

	UNIVERSIDAD AUTONOMA DE OCCIDENTE					
uao	FACULTAD DE INGENIERIA			NOMBRE DE LA ASIGNATURA	Servicios Telemáticos	
	CODIGO:		NOMBRE:			
					Valoración	
PRIMER PARCIAL					Septiembre 2 de 2025	

PRIMERA PARTE	(2.0 Puntos) Problema de Configuración de Autenticación PAM en Servidor Apache en Ubuntu 22.04	PUNTAJE	
---------------	--	---------	--

Suponga que administra un servidor web Apache que aloja contenido sensible en un directorio llamado "/archivos_privados". Su tarea es configurar la autenticación usando PAM (Pluggable Authentication Module) para asegurar que solo los usuarios del sistema autorizados puedan acceder a este directorio. Además, se requiere que los usuarios de una lista específica sean denegados el acceso a este directorio.

Pasos a seguir:

- Configure el archivo de configuración de Apache para el sitio correspondiente y especifique las reglas de acceso al directorio "archivos_privados".
- Utilice los módulos PAM adecuados para gestionar la autenticación. Asegúrese de que solo los usuarios del sistema puedan autenticarse exitosamente.
- Cree una lista de usuarios que deben ser denegados el acceso al directorio "archivos_privados". Esta lista debe almacenarse en un archivo separado.
- Configure la restricción de acceso para los usuarios de la lista creada en el paso anterior.
- Si durante el proceso de login, al intentar acceder al directorio el usuario presiona el botón cancelar, debe recibir un mensaje de error.
- Asegúrese de estar en la capacidad de explicar cómo se garantiza de que la autenticación se realice mediante PAM y cómo se aplica la denegación de acceso a la lista de usuarios.

Puntos a evaluar:

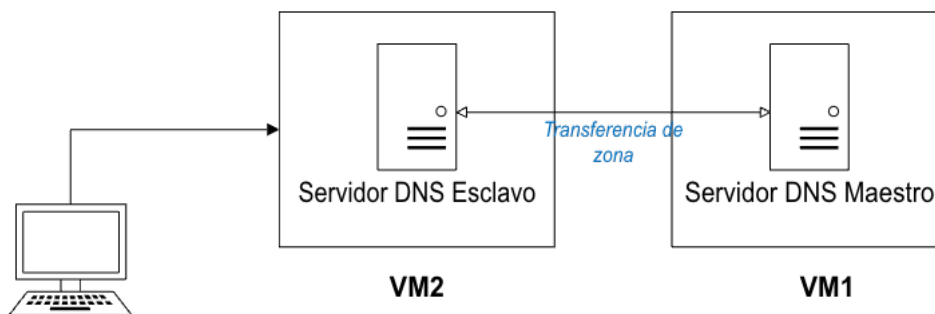
- Correcta configuración de Apache para el sitio y el directorio especificado.
- Uso adecuado de módulos PAM para gestionar la autenticación.
- Creación y aplicación de la lista de usuarios denegados.
- Explicación clara y concisa de los pasos realizados y las configuraciones implementadas.
- Capacidad para solucionar problemas relacionados con la configuración de autenticación y acceso.

Nota:

Este problema está diseñado para evaluar su comprensión de la configuración de autenticación PAM en un servidor Apache y su capacidad para aplicar restricciones de acceso específicas a usuarios del sistema. Asegúrese de proporcionar detalles completos en su respuesta y de demostrar su conocimiento en la configuración y administración de sistemas web y autenticación.

SEGUNDA PARTE	(2.0 Puntos) Servidores DNS Maestro/Esclavo con Transferencia de Zona y Resolución Inversa	PUNTAJE	
---------------	---	---------	--

Implemente una configuración de servidores DNS maestro y esclavo que permita la transferencia de zona y valide la correcta resolución de nombres y direcciones IP en un entorno simulado.



Requerimientos:

1. Instale y configure **Bind9** en dos máquinas virtuales:
 - o **VM1:** Servidor DNS maestro (**maestro.empresa.local**).
 - o **VM2:** Servidor DNS esclavo (**esclavo.empresa.local**).
2. Configure el servidor maestro con:
 - o Una zona principal (**empresa.local**) con registros **A**, **CNAME**.
 - o Una zona de resolución inversa para la red local (**ejemplo: 1.168.192.in-addr.arpa**).
3. Configure el servidor esclavo para obtener la zona del servidor maestro mediante transferencia de zona (**AXFR**).
4. Verifique que cualquier máquina cliente configurada con el servidor esclavo pueda:
 - o Resolver correctamente los nombres de dominio.
 - o Realizar resolución inversa de direcciones IP.
5. Apague temporalmente el servidor maestro y demuestre que el esclavo sigue resolviendo nombres correctamente.

Evaluación:

- Configuración correcta del DNS maestro con registros **A**, **CNAME**.
- Implementación de resolución inversa en el maestro.
- Configuración del DNS esclavo con transferencia de zona habilitada.
- Validación de resolución de nombres y direcciones IP desde diferentes máquinas.
- Demostración del funcionamiento del esclavo en ausencia del maestro.
- Explicación detallada del proceso con evidencia de archivos de configuración y comandos utilizados.

TERCERA PARTE	(1.0 Puntos) Exponer un Servidor Web Local a Internet usando	PUNTAJE	
---------------	--	---------	--

Configurar un túnel hacia el servidor web implementado en clase, de manera que los recursos del servidor puedan ser accesibles desde cualquier lugar fuera de la red local. Para validar el funcionamiento, se debe agregar una página personalizada al sitio web.

Requisitos:

1. Tener un servidor web en funcionamiento en tu entorno local (por ejemplo, Apache, Nginx o cualquier servidor web implementado en clase).
2. Instalar y configurar **ngrok** (versión gratuita) para crear un túnel seguro hacia el servidor web.
3. Agregar una página personalizada al sitio web para fines de prueba.

Pasos sugeridos:

1. **Instalación de Ngrok:**
 - Descargar e instalar **ngrok** desde <https://ngrok.com/download>.
 - Agregar **ngrok** al PATH del sistema (variables de entorno) para poder ejecutarlo desde cualquier ubicación en la terminal o línea de comandos.
2. **Configuración del Servidor Web:**
 - Asegurarse de que su servidor web esté en funcionamiento y accesible desde el anfitrión
 - Crear una página personalizada en el directorio raíz del servidor web (por ejemplo, index.html o pagina_personalizada.html) con contenido único para identificarla durante la prueba.
3. **Crear un Túnel con Ngrok:**
 - Abrir una terminal o línea de comandos y ejecutar el siguiente comando para crear un túnel hacia el puerto en el que está corriendo tu servidor web (por ejemplo, puerto 80):

```
ngrok http 80
```
 - Ngrok generará una URL pública (por ejemplo, <https://abcd1234.ngrok.io>) que redirigirá al servidor web local.
4. **Probar el Acceso Remoto:**
 - Desde un dispositivo externo (por ejemplo, un teléfono móvil con datos móviles o una computadora en otra red), acceder a la URL generada por ngrok (por ejemplo, <https://abcd1234.ngrok.io>).
 - Verifica que la página personalizada creada en el servidor web se muestre correctamente.

Alternativa: Usar Vagrant Share con Ngrok

Si prefiere usar **Vagrant** en lugar de ngrok directamente, puede configurar **Vagrant Share** para exponer tu servidor web. Asegúrate de tener instalado Vagrant y ejecuta:

```
vagrant share
```

Esto generará una URL similar a la de ngrok para acceder al servidor web desde cualquier lugar.

EVALUACION

Valor	Descripción	Puntaje Obtenido
2.0	Apache + Autenticación PAM	
2.0	DNS Maestro/Esclavo	
1.0	Túnel con ngrok / Vagrant share	
	TOTAL	