fichero lmhosts

En este fichero se especificará las distintas direcciones IPs con su respectivo nombre NetBios. El nombre NetBios debe tener un máximo de 8 caracteres. Este fichero se encuentra bajo la ruta /etc/samba/lmhosts.

Se debe añadir el nombre de equipo que se haya elegido para la terminal Windows, este se puede observar en "propiedades" de "Mi PC", asociado a la dirección IP que tenga la misma, dentro de la red local. Opcionalmente podrá añadir también los nombres y direcciones IP del resto de las máquinas que conforman el grupo de trabajo en el entorno de red.

Ejemplo:

127.0.0.1 localhost
192.168.1.1 maqlinux
192.168.1.2 maqsecre
192.168.1.3 maqconta

Fichero smb.conf. -

Este fichero se encuentra en la ruta /etc/samba/; smb.conf es un archivo plano que puede modificarse con cualquier editor de texto como el "vi" o el "gedit". Dentro de este fichero se encuentra la información que será de utilidad para la configuración del servidor, se puede decir que este es el principal archivo, ya que en él se encontraran todas las posibilidades y sus configuraciones para la administración y seguridad de los diferentes recursos, sus líneas vienen comentadas con un símbolo numeral "#" y los ejemplos con punto y coma ";", siendo estos últimos los que tomaremos como referencia para nuestra configuración.

Secciones del Fichero smb.conf. -

El fichero smb.conf consta principalmente de tres partes o secciones que son:

[global]
[homes]
[printers].

Sección [global].- en esta sección se configura las principales opciones del servidor con relación a la red de área local en el que trabajará, aquí se definirá el tipo de

seguridad a utilizar, así también como los diferentes hosts a los que se les permitirá el acceso, host denegados el acceso, si las contraseñas serán encriptadas, archivos .log (temporales) de cada usuario; como podemos observar, esta parte es muy importante ya que controlará la manera en que se realizarán las conexiones a nuestros recursos.

Para establecer el grupo de trabajo se edita el valor del parámetro workgroup asignando el grupo de trabajo deseado:

Workgroup = UDA

Luego se establece el parámetro netbios name, este definirá el servidor en el que se relacionarán las IPs con los nombres de máquina, en este caso es el mismo servidor, tomando en cuenta que dicho nombre deberá corresponder con el establecido en el fichero /etc/samba/lmhosts:

Netbios name = maqlinux

El parámetro Server string indica como se va a mostrar el servidor en el entorno de red

Server string = Servidor Samba Tesis UDA

existen más parámetros siendo los mencionados los más importantes.

Anexo 1.2: Principales opciones de la sección [global] de Samba

Sección [homes]. - en esta sección se definirán los recursos que se van a compartir, sus diferentes permisos y demás características que se explicarán detenidamente en el capítulo dos.

Sección [printers]. -en esta sección es exclusivamente para los recursos de impresión, aquí definiremos sus permisos y características.

1.4 Herramienta web de configuración. -

Es posible modificar directamente los ficheros de configuración con un editor de texto, pero podemos también configurar los mismos con la ayuda de una interfaz gráfica, obteniendo idéntico resultado. Una de ellas es el manejo del **WEB-MIN,** se

trata de una interfaz que se comporta como un servidor Web. El servidor web-min se ejecuta en el puerto 10000.

1.5 Conclusiones. - El servidor Samba cuenta con grandes características para administrar los recursos en una organización a mas de la ventaja de ser un software completamente gratis y fácil de adquirir, su relación con Windows cada día mejora mas, por estas razones se puede concluir que su uso debe ser muy bien estudiado por las personas encargadas de los departamentos de sistemas, de manera que su pueda aplicar y beneficiar de sus utilidades a los usuarios de cualquier organización.

Capítulo 2

Controlando el acceso a los recursos compartidos

Objetivo.- Este capítulo abarca los diferentes formas en las que se podría administrar los recursos en un servidor Samba, empezaremos estudiando los tipos de restricciones que existen para realizar esta labor, luego abordaremos el tema de autentificación, el mismo que se relacionará y se profundizará en el capítulo tres, el objetivo es obtener una idea concreta de la forma en que un servidor Samba labora, es importante mencionar la forma en la que el servidor Samba maneja los diferentes tipos de usuario en especial el usuario invitado, en este punto conoceremos en que modos es factible permitir el ingreso a los usuarios invitados.

Para finalizar el capítulo se estudiará las formas de iniciar el servidor a mas de indicar la manera básica de acceder a los recursos y empezar a trabajar.

2.1 Restricción de acceso a recursos. -

El acceso a los recursos puede controlarse de dos formas:

1. Escondiendo el recurso, es decir, no anunciándolo a ciertas máquinas de la red, este punto se puede conseguir mediante la cláusula "host deny".
2. Estableciendo un sistema de validación basado en usuario/contraseña, que nos permita reconocer a cada uno de los usuarios que intentan conectar.

El grupo de trabajo es un parámetro básico, ya que mediante el cuál podemos administrar recursos a ciertos tipos de usuarios, si necesitáramos utilizar distintos grupos de trabajo, deberíamos tener también distintos servidores Samba de manera que cada uno preste recursos a su grupo específico, esto nos permite separar conjuntos de recursos.

2.2 Diferentes formas de autentificación. -

Existen 3 formas distintas de autentificación, cada una con sus ventajas e inconvenientes.

1. La autentificación por usuario/contraseña
2. El control de acceso por recurso compartido
3. Autentificación contra otro servidor

2.2.1 Autentificación por usuario/contraseña. -

Se trata del método por defecto, representa la ventaja de permitir una gestión de los permisos. Para cada usuario es posible definir el acceso o no a los recursos compartidos. Este método presenta una característica, cada usuario debe disponer de una cuenta en la lista de usuarios Samba del servidor, para que se le permita la autentificación.

2.2.2 Control de acceso por recurso compartido. –

Se trata de un método más general, cada recurso compartido es protegido por un password propio, si el recurso necesita tener diferentes tipos de uso, como por ejemplo de lectura para un grupo y de escritura para otro, este se deberá configurar con dos claves distintas, de manera que se pueda lograr la tarea antes mencionada; para ello es necesario que varios usuarios conozcan el mismo password y que recuerden la contraseña adecuada para cada recurso compartido al que accedan.

Este método presenta la ventaja de que no son tantas cuentas de usuario como usuarios haya, sino tantas como recursos se compartan.

2.2.3 Autentificación contra otro servidor. –

Existen también dos métodos indirectos de control de acceso

Server Password.- este método requiere de un servidor específicamente para validación de contraseñas, los distintos usuarios y claves deberán estar registrados en este servidor, de manera que el servidor Samba sólo trabaja como servidor de recursos, este método es muy utilizado a nivel de seguridad ya que se puede impedir el acceso al servidor de passwords, evitando de esta manera posibles ataques a los archivos de configuración smb.

Server NT.- el segundo método es utilizando un servidor NT, la lógica de la autentificación es la misma sólo que en este caso los usuarios beberán estar registrados en el dominio NT con Active Directory.

2.2.4 Autorizar el acceso a los invitados. -

Autorizar el accedo a los invitados se realiza mediante la cláusula "guest" la misma que va relacionada a la par con la cláusula "guest account" que definirá el usuario por defecto que usará el invitado, este método no es muy recomendable, ya que usuarios de otros grupos podrían acceder a los recursos que no sean propios del mismo, con el simple echo de cambiar su grupo, para mayor seguridad se recomienda adicionalmente usar las cláusula "host allow" y "host deny".

2.2.5 Limitaciones de acceso a los usuarios. -

La limitación de acceso a los usuarios se realiza mediante la cláusula "valid users", esta especificará de manera concreta que usuarios tienen acceso, en caso de que esta cláusula no se especifique todos los usuarios del servidor Samba podrán acceder a los recursos, cabe mencionar que se puede también definir si los usuarios tendrán acceso para escritura con la cláusula "read only = no" o sólo lectura, cambiando su valor por "read only = yes", con esto se puede configurar carpetas para varios usuarios dando diferentes formas de acceso para cada uno de ellos.

2.3 Inicio del servidor.-

Existen dos formas de iniciar el servicio smb, la primera es utilizando un script en el archivo /etc/rc.local, este archivo se lee en la inicialización del sistema, el script se escribiría de la siguiente manera:

```
cd /etc/samba/
service smb start
```

o también se puede llegar al mismo objetivo ejecutando en la línea de instrucciones lo siguiente:

```
/sbin/chkconfig smb on
```

Existen otras opciones para el manejo del servicio como son:

```
service smb stop        detiene el servidor Samba
service smb start       inicia el servidor Samba
service smb restart     reinicia el servidor Samba
```

2.3 Acceso a los recursos compartidos.-

Modo texto.

Indudablemente el método más práctico y seguro es el instrucción smbclient, éste permite acceder hacía cualquier servidor Samba o Windows como si fuese el instrucción ftp en modo texto.

Para acceder a algún recurso de alguna máquina Windows o servidor SAMBA determine primero que volúmenes o recursos compartidos posee está, para esto se utiliza la instrucción smbclient del siguiente modo:

smbclient –U usuario –L alguna _ máquina

La siguiente corresponde a la sintaxis básica para poder navegar los recursos compartidos por la máquina Windows o el servidor SAMBA:

smbclient //alguna _ máquina/recurso –U usuario

Ejemplo:

Smbclient //LINUX/FTP –U usuario1

Después de ejecutar lo anterior, el sistema solicitará se proporcione la clave de acceso del usuario usuario1 en el equipo denominado LINUX.

Pueden utilizarse virtualmente las mismos instrucciones que en el interprete de ftp, como serían get, mget, put, del, etc.

Anexo 1.3. - Principales opciones de los recursos en Samba

Conclusiones.- Se debe mencionar que el control de acceso a los recursos comprende muchos puntos a los que se les debería dar la importancia que se amerita, ya que esta tarea es vital para asegurar y administrar los elementos que tenemos a nuestra disposición en una entidad, labor que deberá ser cumplida por el administrador de red según un estudio previo de las diferentes necesidades de cada usuario.

El hecho de restringir tareas como pueden ser modificación de configuraciones, no sólo en el servidor sino en las distintas terminales que se pueda tener, garantiza fuentes confiables de datos así como de recursos, a medida que la autentificación sea mas estricta podremos mantener una mayor confianza y garantiza nuestros recursos.

Capítulo 3

Modos de seguridad

Objetivo.- En este capítulo se dará a conocer los diferentes modos de seguridad aplicables en un servidor Samba, básicamente se maneja dos modos, a nivel de recurso compartido y a nivel de usuario, este modo a su ves se divide en seguridad a nivel de usuario, dominio y servidor.

Se dará a conocer cada uno de los modos con sus diferentes opciones, de manera que se pueda concluir y seleccionar el modo que mas se adapte a uno u otro ambiente, dependiendo básicamente del nivel de confianza que se tenga hacia los usuarios.

3.1 Modo de seguridad a nivel de recurso compartido (Share). -

La seguridad a nivel de recurso compartido usa las combinaciones de nombre de usuario y contraseña guardadas en el sistema y que nos servirán para autentificar el mismo, con el uso de parámetros que se dan a conocer mas adelante se puede manejar el acceso a los recursos sin importar el usuario remoto que este intentando conectarse, cabe destacar el comentario que ha sido echo por algunos de los clientes de Microsoft Windows que han utilizado este método, "Han surgido informes recientes que dicen que existen problemas de compatibilidad entre clientes Windows y servidores de seguridad a nivel de recurso compartido, es por esta razón que los propios desarrolladores de samba no recomiendan el uso de la seguridad en este nivel."

Fuente: BANDEL, David y NAPIER Robert, Edicion Especial Linux 6ta edición, 6th ed., Vol 1, PEARSON EDUCACION, Madrid, 2001, Cap 29 ".

Cada recurso compartido puede permitir autentificar diferentes contraseñas asociadas con él, mediante la especificación en la cláusula "valid users", esto con el fin de permitir flexibilidad al mismo, por ejemplo otorgar a ciertos usuarios permisos de

sólo lectura, a otros, lectura-escritura, etc, esta seguridad seria válida mientras las contraseñas no lleguen a ciertos usuarios no autorizados.

Anexo 1.4. - Opciones de seguridad a nivel de recurso.

La seguridad se implementa directamente dentro del archivo smb.conf, la directiva es la siguiente

[GLOBAL.]

security = share

……..

[COMPARTIDA]

Path: especifica la ruta del recurso compartido

Path = /Archivos/carpeta8

Guest account: parámetro que especifica el usuario del cuál se heredaran las propiedades para acceder al recurso, generalmente se especifica al usuario ftp.

Guest account = ftp

Guest ok: parámetro que define si el usuario accederá con password o sin password

Opciones:

Guestok = yes; el usuario accede libremente hacia el recurso, con las propiedades del usuario definido en el guest account.

Guestok = no; el usuario necesitará digitar la contraseña para acceder al recurso al menos la primera ves, luego accede libremente.

Username: este parámetro define específicamente los usuarios contra los que Samba validará la contraseña digitada en el lado remoto, ingresará al recurso aquel que digite una contraseña que coincida con alguna de los usuarios especificados aquí, trabaja junto con guestok = no; ya que con guestok = yes pueden acceder al recurso cualquier usuario.

Ejemplo:

Username = usuario1, usuario2

Onlyuser: este parámetro permite conexiones solamente a los usuarios detallados en username, en lugar de aquellos establecidos en la lista interna de Samba.

Ejemplo:

[Compartida]

Username = usuario1, usuario2

Onlyuser = yes

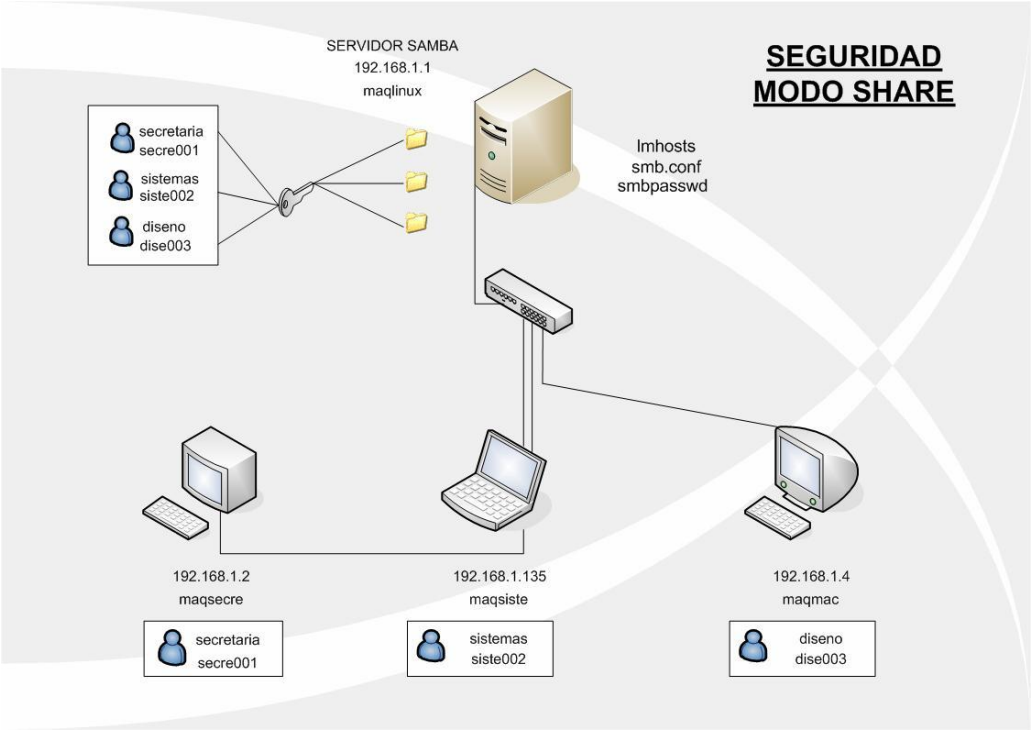
Writeable; este parámetro define si los recursos tienen permiso de escritura, si no se especifica o por defecto esta en "no",

Writeable = yes

Revalidate; este parámetro se usa para validar nuevamente una contraseña cuando el usuario inicie sesión en la máquina remota.

Revalidate = yes

Gráfico 1.1: Modo de Seguridad a Nivel de Recurso Compartido



3.2 Modo de seguridad a nivel de usuario (user). -

La seguridad a nivel de usuario viene por defecto en el servidor, así no se la mencione en el archivo de configuración (smb.conf), la configuración se la realiza en el recurso compartido, especificando los usuarios que tendrán acceso, samba se vale de la conexión inicial del usuario para la respectiva validación, de manera que se valida el nombre de máquina Netbios y el usuario de la sesión actual con su respectiva contraseña.

Este modo es el más aconsejable para trabajar, ya que se puede administrar los recursos solamente para los usuarios que realmente lo necesiten, la manera de indicar al servidor Samba que se utilizará el modo "user" es la siguiente.

[GLOBAL.]
security = user
……..

El modo usuario es el más utilizado en la actualidad, ya que se puede compartir las carpetas usando diferentes parámetros, una gestión adecuada de los recursos compartidos se lo realiza mediante la combinación de estos parámetros.

Proceso de autentificación. -

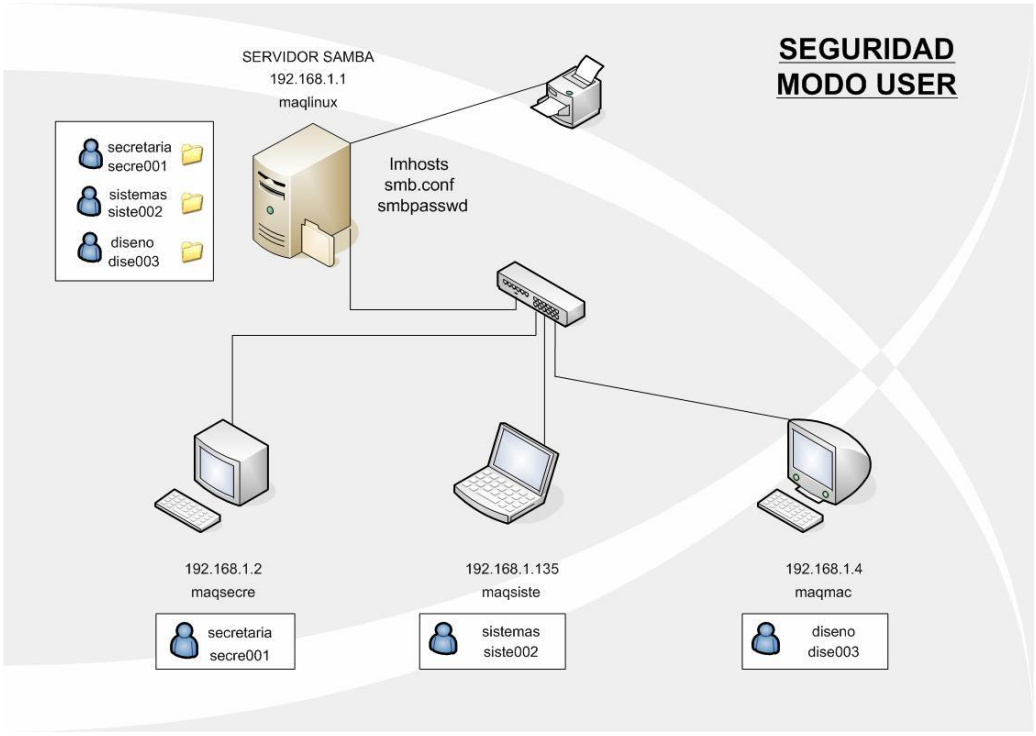
Samba autentifica validando el nombre de usuario y la contraseña frente a los usuarios autorizados en el fichero de configuración y las contraseñas almacenadas en la lista de usuarios del servidor Samba.

A cada uno de los usuarios especificados en el recurso se le permitirá el acceso al mismo si la contraseña proporcionada coincide con la establecida en la lista de usuarios de Samba, específicamente en el fichero /etc/smbusers; si esta autentificación inicial tiene éxito, el usuario no necesita volver a escribir la contraseña para acceder a este recurso.

Si se necesita que los usuarios tengan acceso a los recursos desde cualquier máquina cliente, se debe registrar las contraseñas tanto en la base de datos de cuentas tradicional (texto plano), como en la base de datos de contraseñas encriptados (smbpasswd).

De todas formas, es recomendable que se use siempre contraseñas encriptadas debido a que la seguridad de los recursos es el objetivo prioritario.

Gráfico 1.2: Modo de Seguridad a Nivel de Usuario



3.3 Modo de seguridad a nivel de dominio. -

La seguridad a nivel de dominio maneja dos tipos de entorno de red que son el entorno de red NT y el segundo en el cuál las máquinas trabajan autónomamente.

Dominio NT: en este tipo de entorno de red, todos los usuarios se autentifican con el servido PDC, los usuarios y contraseñas están guardados dentro de su base de datos, los usuarios se autentifican al acceder por primera vez al dominio durante cada sesión o cuando acceden desde otro terminal.

Autónomo: en este tipo de red, los usuarios son los encargados de administrar sus recursos, mediante la compartición de carpetas, "Con la seguridad a nivel de dominio, tenemos la opción de usar el mecanismo nativo de NT. Esto tiene una serie de ventajas:

1.- Proporciona una mejor integración con NT: hay menos 'arreglos' en las opciones del smb.conf referidas a los dominios que con la mayoría de las

posibilidades de Windows. Esto va a permitir utilizar de forma extensiva las opciones de administración de NT, como el Administrador de Usuarios para Dominios que permitirá a los usuarios individuales de los PC tratar los servidores Samba como si fueran grandes máquinas NT.

2.- Con la mejor integración vienen depuraciones del protocolo y del código, lo que permite al equipo Samba seguir con la evolución de la implementación NT. NT Service Pack 4 soluciona determinados problemas en el protocolo, y la mejor integración de Samba hace más fácil identificar y adaptarse a estos cambios.

3.- Hay una menor carga sobre el PDC porque hay una conexión permanente menos entre el y el servidor Samba. Independientemente del protocolo usado por la opción security = server, el servidor Samba puede hacer un Procedimiento de Llamada Remota (RPC) sólo cuando necesita información de autenticación. No necesita mantener una conexión permanente para esto.

4.- El procedimiento de autentificación de dominio en NT devuelve todos los atributos del usuario, no sólo si ha tenido o no éxito. Los atributos incluyen una lista larga y orientada a la red de los identificadores Unix, grupos NT, y mucha más información. Esto incluye:

- Nombre de usuario
- Nombre completo
- Descripción
- Identificador de seguridad (una extensión del identificador Unix orientada al dominio)
- Pertenencia a grupos NT
- Horas de entrada, y en su caso si hay que forzar al usuario a salir inmediatamente.
- Puestos de red que el usuario esta autorizado a utilizar
- Fecha de expiración de la cuenta
- Directorio personal
- Secuencia de entrada

- Perfil
- Tipo de cuenta

Los desarrolladores de Samba utilizaron seguridad a nivel de dominio en Samba versión 2.0.4 para permitirle añadir y eliminar usuarios del dominio de forma semiautomática. Además, añadió soporte para otras prestaciones al estilo NT, como soportar listas de control de acceso y cambiar los permisos de los ficheros desde el cliente. “

Fuente:http://es.tldp.org/Manuales-LuCAS/USANDO-SAMBA/usando-samba-html/node214.html

Con esta posibilidad se tiene sólo una base de datos de autenticación es por eso que la sincronización entre usuarios del dominio y la lista de usuarios del servidor Samba se vuelve mas sencilla.

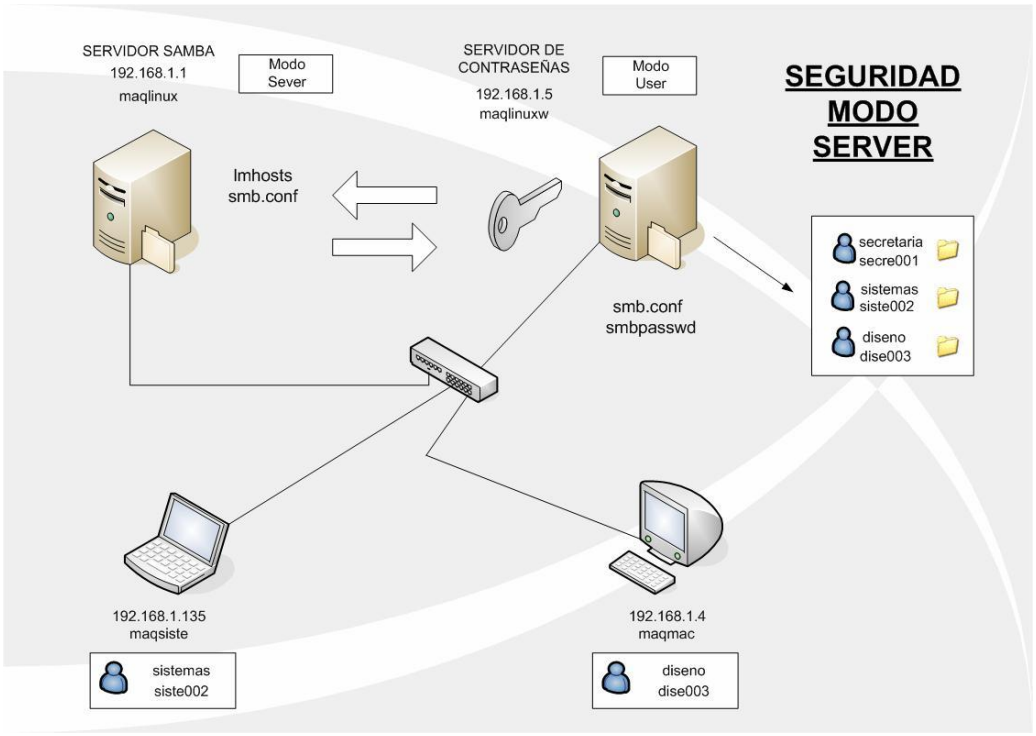
3.4 Modo de seguridad a nivel de servidor. -

La seguridad a nivel de servidor, es semejante que la seguridad a nivel de usuario, con la única diferencia de que Samba delega la autentificación de usuarios y contraseñas ha otro servidor, pudiendo ser este, otro servidor samba o Windows NT que actué como PDC (controlador principal de dominio).

Samba, en este caso seguirá manteniendo su listado de configuraciones y recursos en su principal archivo smb.conf.

El procedimiento es el siguiente, cuando un cliente intenta acceder a un determinado recurso samba, se valida este cliente en su archivo de configuración (smb.conf), y luego valida la contraseña ingresada conectando con su servidor Samba mediante la lista de usuarios del mismos o NT mediante usuarios de Active Directory, si la contraseña es aceptada, la conexión será establecida con el cliente, como se indica en el gráfico 3.

Gráfico 1.3: Modo de seguridad a nivel de Servidor



Este modo es muy aconsejable ya que permite tener separados los recursos compartidos de los ficheros de configuración, garantizando que ningún usuario pueda acceder ni siquiera en forma de lectura al servidor de contraseñas.

La opción para configurar Samba en un servidor distinto para validar las contraseñas es la siguiente:

```
[global]
        Security = Server
        Password Server =  maqlinuxw, maqlinuxw1
```

Como podemos ver en el ejemplo se puede configurar mas de un servidor a la ves, entonces Samba irá validando de acuerdo a la lista de servidores, pero cabe recalcar que si uno de los servidores rechaza la contraseña, se denegará el acceso inmediatamente y samba no seguirá validando en los demás servidores, el servidor de password deberá estar en modo user, para que pueda comprobar la autentificación de los usuarios, se debe tener en cuenta que los nombres de los servidores son nombre NetBios, los mismos que se enlazan con la dirección IP especificada en el archivo /etc/samba/lmhosts.

Conclusiones. – La seguridad en cualquier ámbito, es un tema al que se le debe dar la importancia que merece, mas aun cuando está de por medio información útil para las actividades vitales en una empresa; es por esto que concluimos que, la seguridad en un entorno de trabajo es el primer punto a implementar, el modo de seguridad a usar queda exclusivamente a criterio de las personas encargadas de sistemas, pero podemos recomendar que el modo que nos pareció el mas seguro es el modo de seguridad a nivel de servidor, por las razones en las que el servidor de contraseñas, que sería el que necesita mayor protección, no es accesible por ningún motivo a ningún usuario en la red(si así se lo requiere), mientras que los demás modos al contener los recursos y las contraseñas en uno mismo es mas expuesto a ataques.

Capítulo 4

Contraseñas encriptadas

Objetivo.- Las contraseñas en Samba, pueden ser el problema de varios administradores de red que están operando este tipo de servidor, debido a que estas pueden ser encriptadas o no encriptadas. Las contraseñas de clientes individuales que utilizan el sistema operativo Windows XP son encriptadas y desde luego más seguras debido a que no son propensas a ser leídas por programas de lectura de paquetes (sniffer), las contraseñas no encriptadas recorren la red en un archivo plano, siendo accesible para cualquier persona malintencionada.

La siguiente tabla nos indican que sistemas operativos encriptan las contraseñas antes de enviarlas al controlador primario de dominio para su autenticación:

Cuadro 1.2: Sistemas Operativos Windows con Contraseñas Encriptadas.

Sistema Operativo	**Encriptado o No-Encriptado**
Windows 95	No-Encriptado
Windows 95 con la Actualización SMB	Encriptado
Windows 98 Windows NT 3.x	Encriptado No-Encriptado
Windows NT 4 anterior al SP3	No-Encriptado
Windows NT 4 después del SP3	Encriptado

Fuente:http://es.tldp.org/Manuales-LuCAS/USANDO-SAMBA/usando-samba-html/node216.html

Para la encriptación de las contraseñas existen dos sistemas, uno para clientes Windows 95 y 98 que utiliza el estilo de Microsoft LAN Manager y otro distinto para Windows NT clientes y servidores, estos utilizan un sistema nuevo.

4.1 Configuración de contraseñas encriptadas en Samba. –

Samba almacena las contraseñas en el fichero /etc/samba/smbpasswd, a la vez que los usuarios hacen lo mismo en su máquina terminal, la versión que se almacena en la máquina terminal se realiza a través de un algoritmo el mismo que es notificado al servidor si se modifica o cambia, las contraseñas sin encriptar no se almacenan en ningún lugar ya que no se necesitan ser verificadas.

Para que Samba use contraseñas encriptadas, se configura el fichero smb.conf que se encuentra bajo la ruta /etc/samba/ de las siguiente manera:

```
[global]
 security = user
 encrypt passwords = yes
 smb passwd file = /etc/samba/smbpasswd
```

Pasos de conexión entre el cliente y el servidor Samba.-

"1. El cliente intenta negociar un protocolo con el servidor

2.El servidor responde con un protocolo e indica que soporta contraseñas encriptadas. En este momento; devuelve una cadena de 8 bytes generada aleatoriamente.

3. El cliente utiliza esta cadena como una llave para encriptar la ya encriptada contraseña usando un algoritmo predefinido por el protocolo negociado. Entonces envía el resultado al servidor.

4. El servidor realiza el mismo proceso con la contraseña almacenada en su propia base de datos. Si los resultados coinciden, las contraseñas y el usuario es autenticado".

Fuente:http://es.tldp.org/Manuales-LuCAS/USANDO-SAMBA/usando-samba-html/node218.html

4.2 El fichero smbpasswd.-

El fichero smbpasswd es el que va a contener todas las contraseñas de la lista de usuarios del servidor Samba, este fichero debe ser cuidado celosamente, de manera que solo el usuario root tenga derechos de escritura y lectura, los demás usuarios no deberán poder ingresar ni siquiera al directorio donde esta ubicado.

Para usar las contraseñas encriptadas, se deberá crear como primer paso al usuario en la lista de Samba o sea que el usuario deberá estar registrado en el fichero smbpasswd.

Cuadro 1.3: Contraseñas Encriptadas.

Fuente:http://es.tldp.org/Manuales-LuCAS/USANDO-SAMBA/usando-samba-html/node218.html

"Detalle de los campos:

Username (Nombre de usuario).

Este es el nombre de usuario de la cuenta. Se toma directamente del fichero de contraseñas del sistema.

UID.

Es el ID Unix del usuario. Como el nombre de usuario, se toma directamente del fichero de contraseñas del sistema y debe coincidir con el usuario que representa en este.

Información sobre la contraseña LAN Manager.

Es una secuencia hexadecimal de 32 bits que representa la contraseña que utilizaran los clientes Windows 95 y Windows 98.

Si no hay contraseña para el usuario, los primeros 11 caracteres consistirán en la secuencia NO PASSWORD seguida por tantas X como sea necesario. Todo el mundo puede acceder a un recurso que no tenga establecida una contraseña. Por otro lado, si la contraseña ha sido desactivada, consistirá en 32 caracteres X. Samba no dará acceso a ningún usuario a menos que se establezca la opción null passwords.

Información sobre la contraseña NT.

Es una secuencia hexadecimal de 32 bits que representa la contraseña que utilizarán los clientes NT.

Datos de la cuenta.

Este campo consiste en 11 caracteres entre 2 corchetes ([]). Cualquiera de los siguientes caracteres puede aparecer en cualquier orden, el resto serán espacios:

U Esta cuenta es una cuenta de usuario estándar de Unix.

D Esta cuenta está desactivada y Samba no permitirá ningún acceso.

N Esta cuenta no tiene contraseña asociada

W Esta es una cuenta de confianza que puede ser utilizada para configurar Samba como Controlador Primario de Dominio (PDC) cuando se permita a equipos Windows NT unirse a su dominio.

Hora del último cambio.

Este código consiste en los caracteres LCT seguido por la representación hexadecimal del número de segundos transcurridos desde el inicio de los tiempos (medianoche del 1 de Enero de 1970 en tiempo Unix) hasta que se modificó el fichero por última vez “.

Fuente:http://es.tldp.org/Manuales-LuCAS/USANDO-SAMBA/usando-samba-html/node218.html

4.3 Añadiendo entradas a smbpasswd. –

Para añadir las distintas contraseñas en el fichero smbpasswd, usamos el siguiente comando:

smbpasswd –a maqlinux

se debe mencionar que el usuario “maqlinux” debe estar creado en la lista de usuarios de samba de la siguiente manera:

useradd –s /sbin/nologin/ maqlinux

Hay una forma de crear la contraseña manualmente, editando el archivo smbpasswd de la sisguiente manera:

maqlinuc:500:XXXXXXXXXXXXXXXXXXXXXXXXXXXX:XXXXXXX
XXXXXXXXXXXXXXXXXXXX:[U]:LCT-00000000:

Anexo 1.5. - Opciones de Configuración de las Contraseñas.

4.4 Conclusiones. – Las contraseñas en servidores Samba es un tema muy importante, ya que estas sirven para autentificar usuarios que deseen acceder a recursos compartidos, las contraseñas deben estar protegidas para evitar cualquier plagio, estas deben ser manipuladas únicamente por el usuario "root", es decir el fichero smbpasswd tiene que tener permisos 600, a mas de tener en cuenta el modo de encripción, ya que este depende del sistema operativo en el que trabajen los diferentes terminales.

Capítulo 5

Aplicación Práctica

Objetivo.- Todo lo expuesto en los capítulos anteriores se aplicará de manera práctica, nos basaremos específicamente para la demostración en el archivo smb.conf, que varía con cada modo de seguridad, a más de la creación de hosts y usuarios requeridos para cada uno de los niveles, esta aplicación tiene como objetivo comprobar lo estudiado tomando en cuenta que algunas de las características varían con cada versión del sistema operativo Linux y del servidor Samba.

5.1 Recursos de hardware y software. -

51.1 Equipos:

1. Servidor Samba
   Descripción: "maqlinux"
   Pentium 4 Intel 2.0 Ghz
   Disco 60 Gigas
   Memoria RAM 512 mgbytes
   Sistema Operativo: Linux CentOS 4.2
   Observaciones: Disco particionado
   30 gigas NTFS
   30 gigas EXT3 (Linux CentOS)
2. Terminal Usuario1
   Descripción: "maqsecre"
   Procesador: Pentium 4 Intel 1.7 Ghz
   Disco duro: 60 Gigas
   Memoria RAM: 256 mgbytes
   Sistema Operativo: Windows XP SP2
   Observaciones: Disco particionado
   45 gigas NTFS
   15 gigas EXT3 (Linux CentOS)
3. Terminal Usuario2
   Descripción: "maqsiste"
   Procesador: Celeron Intel 1.5 Ghz
   Disco duro: 20 Gigas
   Memoria RAM: 256 mgbytes

Sistema Operativo: Windows XP SP2

4. Terminal EMac
   Descripción: “maqmac”
   Procesado: G4
   Disco duro: 40 Gigas
   Memoria RAM: 512 mgbytes
   Sistema Operativo: Mac Osx version 10.3 PANTER

51.2 Entorno de Red:

Topología de red: Estrella
Switch:
Marca: EDIMAX
Fast Ethernet 10/100
Cable:
UTP categoría 5 E

5.2 Pasos de Configuración. -

5.2.1 Creación de cuentas de usuario. - se deberá crear todas las cuentas de usuario que ocuparán los recursos del servidor Samba.

Ejemplo:
Useradd –s /sbin/nologin secretaria
Sistemas
Diseno

5.2.2 Configuración de password de usuarios samba. - se deberá configurar los passwords de cada usuario, el que deberá ser el mismo que en la máquina terminal en este caso las máquinas Windows, cabe recordar que estos passwords no son válidos para uso del servidor Linux sino únicamente para los recursos de samba, con esto queremos decir que dichos usuarios no podrán acceder al interprete de instrucciones.

Ubicación del fichero: /etc/samba/smbpasswd

Ejemplo:

Smbpasswd –a secretaria

New Smb password: secre001

Retype Smb password: secre001

5.2.3 Configuración del fichero lmhosts. - el paso siguiente es configurar el archivo de hosts, este se usa para relacionar los nombre netbios a una determinada dirección

ip, que luego nos servirá para dar o denegar acceso a ciertos terminales; el nombre deberá ser máximo de 11 caracteres.

Ubicación del fichero: /etc/samba/lmhost

Editamos el fichero con vi o con gedit y añadimos los nombres netbios:

127.0.0.1 localhost

192.168.1.1	maqlinux
192.168.1.2	maqsecre
192.168.1.135	maqsiste
192.168.1.4	maqmac

5.2.4 Configuración del fichero smb.conf. - el fichero smbconf es donde se especificará el modo de seguridad que utilizaremos, a más de las diferentes posibilidades que tendrán los usuarios para administrar los recursos.

5.2.4.1 Fichero smb.conf para seguridad a nivel de recurso compartido. -

La seguridad a nivel de recurso compartido se implementa de la siguiente manera.

```
[global]
#Especificamos el modo de seguridad "share"
  security = share


**********************************************************
#COMPARTIENDO CARPETAS
**********************************************************
#ADMINISTRADORES
**********************************************************
#Sólo el usuario secretaria puede acceder a esta carpeta,
#tiene permisos administrativos. Es decir funciona como Super Usuario.
#Gestiona los recursos compartidos.
[secretaria]
path = /Archivos/secretaria
guest ok = no
read only = no
username = secretaria
valid users = secretaria
directory mask = 0755
create mask = 0644
comment = Administrador máquina secretaria
```

#Sólo el usuario sistemas puede acceder a esta carpeta,
#tiene permisos administrativos. Es decir funciona como Super Usuario.
#Gestiona los recursos compartidos.
[sistemas]
path = /Archivos/sistemas
guest ok = no
read only = no
username = sistemas
valid users = sistemas
directory mask = 0755
create mask = 0644
comment = Administrador máquina sistemas

#Sólo el usuario diseño puede acceder a esta carpeta,
#tiene permisos administrativos. Es decir funciona como Super Usuario.
#Gestiona los recursos compartidos.
[diseno]
path = /Archivos/diseno
guest ok = no
read only = no
username = diseno
valid users = diseno
directory mask = 0755
create mask = 0644
comment = Administrador máquina secretaria

****
#LECTURA
****
#Permisos de sólo lectura para todos los usuarios
[lectura]
path = /Archivos/carpeta0/
guest ok = no
read only = yes
username = secretaria, sistemas, diseno
comment = Lectura todos usuarios

****
#ESCRITURA-LECTURA
****
#Permisos de escritura - lectura para todos los usuarios
[escritura]
path = /Archivos/carpeta1
guest ok = no
read only = no
username = secretaria, sistemas, diseno
directory mask = 0755

create mask = 0644
comment = Lectura-Escritura todos usuarios

;directory mask = 0755
;create mask = 0644

****
#VALIDEZ USUARIOS PARA LECTURA
****
#valido sólo para secretaria y sistemas lectura
[secre-sist]
path = /Archivos/carpeta2
guest ok = no
read only = yes
username = secretaria,sistemas
valid users = secretaria,sistemas
directory mask = 0755
create mask = 0644
comment = acceso sólo secretaria y sistemas como lectura

****
#VALIDEZ USUARIOS PARA ESCRITURA
****
#valido sólo para sistemas y diseno escritura
[siste-dise]
path = /Archivos/carpeta3
guest ok = no
read only = no
username = sistemas,diseno
valid users = sistemas,diseno
directory mask = 0755
create mask = 0644
comment = acceso sólo sistemas y diseno como escritura

****
#PERMISOS DE ESCRITURA Y LECTURA
****
#secretaria puede escribir, sistemas y diseno sólo lectura
[opcion1]
path = /Archivos/secretaria
guest ok = no
read only = no
username = secretaria
valid users = secretaria
directory mask = 0755

create mask = 0644
comment = Escritura secretaria - Lectura sistemas y diseño

[opcion1 inv]
path = /Archivos/secretaria
guest ok = no
read only = yes
username = diseno,sistemas
valid users = diseno,sistemas
directory mask = 0755
create mask = 0644
comment = Escritura secretaria - Lectura sistemas y diseño

****
#sistemas puede escribir, secretaria y diseno sólo lectura
[opcion2]
path = /Archivos/carpeta5
guest ok = no
read only = no
username = sistemas
valid users = sistemas
directory mask = 0755
create mask = 0644
comment = Escritura sistemas - Lectura secretaria y diseño

[opcion2 inv]
path = /Archivos/carpeta5
guest ok = no
read only = yes
username = secretaria, diseno
valis users = secretaria,diseno
directory mask = 0755
create mask = 0644
comment = Escritura sistemas - Lectura secretaria y diseño

****
#diseno puede escribir, sistemas y secretaria sólo lectura
[opcion3]
path = /Archivos/carpeta6
guest ok = no
read only = no
username = diseno
valid users = diseno
directory mask = 0755
create mask = 0644
comment = Escritura diseno - Lectura secretaria y sistemas

[opcion3 inv]
path = /Archivos/carpeta6

```
guest ok = no
read only = yes
username = sistemas,secretaria
valid users = sistemas,secretaria
directory mask = 0755
create mask = 0644
comment = Escritura diseno - Lectura secretaria y sistemas


*****************************
#carpeta para invitados
[invitado]
path = /Archivos/carpeta7
reas only = no
public
guest account = secretaria
comment = Invitados


*****************************************************************
#DISPOSITIVOS
*****************************************************************
[cdrom]
path = /media/cdrom
comment = cdrom compartido
case sensitive = yes
*****************************
 [floppy]
path = /media/floppy
comment = floppy compartido
case sensitive = yes
*****************************
 [usb]
path = /media/UDISK_20X
comment = Pen drive compartido (USB)
case sensitive = yes
```

5.2.4.2 Fichero smb.conf para Seguridad a nivel de usuario. –

La seguridad a nivel de usuario se implementa de la siguiente manera:

```
[global]
  security = user

# Define el grupo de trabajo o dominio
workgroup = UDA

# Define el nombre del Server netbios
netbios name = maqlinux
```

```
# Especifica si puede tener passwords nulos
null passwords = yes

# Nombre de Servidor para mostrar en el entorno de red
server string = Samba Server Tesis UDA

# Host a los que se permite el acceso
hosts allow = 192.168.1. 127.

# Host a los que se deniega el acceso
# hosts deny  = 192.168.1.4

# Permite leer automáticamente la lista de impresoras
printcap name = /etc/printcap

# Indica el fichero de log.files para los usuarios que accedan a samba
log file = /var/log/samba/%m.log

# Tamaño máximo
max log size = 50

# Permite configura múltiples interfaces de red
;   interfaces = 192.168.12.2/24 192.168.13.2/24

winbind uid = 16777216-33554431
winbind gid = 16777216-33554431


# NOTE: If you have a BSD-style print system there is no need to
# specifically define each individual printer


[printers]
comment = All Printers
path = /var/spool/samba
browseable = no
# Set public = yes to allow user 'guest account' to print
printable = yes
vfs objects = /usr/lib/samba/vfs/vasambavfsemu.so


**********************************************************
#COMPARTIENDO CARPETAS
#**********************************************************
#ADMINISTRADORES
#**********************************************************
#Sólo el usuario secretaria puede acceder a esta carpeta,
#tiene permisos administrativos. Es decir funciona como Super Usuario.
#Gestiona los recursos compartidos.
```

[secretaria]
read only = no
admin users = secretaria
path = /Archivos/secretaria
comment = Administrador máquina secretaria
valid users = secretaria
case sensitive = yes

#Sólo el sistemas puede acceder a esta carpeta,
#tiene permisos administrativos. Es decir funciona como Super Usuario.
#Gestiona los recursos compartidos.
[sistemas]
read only = no
admin users = sistemas
path = /Archivos/sistemas
comment = Administrador máquina sistemas
valid users = sistemas
case sensitive = yes
#Sólo el usuario diseño puede acceder a esta carpeta,
#tiene permisos administrativos. Es decir funciona como Super Usuario.
#Gestiona los recursos compartidos.
[diseno]
read only = no
admin users = diseno
path = /Archivos/diseno
comment = Administrador diseño
valid users = diseno
case sensitive = yes

#**
#LECTURA
#**
#Permisos de sólo lectura para todos los usuarios
[lectura]
path = /Archivos/carpeta0/
case sensitive = yes
comment = Lectura todos usuarios
guest account = nobody
browseable = yes
#**
#ESCRITURA-LECTURA
#**
#Permisos de escritura - lectura para todos los usuarios
[escritura]
path = /Archivos/carpeta1
directory mask = 0777
create mask = 0777
read only = no
case sensitive = yes

comment = escritura todos usuarios

#***
#VALIDEZ USUARIOS PARA LECTURA
#***
#valido sólo para secretaria y sistemas lectura
[secre-sist]
path = /Archivos/carpeta2
case sensitive = yes
valid users = secretaria,sistemas
comment = acceso sólo secretaria y sistemas como lectura

#***
#VALIDEZ USUARIOS PARA ESCRITURA
#***
#valido sólo para sistemas y diseno escritura
[siste-dise]
path = /Archivos/carpeta3
read only = no
case sensitive = yes
valid users = sistemas,diseno
comment = acceso sólo sistemas y diseno como escritura
#***
#PERMISOS DE ESCRITURA Y LECTURA
#***
#secretaria puede escribir, sistemas y diseno sólo lectura
[opcion1]
path = /Archivos/carpeta4
write list = secretaria
case sensitive = yes
comment = Escritura secretaria - Lectura sistemas y diseño
valid users = secretaria,sistemas,diseno

#sistemas puede escribir, secretaria y diseno sólo lectura
[opcion2]
path = /Archivos/carpeta5
write list = sistemas
case sensitive = yes
comment = Escritura sistemas - Lectura secretaria y diseño
valid users = secretaria,sistemas,diseno

#sistemas puede escribir, secretaria y diseno sólo lectura
[opcion3]
path = /Archivos/carpeta6
write list = diseno
case sensitive = yes
comment = Escritura diseno - Lectura secretaria y sistemas
valid users = secretaria,sistemas,diseno

```
#carpeta para invitados
[invitado]
path = /Archivos/carpeta7
case sensitive = no
comment = Invitados
public = yes
guest ok = yes
guest account = Invitado


#============================================================
#DISPOSITIVOS
#============================================================
[cdrom]
path = /media/cdrom
comment = cdrom compartido
case sensitive = yes
#============================================================
[floppy]
path = /media/floppy
comment = floppy compartido
case sensitive = yes
#============================================================
[usb]
path = /media/UDISK_20X
comment = Pen drive compartido (USB)
case sensitive = yes
```

5.2.4.3 Fichero smb.conf para Modo Seguridad a nivel de servidor. -

Para la seguridad a nivel de servidor necesitaremos especificar dos servidores, el primero para que sea el servidor Samba, configurado con todos los recursos a compartir y el segundo que será el servidor donde se validarán las contraseñas, para el ejemplo se usará otro servidor samba.

Smb.conf del servidor Samba "maqlinux"

```
# La única diferencia con el modo share esta en las siguientes líneas de la sección
global.

#Especificamos el modo de seguridad "share"
[global]
security = server

#Especificamos el Server password en donde se validarán las claves
 password server = maqlinuxw
```

Nota: la sección [printers] y [homes] no se modifican.

Smb.conf del servidor de passwords "maqlinuxw"

La única diferencia con el modo share esta en las siguientes líneas de la sección global

#Especificamos el modo de seguridad "user", debido a que el servidor Samba manda los nombres hacia este servidor para que lo valide

[global]

security = user

5.3 Conclusiones. – los diferente niveles de seguridad tienen características especificas de cada uno, con esto podemos obtener una administración flexible para cualquiera que fuere la necesidad, es básico escoger el modo que usaremos, esto dependerá de los usuarios que accedan a los recursos y su diferentes necesidades, como podemos observar el método manual para la configuración del servidor Samba, es de fácil implementación, o nos podemos ayudar con cualquiera de las herramientas gráficas que han sido desarrolladas, teniendo como base el conocimiento de cada párrafo del archivo de configuraciones, y de la creación de usuarios y hosts.

ANEXOS

Anexo 1.1: Roles de Samba (desde 2.0.4b).

Rol	**¿Puede hacerlo?**
Servidor de Archivos	Sí
Servidor de Impresión	Sí
Controlador Primario de Dominio	Sí (Samba 2.1 o superior recomendado)
Controlador de Dominio de Seguridad	No
Autentificación de clientes Windows 95/98	Sí
Visualizador Maestro Local	Sí
Visualizador de Seguridad	No
Visualizador Maestro de Dominio	Sí
Servidor WINS Primario	Sí
Servidor WINS Secundario	No

Fuente: http://es.tldp.org/Manuales-LuCAS/USANDO-SAMBA/usando-samba-html

Anexo 1.2.- Principales opciones de la sección [global] de Samba

Opción	Significado	Valor por defecto
netbios name	Nombre (NetBIOS) del ordenador Samba.	Primer componente del nombre DNS del ordenador.
workgroup	Nombre del dominio (o grupo de trabajo) al que pertenece Samba.	Nulo
security	Nivel de seguridad (share, user, server, domain).	User
encrypt passwords	Utilizar contraseñas cifradas de Windows (en modo domain, sí deben utilizarse).	No
password server	Ordenador Windows utilizado para la autentificación. En modo domain, debe ser una lista de los DCs del dominio.	Nulo
map to guest	Establece en qué condiciones un acceso a Samba debe considerarse en modo invitado (en el nivel domain, este parámetro afecta sólo cuando el acceso no ha sido acreditado por el DC del dominio).	Mever
log level	Nivel de detalle en la auditoría de Samba. Es un número que indica la cantidad de información a auditar. A mayor valor, más cantidad de información.	Se establece en el script que inicia el servicio Samba.
log file	Nombre del fichero donde se almacenan mensajes de auditoría de Samba.	Se establece en el script que inicia el servicio Samba.

Fuente: http://groucho.dsic.upv.es/cursos/Integracion/html/ch04s08.html

Anexo 1.3.- Principales opciones de los recursos en Samba

Opción	Significado	Valor por defecto
read only ({yes/no})	Recurso exportado como sólo lectura.	Yes
browseable ({yes/no})	El servicio aparece en la lista de recursos compartidos al explorar el ordenador Samba desde el Entorno de Red Windows.	Yes
Path	Ruta absoluta al directorio compartido por el recurso.	Nulo
comment	Descripción del servicio (cadena de caracteres).	Nulo
guest ok ({yes/no})	Permitir accesos como invitado al recurso.	No
guest account	Si un acceso se realiza como invitado, se utiliza el usuario indicado para representar la conexión.	Nobody
guest only ({yes/no})	Todos los accesos se aceptan en modo invitado.	No
Copy	Duplica otro recurso existente.	Nulo
force user	Los accesos al recurso se realizan como si el usuario que accede es el usuario indicado.	nulo (se utiliza el mismo usuario que ha realizado la conexión
force group	Los accesos al recurso se realizan como si el usuario que accede pertenece al grupo indicado.	Nulo (se utiliza el grupo primario del usuario que ha realizado la conexión).
hosts allow	Lista ordenadores desde los que se permite acceder al recurso	Lista vacía (i.e., todos los ordenadores).
hosts deny	Lista ordenadores desde los que no se permite acceder al recurso. En caso de conflicto, prevalece lo indicado en hosts allow.	Lista vacía (ningún ordenador).
valid users	Define que usuarios o grupos pueden acceder. Los valores pueden ser nombres de usuarios separados por comas o bien nombres de grupo antecedidos por una @. Ejemplo: usuario1, usuario2, @usuario3	Lista vacía (i.e., todos los usuarios).
follow symlinks ({yes/no})	Permitir el seguimiento de los enlaces simbólicos que contenga el recurso.	Yes
Writable	Define si ser permitirá la escritura. Es el parámetro contrario de read only. El valor puede ser Yes o No. Ejemplos: «writable = Yes» es lo mismo que «read only = No». Obviamente «writable = No» es lo mismo que «read only = Yes»	No
Write list	Define que usuarios o grupos pueden acceder con permiso de escritura. Los valores pueden ser nombres de usuarios separados por comas o bien nombres de grupo antecedidos por una @. Ejemplo: usuario1, usuario2, @usuario3	Se debe definir
Admin. users	Define que usuarios o grupos pueden acceder con permisos administrativos para el recurso. Podrán acceder hacia el recurso realizando todas las operaciones como súper-usuarios. Los valores pueden ser nombres de usuarios separados por comas o bien nombres de grupo antecedidos por una @. Ejemplo: @usuario1, @usuario2.	Se debe definir

Fuente: http://groucho.dsic.upv.es/cursos/Integracion/html/ch04s09.html

Anexo 1.4. - Opciones de seguridad a nivel de recurso.

Opción	Parámetros	Función	Valor por defecto	Ámbito
only user	Booleano	Indica cuando los nombres de usuario especificados por username serán los únicos permitidos.	No	Recurso
Username	Cadena (lista de usuarios)	Especifica una lista de usuarios contra los que se comprobará la validez de la contraseña.	Ninguno	Recurso

Fuente: http://es.tldp.org/Manuales-LuCAS/USANDO-SAMBA/usando-samba-html/node209.html

Anexo 1.5. - Opciones de Configuración de las Contraseñas.

Opción	Parámetros	**Función**	**Valor por defecto**	**Ámbito**
encrypt passwords	Lógico	Activa las contraseñas encriptadas.	No	Global
Unix password sync	Lógico	Si su valor es yes, Samba actualiza las contraseñas estándar de Unix cuando un usuario cambia su contraseña encintada.	no	Global
passwd chat	Carácter (instrucciones del "chat")	Establece la secuencia de instrucciones que se enviará al programa de contraseñas.	Mira la sección anterior en este capítulo	Global
passwd chat debug	Lógico	Envía la depuración del proceso de cambio de contraseñas a los ficheros de registro con una profundidad de 100	no	Global
passwd program	Carácter (instrucciones Unix)	Establece el programa a usar para cambiar las contraseñas.	/bin/passwd %u	Global
password level	Numérico	Establece el numero de permutaciones con letras mayúsculas que se usarán al comprobar una contraseña.	None	Global
update encrypted	Lógico	Si su valor es yes, Samba actualizará la contraseña encriptada cuando un usuario se conecte con una contraseña de texto plano.	no	Global
Null passwords	Lógico	Si su valor es yes, Samba permitirá el acceso a usuarios con contraseñas nulas.	no	Global
Smb passwd file	Carácter (Ruta completa al fichero)	Especifica el nombre del fichero de contraseñas encriptadas.	/usr/local/samba /private /smbpasswd	Global

Fuente: http://es.tldp.org/Manuales-LuCAS/USANDO-SAMBA/usando-samba-html/node222.html

Bibliografía:

BANDEL, David y NAPIER Robert, Edicion Especial Linux 6ta edición, 6th ed., Vol 1, PEARSON EDUCACION, Madrid, 2001, Cap 29 "Compartición de Recursos con Samba".

ARENA, Hector Facundo, La Biblia de Linux, 1th ed, Vol 1, MP Ediciones, Ciudad de Buenos Aires, Argentina, 2002,Cap 11 Interconexión en red con Windows

Fuente:http://es.tldp.org/Manuales-LuCAS/USANDO-SAMBA/usando-samba-html/node3.html

Fuente.- http://bulma.net/body.phtml?nIdNoticia=615

Fuente:http://es.tldp.org/Manuales-LuCAS/USANDO-SAMBA/usando-samba-html/node214.html

Fuente:http://es.tldp.org/Manuales-LuCAS/USANDO-SAMBA/usando-samba-html/node216.html

Fuente:http://es.tldp.org/Manuales-LuCAS/USANDO-SAMBA/usando-samba-html/node218.html

Fuente: http://es.tldp.org/Manuales-LuCAS/USANDO-SAMBA/usando-samba-html

Fuente: http://groucho.dsic.upv.es/cursos/Integracion/html/ch04s08.html

Fuente: http://groucho.dsic.upv.es/cursos/Integracion/html/ch04s09.html

Fuente: http://es.tldp.org/Manuales-LuCAS/USANDO-SAMBA/usando-samba-html/node209.html

Fuente: http://es.tldp.org/Manuales-LuCAS/USANDO-SAMBA/usando-samba-html/node222.html