M.0374 - Administració de SO

RA4- AMINISTRACIÓ REMOTA

Administració remota

- És l'administració d'un equip des d'un altre equip.
- Usos més freqüents:
  - Administració de sistemes
  - Helpdesk (suport i assistència tècnica)
  - Treball a distància
  - Supervisió d'activitats
  - Reunions i presentacions en línia
  - Aplicacions d'ensenyament

Administració remota

- Bàsicament hi ha 3 tipus:
  - Sessió de treball a la consola (el més lleuger)
    - Ex: Telnet i SSH
  - Sessió de treball amb interfície gràfica (el més visual)
    - Ex: VNC
  - Client o eina d'administració local (visual i flexible però cal instal·lar programa localment):
    - Ex: Remote Desktop, Webmin
- El tipus vé condicionat per les condicions de la xarxa de capacitat i seguretat.

TELNET - TELecommunication NETwork

Telnet és un protocol de xarxa que ens permet accedir a una altra màquina **remotament** i poder treballar-hi com si la tinguéssim al davant.

Està basat en una arquitectura **client-servidor.**

Transmet la informació com a text clar, **sense encriptar**, per tant suposa un **problema greu de seguretat.**

Utilitza el port **23**.

Instal·lació TELNET

En la majoria de distribucions GNU/Linux, el **client Telnet** està instal·lat de manera predeterminada (a Windows també, però cal activar-ho), però en cas que no ho sigui es pot instal·lar amb la següent comanda:

apt-get install telnet

El **servidor Telnet** es pot instal·lar amb la següent comanda:

apt-get install telnetd

Accés remot via TELNET

Un cop instal·lat el servidor, ja hi podrem accedir des de la màquina client.

Sintaxi bàsica de Telnet:

telnet <hostname> <port>

hostname: nom o IP del servidor on volem connectar-nos

port: 23

SSH- Secure Shell

SSH és un protocol de xarxa que permet l'intercanvi d'informació de manera **segura**.

Utilitza **xifrat i criptografia de clau pública** per tal de fer l'autenticació de l'estació remota.

L'ús de **SSH** més comú és utilitzar-ho per iniciar sessió remota per **executar ordres en substitució de Telnet**. Permet, entre d'altres, transmetre fitxers de **manera segura**.

SSH - Funcions

- Iniciar una sessió remota per tal d'executar ordres.
- Evitar enviar les contrasenyes en text pla.
- Transmetre fitxers de manera segura.
- Fer còpies de seguretat de manera eficient i segura en combinació a l'ordre **rsync**.

SSH - Funcions

- Fer túnels per assegurar qualsevol servei que no es transmeti encriptat (HTTP, SMTP, VNC, etc) o per travessar tallafocs que estiguin bloquejant el protocol.
- Fer segures les connexions X_{11} (des d'un host remot).
- Actuar com a sistema de fitxers en xarxa fent servir SSHFS (SSh File System) - sistema d'arxius basat en SSH que pot crear de manera segura un directori en un servidor remot

Instal·lació de SSH

SSH utilitza una arquitectura client-servidor, en què el client es connecta a una màquina remota, el servidor. Com en Telnet, normalment el client ja està instal·lat.

OpenSSH-server és la implementació més popular, per instal·lar-la executem la següent comanda al servidor:

```
apt-get install openssh-server
```

Arxius de configuració SSH

El **client OpenSSH** fa servir:

- Les opcions indicades a la **línia de comandes.**
- Els valors especificats a l'arxiu de **configuració de l'usuari**:

  $HOME/.ssh/ssh_config

- Els valors especificats a l'arxiu de **configuració del sistema:**

  /etc/ssh/ssh_config

Arxius de configuració SSH

La funció del servidor **SSH** és **esperar les connexions dels clients** (normalment al port TCP **22**), fer la seva **autenticació** i si tot ha anat bé, obrir sessió de treball, executar una ordre, o bé redreçar ports.

Cada cop que es rep un intent de connexió des d'un client, es fan totes les **comprovacions i inicialitzacions criptogràfiques** per **garantir la seguretat**. Després es tracta d'**autenticar l'usuari i iniciar sessió.**

Restriccions d'Accés

Si volem **habilitar o restringir** l'accés a determinats equips i serveis podem editar els arxius de configuració:

/etc/hosts.deny

/etc/hosts.allow

indicant els servei que volem controlar, en aquest cas, el **dimoni ssh.** El sistema, davant una petició d'aquest servei, comprovarà aquests arxius i segons el que trobi validarà l'accés o no.

Restriccions d'Accés

- Comprova a l'arxiu **hosts.allow**, si hi troba coincidència **valida** l'accés.
- Comprova a l'arxiu **hosts.deny**, si hi troba coincidència **no valida** l'accés.
- En cas de no trobar coincidència en cap dels arxius, **valida** l'accés.

Restriccions d'Accés

- Recordeu que perquè qualsevol canvi tingui efecte s'ha de reiniciar el servei:

  /etc/init.d/ssh restart

Exemples:

sshd: ALL (permet/denega l'accés ssh a tothom)

sshd: 192.168.56.10 (permet/denega accés SSH de la IP 192.168.56.10)

Connexió remota amb SSH

La funció més comuna per a **SSH** és **establir una sessió de treball remota** fent ús de les tècniques criptogràfiques per transmetre la informació. Lús del client SSH és força senzill:

```
ssh user@host
```

Ens demanarà pwd de l'equip remot, si és correcte podrem accedir a la sessió de treball remota.

Transferència d'arxius

Entre les utilitats d'**OpenSSH** trobem les ordres **scp** i **sftp**. Ens permeten transferir fitxers amb totes les **garanties de seguretat d'SSH.**

Còpia d'arxius

D'equip local a equip remot:

scp [opcions] fitxer1 [[user@]host2:]fitxer2

D'equip remot a equip local:

scp [opcions] [[user@host1:]fitxer1 ./

D'equip remot a equip remot:

scp [opcions] [[user@host1:]fitxer1 [[user@]host2:]fitxer2

SSH - Ordres

- **bye, exit, quit:** finalitzar sessió.
- **cd** camí: canviar al directori camí.
- **chgrp, chown, chmod:** canviar grup, propietari o permissos.
- **get** fitxer: portar el fitxer de remot a local.
- **put** fitxer: portar el fitxer de local a remot.
- **ls, mkdir, pwd, rename, rm, rmdir, ln**.
- **lcd, lld, lmkdir, lpwd**: versions de les ordres per “local”.