Fase 4 - Activitat 6: Configuració bàsica del servei SSH

1- Identificació del grup i activitat:

Curs: ASIX2
Projecte: PJ6 Administració de xarxes i sistemes operatius
Fase: 4
Activitat: 6
Grup/Individual: Individual

2- Objectius de l'activitat

Els objectius d'aquesta activitat són:

- Instal·lació del servei SSH
- Arxius de configuració i control del servidor.
- Estudi dels paràmetres bàsics de configuració del servidor SSH
- Resolució de noms amb /etc/hosts
- Instal·lació i configuració de clients SSH
- Claus públiques i privades.
- Configuració d'accés via SSH utilitzant claus remotes i privades
- Configuració del servei SFTP
- Instal·lació i configuració de clients SFTP
- Proves de funcionament

3- Documentació

- Documentació sobre criptografia de clau pública i privada
- Documentació sobre ssh-agent i ssh-add
- Documentació sobre ssh-keygen
- Documentació sobre sshd_config
- Documentació sobre ssh_config
- SFTP

4- Instal·lació dels sistemes operatius de proves i del programari

4.1- Instal·lació del sistema operatiu del servidor

a) Crea una màquina virtual utilitzant VirtualBox o VMware que tingui les següents característiques:

- Sistema operatiu: **Linux Debian (64 bits)**
- Nom: **srv-pj6**
- RAM: **2GiB**
- Disc dur: **20GiB**
- Xarxa: **Adaptador Pont**

b) Instal·la un sistema operatiu sobre la màquina anterior que tingui les següents característiques:

- Nom del sistema: **xxyyzz-srv-pj6** (**xx**=dues primeres lletres del teu nom, **yy**=dues primeres lletres del teu primer cognom, **zz**=dues primeres lletres del teu 2n cognom).
- Domini: **clotfje.net**
- Nom de l'usuari per defecte: **xxyyzz** (**xx**=dues primeres lletres del teu nom, **yy**=dues primeres lletres del teu primer cognom, **zz**=dues primeres lletres del teu 2n cognom).
- Durant el procés d'instal·lació demana la instal·lació de **Debian desktop environment**, **MATE** i **Utilitats estàndard del sistema**.

c) Un cop instal·lat el sistema, afegeix les **GuestAdditions**, i fes al teu usuari per defecte membre dels grups **sudo** i **vboxsf**.

4.2- Instal·lació del sistema operatiu del client

a) Crea una màquina virtual utilitzant VirtualBox o VMware que tingui les següents característiques:
- Sistema operatiu: **Linux Debian (64 bits)**
- Nom: **cli-pj6**
- RAM: **2GiB**
- Disc dur: **20GiB**
- Xarxa: **Adaptador Pont**

b) Instal·la un sistema operatiu sobre la màquina anterior que tingui les següents característiques:
- Nom del sistema: **xxyyzz-cli-pj6** (**xx**=dues primeres lletres del teu nom, **yy**=dues primeres lletres del teu primer cognom, **zz**=dues primeres lletres del teu 2n cognom).
- Domini: **clotfje.net**
- Nom de l'usuari per defecte: **asix2**.
- Durant el procés d'instal·lació demana la instal·lació de **Debian desktop environment**, **MATE** i **Utilitats estàndard del sistema**.

c) Un cop instal·lat el sistema, afegeix les **GuestAdditions**, i fes al teu usuari per defecte membre dels grups **sudo** i **vboxsf**.

4.3- Instal·lació del programari servidor SSH i client SSH

a) Dins del sistema **xxyyzz-srv-pj6** instal·la el programari **openssh-server**, **whois** i **net-tools**.

b) Dins del sistema **xxyyzz-cli-pj6** instal·la el programari **openssh-client**, **whois** i **net-tools**.

c) Comprova les adreces IP dels 2 equips.

d) Comprova la connectivitat entre equips.

e) Realitza una connexió via SSH des de l'equip client com usuari **asix2** al compte de l'usuari **xxyyzz de** l'equip servidor.

f) Comprova que pots crear/esborrar/modifica/visualitzar contingut dins de la carpeta personal de l'usuari **xxyyzz** des de l'equip client.

4.4- Control del servidor SSH i monitorització del port TCP obert pel servidor SSH

a) Comprova l'estat del servido amb l'ordre: **systemctl status ssh**

b) Comprova el port TCP obert pel servidor SSH amb l'ordre: **sudo netstat -atupn | grep -E '(Proto|ssh)'**

c) Comprova que pots **finalitzar/iniciar/reiniciar** el servidor amb les opcions **stop/start/restart**.

d) Què passa si finalitzes el servidor amb el port obert?. Continua obert o es tanca?

e) Què passa si reinicies el servidor amb el port obert?. Continua obert o es tanca?. Continua utilitzant el mateix número de port TCP?.

5- Treballant amb el fitxer /etc/hosts per fer resolució de noms

a) Comprova la seva adreça IP del servidor.

b) Modifica el fitxer **/etc/hosts** de l'equip **client** afegint l final una nova línia amb tres columnes:

- Primera columa → Adreça IP del servidor
- Segona columna → Nom complet del servidor (nom de host i nom de domini)
- Tercera columna → Nom de host del servidor

c) Des del client, fes un **ping** al servidor utilitzant el seu nom complet i el seu nom de host. Comprova que hi ha resposta.

d) Estableix una connexió del client al servidor utilitzant el nom complet o el nom de host en comptes de la seva adreça IP.

e) Modifica el fitxer **/etc/hosts** de l'equip **servidor** per poder resoldre el nom del client a la seva IP. Comprova si es pot fer un **ping** des del **servidor** al **client** utilitzant el nom del **client**.

6- Accés al servidor des del client utilitzant claus d'accés públiques i privades

a) Des del **servidor Debian** crea una carpeta dins del directori personal de l'usuari **xxyyzz** de nom **.ssh** per desar les claus públiques dels clients que accediran al servidor com usuari **xxyyzz**.

b) Accedeix al **client Debian** com usuari **asix2** i genera una *clau pública* per l'usuari. Executa:

```
ssh-keygen -t rsa
```

i respon així a les preguntes mostrades pel sistema:

- A la pregunta "Enter file in which to save the key (/home/inf1/.ssh/id_rsa): " deixa l'opció per defecte (prem Enter directament).
- A la pregunta "Enter passphrase (empty for no passphrase): " deixa l'opció per defecte (prem Enter directament).
- A la pregunta "Enter same passphrase again: " prem Enter directament.

c) Comprova que s'han creats els fitxers **id_rsa** i **id_rsa_pub** al directori **~/.ssh** de l'usuari **asix2** del **client Debian**.

d) És important que el sistema pugui gestionar i controlar de manera automàtica totes les claus públiques que pot utilitzar el **client Debian** per mitjà d'un agent SSH. Per fer-ho, executa les ordres:

```
eval $(ssh-agent)
ssh-add
```

NOTA: A l'enllaç https://kb.iu.edu/d/aeww trobareu informació sobre **ssh-add** i **ssh-agent**.

Comprova a continuació amb l'ordre:

```
ssh-add -l
```

que s'ha afegit la nova clau a la llista gestionades per **ssh-agent**.

e) Des del **client Debian** entra al directori **~/.ssh** de l'usuari **asix2** i executa:

scp id_rsa.pub xxyyzz@xxyyzz-srv-pj6.clotfje.net:~/.ssh/authorized_keys2

i comprova que el fitxer **id_rsa.pub** de de l'usuari **asix2** de l'ordinador **client Debian** es copia dins del directori **.ssh** de l'usuari **xxyyzz** de l'ordinador **servidor Debian** amb el nom **authorized_keys2**.

f) Ara, des de l'ordinador **client Debian** i des del compte de l'usuair **asix2** estableix una connexió al compte de l'usuari **xxyyzz** del **servidor Debian** executant:

ssh xxxyyy@ xxyyzz-srv-pj6.clotfje.net

Contesta "yes" a la primera pregunta (això només passarà una vegada) i comprova que pots connectar-te sense haver d'escriure la contrasenya de l'usuari **xxyyzz** de la màquina servidora. La connexió pot trigar uns segons.

g) Comprova que amb exit pots sortir de la connexió establerta des del client amb el servidor.

h) Què passaria si esborressis **authorized_key2** del directori **~/.ssh** de l'usuari **xxyyzz** del servidor **Debian i** intentessis connectar-te al servidor novament des del client?

7- Connexió via SFTP amb Filezilla

a) Què és *SFTP*?.

b) Instal·la el **client SFTP Filezilla** dins del **client Debian** executant les ordres:

sudo aptitude update
sudo aptitude install filezilla

c) Comprova que a la secció Internet del menú principal s'ha creat un accés al **client SFTP Filezilla** i que pots executar el programa sense cap problema. A continuació configura Filezilla per poder connectar-te al compte de l'usuari **xxyyzz** del **servidor Debian** utilitzant certificats de seguretat:

- Selecciona *File → Site Manager*
- Crea un *New Site* de nom **xxyyzz-srv-pj6**
- Selecciona *General → Protocol → SFTP*
- Completa el formulari de la pestanya General:
  - Protocol → **SFTP**
  - Host --> **xxyyzz-srv-pj6.clotfje.net**
  - Port → **22**
  - Logon Type → **Key File**
  - User → **xxyyzz**
  - Key file → és el fitxer que té la clau privada → **/home/asix2/.ssh/id_rsa**

A continuació prem el botó **Connect** per establir la connexió des del client **Filezilla** al sevidor **SSH** i accedeix des del **client Debian**, via **SFTP**, al compte i la carpeta de l'usuari **xxxyyy** del **servidor Debian**.

d) Comprova que tens dues finestres. A l'esquerra pots veure l'equip client i a dreta l'equip servidor.

e) Comprova que et connectes directament perquè el servidor confia en el teu client com a conseqüència de treballar amb claus públiques i privades i no cal indicar la contrasenya de l'usuari.

f) Desconnecta **Filezilla** del servidor correctament fent clic a l'opció de menú *Server --> Disconnect*.

g) Dins del **directori personal** del compte d'usuari **xxxyyy** del **servidor Debian** crea una carpeta de nom **sftp**. Dins de la carpeta **sftp** crea un fitxer de nom **test00.txt**. Escriu dins del fitxer el teu nom i cognoms. Desa el fitxer.

h) Des de **Filezilla** troba i selecciona el fitxer **test00.txt** i descarrega-ho a l'escriptori del teu equip client.

i) Modifica dins del teu equip client el fitxer **test00.txt** i afegeix una nova línia amb el teu cicle i curs (ASIX2), i una altra amb l'any acadèmic (2025-2026).

j) Des de **Filezilla** selecciona i refresca el fitxer **test00.txt** que es troba al teu equip client i puja-ho a la carpeta **sftp** de l'usuari **xxxyyy** del **servidor Debian** sobreescrivint el fitxer existent.

k)- Des del **servidor Debian** comprova que ara tens la nova versió del fitxer **test00.txt**.

l) Desconnecta **Filezilla** del servidor correctament

Lliurament 1 de l'activitat

a) Comprovacions:
- Connexió SSH directa des del client al servidor per mitjà de claus públiques i privades com usuari **xxyyzz**. Prova d'execució d'ordres des del client en el servidor.
- Connexió SFTP directa des del client al servidor per mitjà de claus públiques i privades i utilitzant Filezilla com usuari **xxyyzz**. Prova de pujada d'un fitxer del client al servidor.
- Connexió SFTP directa des del client al servidor per mitjà de claus públiques i privades i utilitzant Filezilla com usuari **xxyyzz**. Prova de baixada d'un fitxer del servidor al client.

b) Data límit: **Dijous 2-10-25** fins a les **21.00**. Fora d'aquest límit, aquesta activitat tindrà una menor puntuació.

8- CONFIGURACIÓ BÀSICA DEL SERVIDOR SSH

a) Crea des **del servidor Debian** un:
- Grup d'usuaris de nom **fje** amb GID igual a **1001**.
- Un usuari de nom **fje**, amb UID igual a **1001**, membre per defecte del grup **fje**, amb directori personal **/home/fje**, default shell igual a **/bin/bash**, skeleton igual a i contrasenya **clotfje25**. Comprova a continuació que s'ha creat l'usuari i també la seva carpeta personal.

b) L'arxiu de configuració del servidor SSH és **/etc/ssh/sshd_config**. Troba el significat dels següents paràmetres de configuració:

- Port
- ListenAddress
- LoginGraceTime
- PermitRootLogin
- AllowUsers
- MaxAuthTries

dins de la documentació del servidor SSH que pots trobar *aquí*.

c) L'arxiu de configuració del client SSH és **/etc/ssh/ssh_config**. Troba el significat dels següents paràmetres de configuració:

- NumberOfPasswordPrompts.

dins de la documentació del client SSH que pots trobar *aquí*.

d) A partir de la informació recollida a l'apartat **b)**, configura el **servidor SSH** de **xxyyzz-srv-pj6** manera que:

- El servidor escolti pel **port 2222** i la seva adreça IP.
- El servidor tanqui la connexió amb el client després de **15 segons** si l'usuari no s'ha validat.
- Permetre a l'usuari **root** validar-se via SSH.
- Permetre **només** la **validació** dins del servidor com els usuaris **fje** o **root**.
- Màxim nombre d'intents des del client abans que el servidor no permeti la connexió igual a **3**.

NOTA: Recorda que has de reiniciar el servidor un cop fets els canvis de l'arxiu de configuració.

e) A partir de la informació recollida a l'apartat **c)**, configura el **client SSH** de **xxyyzz-cli-pj6** de manera que el màxim número d'intents de connexió a un servidor sigui **10**.

f) Comprova amb que elv**servidor ssh** de l'ordinador **servidor Debian** està escoltant (LISTEN) per la seva adreça IP i pel port **2222**.

g) Connectat al **servidor Debian** des del **client Debian** com usuari **fje** del servidor i indicant el número de port de connexió afegint el paràmetre **-p** i després, el número de port.

h) Torna a intentar una connexió com **fje** però no finalitzis la validació fins passats **30 segons**. Un cop passar aquest temps, intenta validar-te i comprova la resposta del servidor. Què passa?.

i) Comprova que pots accedir com a **root** via **ssh** al servidor des del client.

j) Surt de la connexió com usuari **root** del servidor des del client. Intenta ara connectar-te com usuari **xxyyzz**. Què passa?.

k) Torna a intentar una connexió com **fje** però escriu una contrasenya en blanc (i per tant incorrecta) fins a 3 vegades. Què passa?.

Lliurament 2 de l'activitat

a) Comprovacions:

- Comprovació del port i adreça IP pel qual el servidor SSH admet connexions.
- Connexió SSH com usuari **fje** al servidor utilitzant el port **2222**.
- Connexió SSH com usuari **root** al servidor utilitzant el port **2222**.
- Comprovació que l'usuari **xxyyzz** no pot establir connexió.
- Comprovació del missatge mostrat pel sistema si l'usuari **fje** escriu incorrectament la contrasenya **3** vegades.
- Comprovació del missatge mostrat pel sistema si l'usuari **fje** espera més de 15 segons per efectuar el procés de validació..

b) Data límit: **Dijous 2-10-25** fins a les **21.00**. Fora d'aquest límit, aquesta activitat tindrà una menor puntuació.