Seguridad Informatica I

Ciclo 2023-2024

Trabajo Final

Alumnos: **Gaston Fenske**
Lucas Galdame Villegas
Santiago Moyano
Danilo Cerna Verardo
Enzo Fernandez
Ezequiel Garcia

Profesor: **Lic. Gabriel Arenas**

Informe

En este informe detallaremos como realizaremos nuestro sistema para la materia de Seguridad Informatica I.

Utilizaremos Samba y OpenLDAP.

Samba es una implementación libre y gratuita del protocolo de compartición de archivos de Microsoft Windows, conocido como SMB (Server Message Block). Con Samba, un sistema Linux o Unix puede compartir archivos e impresoras con clientes Windows, y viceversa.

Samba fue desarrollado inicialmente para proporcionar servicios de interconexión entre sistemas Unix/Linux y Windows. Proporciona un conjunto de servicios que permiten a los usuarios acceder a archivos e impresoras compartidos en una red, independientemente del sistema operativo utilizado.

Estos servicios incluyen:

- Servicio de nombres NetBIOS
- Servicio de autenticación
- Servicio de compartición de archivos e impresoras

Samba es muy utilizado en entornos empresariales y educativos, ya que permite la integración de sistemas Windows y Linux/Unix de manera transparente. Además, Samba es muy flexible y configurable, lo que permite adaptarlo a diferentes necesidades y requisitos de seguridad.

OpenLDAP es una implementación libre y gratuita del protocolo de directorio LDAP (Lightweight Directory Access Protocol). Es un software de servidor de directorio que permite acceder y gestionar información almacenada en un directorio LDAP.

Un directorio LDAP es una base de datos jerárquica que se utiliza para almacenar información de red, como nombres de usuario, contraseñas, direcciones de correo electrónico, direcciones IP, grupos y otros datos de configuración de red. El protocolo LDAP se utiliza para acceder y administrar esta información en el directorio.

OpenLDAP se puede utilizar para implementar servicios de autenticación y autorización en una red, así como para la gestión de recursos y servicios. Entre las características más importantes de

OpenLDAP se encuentran:

- Alta disponibilidad y escalabilidad: OpenLDAP es capaz de gestionar grandes volúmenes de datos y de usuarios, y puede ser configurado para ser altamente disponible y tolerante a fallos.
- Seguridad: OpenLDAP incluye características de seguridad como el cifrado de datos, la autenticación y la autorización basadas en políticas de acceso.
- Interoperabilidad: OpenLDAP puede integrarse con otros sistemas y protocolos de directorio, y es compatible con diferentes plataformas de hardware y software.

OpenLDAP es utilizado en muchas organizaciones, tanto empresariales como educativas, para proporcionar servicios de autenticación, autorización y gestión de recursos en una red.

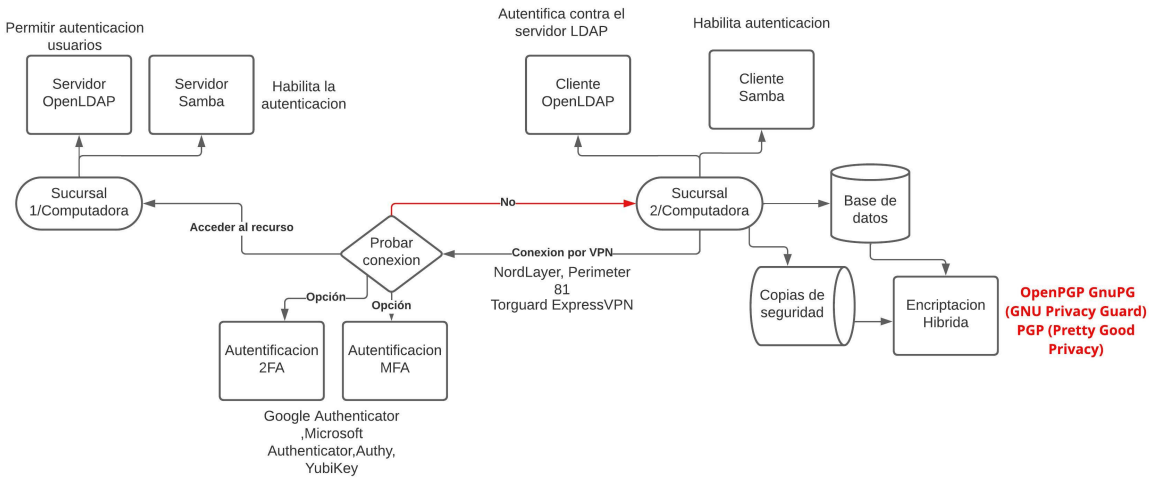
Samba y OpenLDAP son dos tecnologías diferentes pero complementarias. Ambas se utilizan para proporcionar servicios de autenticación y autorización en una red, y se pueden integrar para ofrecer una solución de directorio completa.

OpenLDAP se utiliza para almacenar y gestionar información de usuario y grupo en un directorio LDAP centralizado. Esta información incluye nombres de usuario, contraseñas, permisos de acceso y otra información de configuración de red. Samba, por otro lado, se utiliza para compartir recursos, como archivos e impresoras, en una red de usuarios que utilizan clientes Windows.

Cuando se integran, Samba y OpenLDAP permiten a los usuarios acceder a los recursos compartidos en la red utilizando sus credenciales de usuario almacenadas en el directorio LDAP. Esto significa que los usuarios pueden autenticarse una sola vez en la red y tener acceso a todos los recursos compartidos en la red, sin tener que autenticarse de nuevo para cada recurso.

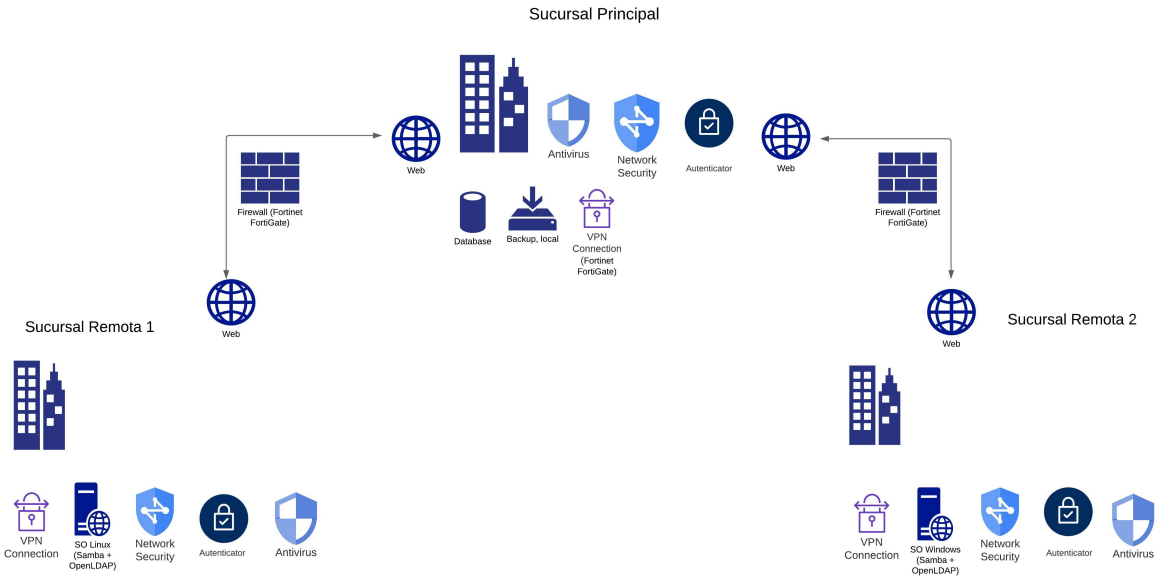
La integración de Samba y OpenLDAP también permite una gestión centralizada de los recursos compartidos y las políticas de acceso en la red. Los administradores de la red pueden configurar políticas de acceso y permisos de usuario en el directorio LDAP, y Samba utiliza esta información para controlar el acceso a los recursos compartidos.

En resumen, la integración de Samba y OpenLDAP permite una gestión centralizada y unificada de la autenticación, la autorización y el acceso a los recursos compartidos en una red, lo que aumenta la seguridad y la eficiencia de la gestión de la red.



Uso

En este diagrama, se detalla de las tecnologías a utilizarse.



En la sucursal principal, encontraremos el servidor físico donde se alojara nuestro sistema, el cual utilizara Samba y OpenLDAP.

Por seguridad, se hara un backup de manera semanal, para garantizar la integridad de la informacion del servidor y su contenido.

Cada sucursal tendra un red LAN, que se interconectaran con una VPN a traves de internet.

Usaremos como VPN Fortinet FortiGate, que nos sirve porque combina firewall, VPN y otras características de seguridad. El firewall restringira las paginas indeseadas.

Como autentificador usaremos el Autentifacador de Google, debido a su portabilidad y fiabilidad en sistemas como el que usaremos. Sera usado como método de seguridad para Samba y OpenLDAP.

Usaremos una base de datos no relacional por su escabilidad y descentralizacion. MongoDB: Es una base de datos de documentos que utiliza un formato de documento BSON. Es escalable, flexible y fácil de usar, lo que la convierte en una opción popular para una amplia gama de aplicaciones.

Codigo

```
import samba
import samba.samba_tool

# Configura el nombre del dominio
domain_name = "example.com"

# Configura el nombre del controlador de dominio
dc_name = "dc1"

# Configura el nombre de usuario del administrador
admin_username = "administrator"


# Configura la ruta del archivo de registro
log_file = "/path/to/log/file.log"

# Crea una función para registrar el inicio de sesión de un usuario
def log_login(username):
    with open(log_file, "a") as f:
        f.write("Usuario {} inició sesión.\n".format(username))

# Inicia el controlador de dominio
samba.samba_tool.main(["domain", "provision"])

# Registra el inicio de sesión de un usuario de ejemplo
log_login("usuario_de_ejemplo")
```

El código esta relacionado con la configuración y aprovisionamiento de un controlador de dominio Samba y el registro de eventos de inicio de sesión de usuarios.

Aquí hay algunos pasos y consejos a considerar:

El código importa el módulo “samba_tool”, que es una utilidad de línea de comandos que le permite administrar diferentes aspectos de un controlador de dominio Samba, incluidos usuarios, grupos, sitios, DNS y replicación.

El código establece algunas variables que definen el nombre de dominio, el nombre del controlador de dominio, el nombre de usuario del administrador y la ruta del archivo de registro. Estas variables se utilizan posteriormente para aprovisionar el controlador de dominio y registrar eventos de inicio de sesión.

El código define una función llamada “log_login” que toma un parámetro de nombre de usuario y agrega un mensaje al archivo de registro que indica que el usuario ha iniciado sesión. Esta función se llama con un nombre de usuario de ejemplo después de que se aprovisiona el controlador de dominio.

Para aprovisionar el controlador de dominio, el código llama a la función “samba_tool.main” con los argumentos "domain" y "provision". Este comando crea los archivos y directorios necesarios, configura el reino Kerberos y crea la cuenta de administrador de dominio predeterminada.

Para registrar el evento de inicio de sesión de un usuario, el código utiliza la función “open” para abrir el archivo de registro en modo de anexo, escribe un mensaje que indica que el usuario ha iniciado sesión y cierra el archivo. La declaración “with” se utiliza para garantizar que el archivo se cierre correctamente incluso si se produce una excepción.

Aquí hay algunos consejos y recursos adicionales que pueden ser útiles al trabajar con controladores de dominio Samba:

Para administrar controladores de dominio Samba desde la línea de comandos, puede utilizar la utilidad “samba_tool”. Esta herramienta proporciona una amplia gama de comandos y opciones para administrar usuarios, grupos, sitios, DNS y replicación. Puede utilizar el comando “samba-tool -h” para mostrar opciones y comandos.

Para agregar un nuevo usuario a un controlador de dominio Samba, puede utilizar el comando “samba-tool user add” seguido del nombre de usuario y cualquier opción adicional, como el nombre completo del usuario, e-mail y el shell de inicio de sesión.

También puede listar todos los usuarios existentes con el comando “samba-tool user list”, eliminar un usuario con el comando “samba-tool user delete”, restablecer la contraseña de un usuario con el comando “samba-tool user setpassword” y habilitar o deshabilitar una cuenta de usuario con los comandos samba-tool user enable o samba-tool user disable.

Para agregar atributos Unix a un usuario de Windows, puede utilizar los comandos “wbinfo” y “ldbedit”.

El comando “wbinfo --name-to-sid” recupera el identificador de seguridad (SID) para un nombre de usuario dado, mientras que el comando “wbinfo --sid-to-uid” recupera el identificador de usuario Unix (UID) para un SID dado.

Luego puede utilizar el comando “ldbedit” para agregar los atributos “uidNumber” y “gidNumber” al objeto del usuario en la base de datos LDAP de Samba. Esto permite que el usuario se conecte a un miembro del dominio Unix y use los ID Unix asignados.

Configuración

```
[global]
   workgroup = DOMAIN_NAME
   server role = active directory domain controller
   domain logons = yes
   logon path = \\%L\Profiles\%U
   logon drive = H:
   logon home = \\%L\%U
   domain logons = yes
   log file = /path/to/log/file.log
   log level = 1
```

El fragmento de código proporcionado muestra como seria una configuración del archivo de configuración global de Samba para un controlador de dominio activo de Active Directory. Aquí hay una descripción de las opciones de configuración:

*workgroup: Define el nombre del grupo de trabajo al que pertenece el controlador de dominio. En este caso, se utiliza el valor de la variable DOMAIN_NAME.

*server role: Define el papel del servidor Samba. En este caso, se establece como un controlador de dominio de Active Directory.

*domain logons: Habilita el inicio de sesión de los usuarios del dominio en el controlador de dominio. Esta opción debe estar configurada en "yes" para permitir que los usuarios inicien sesión en el dominio.

*logon path: Define la ubicación del perfil del usuario. En este caso, se utiliza la ruta \\%L\Profiles\%U, que indica que los perfiles de usuario se almacenan en una carpeta compartida llamada "Profiles" en el servidor Samba.

*logon drive: Define la letra de unidad asignada al disco de inicio de sesión del usuario. En este caso, se establece en "H:".

*logon home: Define la ubicación de la carpeta de inicio de sesión del usuario. En este caso, se utiliza la ruta \\%L\%U, que indica que la carpeta de inicio de sesión del usuario se encuentra en una carpeta compartida con el mismo nombre que el nombre de usuario en el servidor Samba.

*log file: Define la ubicación del archivo de registro de Samba. En este caso, se utiliza la ruta /path/to/log/file.log.

*log level: Define el nivel de detalle del registro de Samba. En este caso, se establece en "1", lo que significa que se registrarán mensajes de nivel "Informational" y superiores.

Aquí hay algunas fuentes adicionales que pueden ser útiles al trabajar con Samba y Active Directory:

Para verificar la autenticación en un controlador de dominio Samba, puede conectarse a la carpeta compartida "netlogon" utilizando la cuenta de administrador de dominio. Puede usar el comando “smbclient //localhost/netlogon -UAdministrator -c 'ls'” para listar los archivos en la carpeta compartida.

Para asignar permisos de archivo a usuarios y grupos de dominio en un controlador de dominio Samba, puede utilizar la biblioteca de conmutación de servicios de nombres (NSS). Por ejemplo, para establecer el propietario de un archivo en el usuario de dominio "demo01" y el grupo en el grupo de dominio "Domain Users", puede usar el comando “chown "SAMDOM\\demo01:SAMDOM\\domain users" file.txt”.

Para unirse a un dominio Samba desde un equipo con Windows, debe tener una versión compatible de Windows (por ejemplo, Windows 7 Professional o Ultimate para Windows 7). Puede unirse al dominio desde la configuración del sistema y proporcionar las credenciales de administrador de dominio cuando se le solicite.