LPIC2 2021 Sesión 13 (2021-03-16)

Documentación relacionada:

- Manual Certificacion LPIC-2.pdf, pag XX
- Material Practicas LPIC-2/LPIC-202/
- Presentaciones/2020/202/
- gdrive://

Clase

PAM

- DOC: Material Practicas LPIC-2/LPIC-202/6-Network Client Management/Modulos de autenticacion con conexion (PAM)/Presentacion PAM.pdf
- mucha atención con los cambios. Los cambios se aplican directamente!
- **/etc/pam.d/**
- estructura de la línea:
    - tipo:
        - auth (autenticación): Autentica al usuario mediante un método y le proporciona los privilegios.
        - account (verificación): Comprueba si el usuario tiene permiso para utilizar el servicio o si el servicio esta permitido (control horario, por ejemplo).
        - password (actualización): Actualiza el mecanismo de autenticación.
        - session (sesión): Acciones que deben ejecutarse antes y/o después del acceso del usuario.
    - control: como actua PAM ante un fallo: ignorar, terminar ejecución, etc…
        - palabras (simple o histórica):
            - requisite: Se envía fallo sin ejecutar otros módulos.
            - required: Se enviará fallo, ejecutando previamente los otros módulos.
            - sufficient: Se enviará correcto si no existe fallo previo.
            - optional: Su respuesta solo se usa si no existe otro módulo de este servicio y tipo.
        - acciones (manera nueva):
            - [valor1=accion1 valor2=accion2]
    - camino al módulo:
        - si empieza por **/** es path absoluto
        - si no, bajo **/lib/security**
    - argumentos
- el orden de las líneas importa
- módulos:
    - pam_cracklib
    - pam_deny
    - pam_env
    - pam_limits
    - pam_listfile
    - …
    - módulo keylogger: pam_tty_audit
        - `aureport –tty`
        - DOC: Configurar Snoopy Logger.pdf

Laboratorio

- DOC: 1-Laboratorio PAM Gestión de cuentas de usuario.pdf
- ...
- `yum install vlock`
- permitir solo a los miembros de **wheel** hacer **su -**
  - /etc/pam.d/su
    - descomentar líneas 4 y 6:
      - auth sufficient pam_wheel.so trust use_uid
      - auth required pam_wheel.so use_uid
  - securizar sudo (en centos):
    - `visudo` → comentar **%wheel ALL=(ALL) ALL**
- técnicas de sudo
  - DOC: Configuración y uso de sudo.pdf
  - **NOEXEC:** limita la salida al shell de ciertos programas: vi,vim,cat,less
    - peligro de saltar a root desde una cuenta con sudo (aunque sea limitada)
  - **Defaults log_output**: reproducción sesiones sudo → `sudoreplay`
  - DOC: Clase tareas programadas-sudo-sudoreplay.txt
- DOC: 2-Laboratorios PAM.pdf
  - erratas: pag.7 **Wk** es para WORKING days
  - erratas: pag.7 **Wd** espara WEEKEND days
  - erratas: algunos ejemplos usan : y deberían ser ;
  - pam_time
    - /etc/pam.d/sshd
    - /etc/security/time.conf
    - /var/log/secure o /var/log/oauth
    - DOC: Configuracion time para pam.txt

LDAP

- DOC: pag. 183
- /etc/nsswitch.conf
  - passwd: files sss (primero mira en el fichero correspondiente, después en el sss → ldap)
- DOC: Material Practicas LPIC-2/LPIC-202/3-File Sharing/3-OpenLDAP/

essencials LDAP

- object class: definición de atributos de la clase
- ou = Organization Unit
- dn (distinguised name): ruta para identificar un objeto
- LDIF: LDAP Data Interchange Format
- ...

Laboratorio

- DOC: Laboratorio Configure LDAP Server Orion.pdf
- SOFT: LdapAdminExe-w64-1.8.3.zip
  - alternativa linux → LDAP Browser/Editor v2.8.2:
    - https://superuser.com/questions/217487/the-best-ldap-browser-in-linux
    - https://community.microfocus.com/t5/Identity-Manager-Tips/Jarek-Gawor-s-excellent-LDAP-Browser-Editor-v2-8-2/ta-p/1771772
- recomendaciones Berto:
  - server: Fedora 389 directory server : servidor LDAP recomendado

        - proyecto proviniente de Netscape, comprado por SUN y vendido a RedHat, parte CE
        - DOC:
        - Berto: 15 años experiencia. Mejor que openLDAP
    - cliente: softerra ldap browser (windows)
- instalación y setup básico:

```
yum -y install openldap-servers openldap-clients
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
chown ldap. /var/lib/ldap/DB_CONFIG
/etc/init.d/slapd start
```

- establecer contraseña admin:

```
slappasswd # {SSHA}vi6WZm+vOWA4E5PfgHtZlF+s8IelEfMY
```

- editar

  chrootpw.ldif

```
# specify the password generated above for "olcRootPW" section

dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}vi6WZm+vOWA4E5PfgHtZlF+s8IelEfMY
```

    - olcDatabase: ...
    - cn=config: ...
- añadimos la información:

```
ldapadd -Y EXTERNAL -H ldapi:/// -f chrootpw.ldif
```

- establecer domain name en LDAP DB
    - podemos reaprovechar el hash de la contraseña o crear una nueva con `slappasswd`

- chdomain.ldif

```
changetype: modify
replace: olcAccess
olcAccess: {0}to * by
dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"
  read by dn.base="cn=Manager,dc=curso,dc=local" read by * none

dn: olcDatabase={2}bdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=curso,dc=local

dn: olcDatabase={2}bdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=Manager,dc=curso,dc=local

dn: olcDatabase={2}bdb,cn=config
changetype: modify
add: olcRootPW
```

```
olcRootPW: {SSHA}vi6WZm+vOWA4E5PfgHtZlF+s8IelEfMY

dn: olcDatabase={2}bdb,cn=config
changetype: modify
add: olcAccess
olcAccess: {0}to attrs=userPassword,shadowLastChange by
  dn="cn=Manager,dc=curso,dc=local" write by anonymous auth by self write
by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by dn="cn=Manager,dc=curso,dc=local" write by * read
```

- cargamos:

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f chdomain.ldif
```

- ```
  dn: dc=curso,dc=local
  objectClass: top
  objectClass: dcObject
  objectclass: organization
  o: Curso Local
  dc: curso

  dn: cn=Manager,dc=curso,dc=local
  objectClass: organizationalRole
  cn: Manager
  description: Directory Manager

  dn: ou=People,dc=curso,dc=local
  objectClass: organizationalUnit
  ou: People

  dn: ou=Group,dc=curso,dc=local
  objectClass: organizationalUnit
  ou: Group
  ```

- cargamos:

```
ldapadd -x -D cn=Manager,dc=curso,dc=local -W -f basedomain.ldif
```

- reiniciamos:

```
service slapd restart
```

LDAP + PAM

- DOC: Presentacion FreeIPA.pdf
- IPA: identidad, política, auditoria
- aka AD
- usa, entre otros clientes, SSSD (que enlaza con los métodos permitidos desde PAM)
- DOC: Laboratorios FreeIPA.pdf
```