**2. Configuración de un firewall**

**Ipchains**

ipchains es un firewall para Linux que fue usado antes de iptables. Aunque es menos común hoy en día, aquí hay un ejemplo básico de cómo configurarlo:

* **Listar reglas actuales**:

 ipchains -L

 **Agregar reglas**:

* ipchains -A input -p tcp -s 192.168.1.0/24 -j ACCEPT

**Iptables**

iptables es el sistema de firewall más utilizado en Linux hoy en día. Su configuración básica incluye:

* **Listar reglas actuales**:

 iptables -L -v

 **Agregar reglas**:

 iptables -A INPUT -p tcp --dport 22 -j ACCEPT # Permitir SSH

iptables -A INPUT -p tcp --dport 80 -j ACCEPT # Permitir HTTP

 **Guardar reglas**: Para que las reglas persistan después de reiniciar, se utilizan diferentes métodos según la distribución:

* service iptables save # En algunas distribuciones

**3. Restricción de acceso a servicios**

**TCP Wrappers**

Los TCP Wrappers permiten restringir el acceso a servicios basados en la dirección IP de un cliente. Para configurarlo:

* **Instalación**: Asegúrate de que el servicio esté instalado.
* **Editar /etc/hosts.allow y /etc/hosts.deny**:
  + /etc/hosts.allow: especifica qué IPs están permitidas.

 sshd: 192.168.1.\* # Permitir SSH a toda la red 192.168.1.0/24

 /etc/hosts.deny: especifica qué IPs están denegadas.

* + sshd: ALL # Denegar acceso a todos los demás

**4. Identificación de usuarios mediante PAM**

PAM (Pluggable Authentication Modules) es un sistema que permite gestionar la autenticación de usuarios en Linux. Su configuración se realiza generalmente en los archivos dentro de /etc/pam.d/:

* **Modificar archivos PAM**: Cada servicio puede tener un archivo correspondiente en /etc/pam.d/. Por ejemplo, para sshd puedes editar /etc/pam.d/sshd.
* **Agregar módulos**: Puedes incluir módulos como pam\_unix.so, pam\_tally.so, etc., para diferentes métodos de autenticación.

**5. Configuración de un servidor Kerberos**

Kerberos es un protocolo de autenticación que utiliza criptografía para garantizar la seguridad.

* **Instalación**: En una distribución Debian:

 sudo apt install krb5-kdc krb5-admin-server

 **Configuración**: Edita /etc/krb5.conf y /etc/krb5kdc/kdc.conf para ajustar los parámetros según tu dominio.

 **Inicializar la base de datos**:

 kdb5\_util create -r YOURREALM -s

 **Agregar usuarios**:

* kadmin.local -q "addprinc username"

**6. VPNs con IPsec**

IPsec es un conjunto de protocolos para asegurar la comunicación de red. Para configurarlo:

* **Instalación de herramientas**: En Debian puedes instalar strongSwan o libreswan.

 sudo apt install strongswan

 **Configuración**: Edita los archivos de configuración, generalmente en /etc/ipsec.conf y /etc/ipsec.secrets. Define políticas de seguridad y claves.

 **Iniciar el servicio**:

 sudo systemctl start strongswan

 **Comprobar estado**:

* sudo ipsec status