XARXES 2

Mòdul 1:

Seguretat de Sistemes

Instal·lació i Seguretat Bàsica

Carles Mateu
Departament d'Informàtica i Enginyeria Industrial
Universitat de Lleida

Particionament

- Instal·lació per defecte
  - LVM (volums lògics)
  - Particions
    - /boot : fitxers d'arranc
    - swap: espai d'intercanvi
    - / : directori arrel (tot l'espai restant)

Particionament

- Recomanacions de particions
  - /tmp : Fitxers temporals. Mida suficient (depen de les aplicacions).

  S'ha de crear partició perquè és un directori on tothom pot escriure, i, omplir així altres particions.
  - /var: Emprat per serveis de sistema (daemon) per guardar-hi fitxers que canvien sovint (dades).

  Crear partició per evitar que un servei de sistema pugui esgotar espai de disc d'altres particions.

Particionament

- /var/log : Fitxers de registre del sistema. 10Gbytes normalment és suficient, però dependrà de la durada que vulguem de registre.

S'ha de crear partició per evitar que un problema en un servei ompli una partició principal.

- /var/log/audit : Registre del servei d'auditoria del sistema. Si l'emprem, crear partició.

Particionament

- /home : Si tenim directoris d'usuari, crear partició.

Evita que usuaris puguin omplir particions.

Facilita migració de sistema operatiu: Atenció!!!

- /boot : Fitxers del gestor d'arranc.

Només cal si gestor d'arranc no suporta FS principal.

Convenient per actualitzacions.

Si preupgrade ->mida gran (suficient 250 Mbytes).

Particionament

- Particions xifrades:
  - Ideals per portàtils: en cas de pèrdua de l'equip les dades no son llegibles.
  - No tant ideals per servidors:
    - Menor velocitat d'accés a disc
    - Major dificultat de reparació
    - (més difícil “perdre” un servidor)

Gestor d'arranc

- Posar-hi paraula d'accés
  - Evita modificacions a la configuració del gestor d'arranc.
  - SINGLE BOOT!!!

Dispositius de xarxa

- En servidors:
  - Si no cal, no posar DHCP.
  - Si cal, tampoc posar-lo.
  - Mai.
    - Seqüència d'arranc de servidors no definida.
    - Massa fàcil atacar i liar-la.

Dispositius de xarxa

- Eliminar allò que no faci falta:
  - IPv4: Generalment necessàri.
  - IPv6: Generalment no fa falta.
- Posar 2 DNS (millor 3)

Paraula clau

- Recomanacions:
  - Mínim 12 caràcters
  - Barreja:
    - Majúscules
    - Minúscules
    - Caràcters especials
    - Números
  - No diccionari
  - Truquet: Nmemotècniques

Selecció de paquets

- TOTS FORA.
- Anar a selecció detallada i
- TOT FORA:
  - Especialment Xorg
  - Eines de desenvolupament
- Millor seleccionar paquets individuals que "meta-paquets" o grups (menys paquets).

Arrancada inicial

- Firewall:
  - Activat (en servidors difícilment justificable altra cosa).
- SELinux:
  - Enforcing (si ens ho podem permetre)

Actualitzacions

- Un cop instal·lat:

  ```
  yum check-update
  ```

  ```
  yum update
  ```

- Important, especialment en màquines de producció:
  - Comprovar abans d'aplicar els updates
  - Mantenir actualitzada la màquina (si empreu distribucions orientades a servidor/establilitat)

Actualitzacions

- yum-updatesd
  - Alguns consideren poc “madur”
  - Desactivar:

```
chkconfig yum-updatesd off
```

- Actualització manual:

```
yum -R 60 -y update yum
yum -R 15 -y update
```

  - Posar a cron.daily (recomanat) o weekly (fent un script)

Actualitzacions

- Vigilar molt al posar repositoris addicionals:
  - Seguretat
  - Conflictes de paquets ≥Actualitzacions automàtiques fallides
- Aprendre com funciona bé el sistema de gestió de paquets:
  - Protecció de paquets/versions
  - Múltiples nuclis
  - Downgrading
  - Signatura paquets

Modificacions a fitxers

- Instal·larem AIDE (Advanced Intrusion Detection Environment)
- Això guarda una Base de Dades de checksums dels binaris, per comprovar que no hagi passat res extrany.

Modificacions a fitxers

- Instal·lació:

  `yum install aide`
- Configuració a `/etc/aide.conf`
  (nosaltres deixarem valors per defecte).
- Creem base de dades inicials:

  `/usr/sbin/aide --init`

Modificacions a fitxers

- Copiem base de dades creada:

```
cp /var/lib/aide/aide.db.new.gz  \
/var/lib/aide/aide.db.gz
```

- Fem un check:

```
/usr/sbin/aide --check
```

- Podem automatitzar el check (crontab):

```
0 3 * * *   /usr/sbin/aide --check
```

Modificacions a fitxers

- Copiem base de dades, /usr/sbin/aide i /etc/aide.conf a mitjà de només lectura (per si de cas).

  I ens apuntem sha512sum del binari, la conf i la BBDD:

  ```
  sha512sum /usr/sbin/aide
  ```

- Verifiquem RPMs:

  ```
  rpm -qVa
  ```

  ```
  rpm -qVa | awk '$2 != "c" {print $0}'
  ```

Sistema de fitxers

- Evitar dispositius a particions no root:

  Afegir `nodev` a aquelles particions ext2/ext3 que no siguin /

  (posar ,nodev a la columna 4 d'aquella partició)

- Afegir `nodev,nosuid,noexec` a mitjans removibles.

Sistema de fitxers

- Permisos de fitxer:

```
1 2 3 4    5 6 7 8 9 10

- r w [xs] r w s r w t          Fitxer
```

1. Tipus: - fitxer, d directori, l link, c disp. caràcter, b disp. bloc, s socket, p pipe
2. Lectura propietàri
3. Escriptura propietàri
4. Execució propietàri (x) + SetUID (s)
5. Lectura grup
6. Escriptura grup
7. Execució grup (x) + SetGID (s)
8. Lectura altres
9. Escriptura altres
10. Execució altres (x) + sticky (t)

Molts cops es passa en OCTAL: [0-7][0-7][0-7][0-7]

Sistema de fitxers

- Restringir accés a dispositius des de consola.

  `/etc/security/console.perms.d/50-default.perms`

  - Eliminar (comentar) línies a partir de permission definitions, de tipus:

    ```
    <console>  0600 <floppy> 0600 root.floppy
    <xconsole>  0600 /dev/console 0600 root.root
    ```

  - Reduïr consola:

    ```
    <console>=tty[0-9][0-9]* vc/[0-9][0-9]* :0\.[0-9] :0
    <xconsole>=:0\.[0-9] :0
    ```

Sistema de fitxers - USB

- Eliminar suport automontatge USB.

  A `/etc/modprobe.conf`

  afegir

  `install usb-storage:`

  Això evita autocàrrega de driver USB-storage (càrrega manual possible).
- Eliminació suport USB storage (permanentment):

  `find / -name "usb-storage.ko" --exec rm {} \;`
- Eliminació via bootloader:
  - Afegir `nousb` a la línia kernel a `/etc/grub.conf`

Sistema de fitxers

- Eliminar automontatge:

```
chkconfig autofs off
```

- Si per alguna cosa s'ha de tenir GNOME/KDE/etc. Assegurar-nos de que no es faci automontage des de l'entorn gràfic.
- Eliminar suport de FS no requerits (hfs, hfsplus, udf, etc.). A `modprobe.conf`:

```
install hfs /bin/true
```

Sistema de fitxers

- Permisos de passwd, etc. :

  A /etc:

  ```
  chown root:root passwd shadow group gshadow
  chmod 644 passwd group
  chmod 400 shadow gshadow
  ```

- Sticky bits:

  ```
  find <part> -xdev -type d \( -perm -0002 -a ! -perm -1000 \) -print
  chmod +t <directori>
  ```

Sistema de fitxers

- Fitxers escribibles per tothom:

```
find <part> -xdev -type f -perm -0002  -print
```

```
chmod o-w <fitxer>
```

- Executables SUID/SGID:

```
find <part> -xdev -type f \( -perm -4002 -o
-perm -2000\)  -print
```

```
chmod -s <fitxer>
```

Sistema de fitxers

- Directoris escribibles per tothom amb propietari:

```
find <part> -xdev -type d -perm -0002 -uid +500
-print
```

- Orfes:

```
find <part> -xdev \( -nouser -o -nogroup\)
-print
```

Sistema de fitxers - Executables

- Serveis de sistema: umask. A /etc/sysconfig/init

```
umask 027
```

- Core dumps. A /etc/security/limits.conf

```
* hard core  0
```

- Core dumps de suid. A /etc/sysctl.conf

```
fs.suid_dumpable = 0
```

(comprovar-la després d'arrancar)

```
sysctl fs.suid_dumpable
```

Sistema de fitxers - Executables

- Comprovar l'activació d'ExecShield, a /etc/sysctl.conf:

```
kernel.exec-shield = 1
kernel.randomize_va_space = 1
```

(comprovar-la després d'arrancar)

```
sysctl kernel.exec-shield
sysctl kernel.randomize_va_space
```

Sistema de fitxers - Executables

- Si disposem a BIOS de NX (No Execute, AMD) o XD (Execute Disable, Intel), assegurar-nos de tenir-ho activat.
- Comprovar-ne soport:

  `/proc/cpuinfo -> pae,nx`
- Si 32bits i suport de PAE/NX assegurar-nos de tenir kernel PAE:

  `yum install kernel-PAE`

Control d'accés

- Restringir l'accés a root a només:
  - `console, tty[1-9]` (i si requerit `ttyS[0-9]`) (a `/etc/securetty`)
- Limitar capacitat de `su`:
  - Comprovar existència de grup `wheel`
  - Només grup wheel pot fer su. A `/etc/pam.d/su`:

```
auth    required    pam_wheel.so    use_uid
```

Control d'accés

- Emprar `sudo` per comandes de root

  `%wheel ALL=(ALL) ALL`

  (a `/etc/sudoers`)

- Editar amb `visudo`!

Control d'accés

- Restringir login a comptes de sistema (no root):
  - Buscar comptes de sistema:

    ```
    awk -F: '{print $1 ":" $3 ":" $7}' /etc/passwd
    ```

  - Identificar-ne els de sistema
- Per cada compte de sistema (no root)
  - Bloquejar: `usermod -L <compte>`
  - Eliminar shell: `usermod -s /sbin/nologin <compte>`

Control d'accés

- Revisar la política d'expiració de passwords.
- A `/etc/login.defs`
  - PASS_MAX_DAYS 60
  - PASS_MIN_DAYS 7
  - PASS_MIN_LEN 8
  - PASS_WARN_AGE 7
- Aplicar a usuaris individuals:

```
chage -M 60 -m 7 -W 7 <usuari>
```

Control d'accés

- Crear un grup únic per cada usuari

  (automàtic si no emprem -g al crear usuaris).
- Crear un grup que tingui tots els usuaris humans del sistema

  ```
  groupadd <grup>
  ```

  ```
  usermod -G <grup> <usuari>
  ```

  - Permet restringir algunes comandes a usuaris humans (p.e. eines de l'entorn gràfic):

    ```
    chgrp <grup> <fitxer>
    ```

    ```
    chmod 750 <fitxer>
    ```

Control d'accés

- Demanar autenticació en single boot

  Es trivial arrancar en single (si podem modificar el bootloader) i trencar la seguretat del sistema.

  Afegir a `/etc/inittab`:

  ```
  ~:S:wait:/sbin/sulogin
  ```

- Eliminar arrancada interactiva. A `/etc/sysconfig/init`:

  ```
  PROMPT=no
  ```

PAM

- Implementa autenticació modular
- Objectes que podem carregar/descarregar cada cop que s'ha d'autenticar un usuari
- Permet configurar combinacions múltiples de seguretat de forma fàcil.
- Permet afegir nous sistemes d'autenticació (smartcard, biomètrics, etc.) sense dificultat
- Configuració a /etc/pam.d/<servei>

  Servei system-auth configuració base d'altres serveis.

PAM

- Tenim 2 móduls per qualitat de passwords: pam_cracklib i pam_passwdqc(*)
- pam_cracklib (a `/etc/pam.d/system-auth`):
- Buscar:

```
password  requisite  pam_cracklib.so try_first_pass
retry=3
```

- Canviar per

```
password  required  pam_cracklib.so try_first_pass
retry=3 minlen=12 dcredit=-1 ucredit=-1 ocredit=-1
lcredit=0
```

PAM

- Instal·lar pam_passwdqc

  ```
  yum install pam_passwdqc
  ```

- Més potent que pam_cracklib
- Buscar (a `/etc/pam.d/system-auth`):

  ```
  password  requisite  pam_cracklib.so try_first_pass
  retry=3
  ```

- Canviar per

  ```
  password  requisite  pam_cracklib.so try_first_pass
  retry=3 minlen=12 dcredit=-1 ucredit=-1 ocredit=-1
  lcredit=0
  ```

PAM

- Móduls (inclosos):
  - pam_unix : Autenticació, gestió passwords, etc. tradicionals.
  - pam_deny: Denegació permanent.
  - pam_warn: logging a syslog
  - pam_nologin: si $\exists$ `/etc/nologin`, només root entra, altres veuen contingut de `nologin`
  - pam_tally2: Bloqueig usuaris si fallen login.

PAM

- Móduls (addicionals):
  - pam_ldap: usa LDAP per gestionar usuaris.
  - pam_smb: usa servidor SMB.
  - pam_krb5: usa Kerberos 5.
  - pam_ccreds: caché autenticació
  - pam_pkcs11: autenticació PKCS#11/NSS