Pràctica 2 – Accés als recursos de xarxa

Sessió 1 - Accés al servidor mitjançant SSH i SFTP

Alumnes:
Mariona Farré Tapias,
Adrian Garcia Campillo

- Respon a cadascuna de les següents preguntes tot seguint aquesta estructura:
  - Breu raonament de la resposta.
  - Comanda / menú / opció a utilitzar.
  - Fitxers de configuració involucrats, si s'escau.
  - Evidència d'ús.
  - Bibliografia.

Per fer aquesta pràctica haurem d'instal·lar.
john
openssh-client
openssh-server

1. Verificación de las contraseñas con John the Ripper
Per fer aquest apartat ens hem d'instal·lar la aplicació de john de ripper, utilitzant la comanda: root@seax1:~# apt install john

- Com es pot verificar la seguretat de les contrasenyes dels usuaris d'una màquina amb l'aplicació John de Ripper?
Per verificar la seguretat de les contrasenyes dels usuaris d'una màquina amb John the Ripper, es segueixen aquests passos:

Obtenció dels fitxers necessaris: Primer, es necessiten els fitxers /etc/passwd i /etc/shadow, ja que contenen la informació dels usuaris i les seves contrasenyes xifrades, respectivament. L'accés a aquests fitxers requereix permisos d'administrador.

Utilitzant l'eina unshadow, es combinen els fitxers /etc/passwd i /etc/shadow en un únic fitxer que John the Ripper pugui utilitzar per intentar trencar les contrasenyes. Això es fa amb el següent comandament:

"unshadow /etc/passwd /etc/shadow > combined.txt"

A continuació, s'utilitza John the Ripper per analitzar el fitxer resultant i intentar trencar les contrasenyes. Això es pot fer de diverses maneres, incloent atacs de força bruta, de diccionari, etc. Un exemple utilitzant un atac de diccionari seria:

"john –format=crypt --wordlist=<path_to_dictionary_file> combined.txt"

Aquí, path_to_dictionary_file hauria de ser el camí al fitxer de diccionari que vols utilitzar per l'atac. Hi ha diversos diccionaris disponibles gratuïtament a Internet, i John the Ripper també inclou alguns per defecte. Utilitzarem “passwd.lst” que ja ve inclós amb john.

Anàlisi dels resultats: Després d'executar John the Ripper, es poden revisar les contrasenyes que s'han pogut trencar. Això es pot fer utilitzant el comandament:

“john --show combined.txt”

Aquest comandament mostra les contrasenyes trobades juntament amb els noms d'usuari corresponents.

En el nostre cas ens diu que les ha crackejat les dos contrasenyes d’usuari.
Fitxers de configuració involucrats: /etc/passwd, /etc/shadow

Evidència d'ús: 1-1.txt
Bibliografia:man john

- Com s’utilitzen els diccionaris per verificar la seguretat de les contrasenyes dels usuaris d’una màquina?
L'ús de diccionaris per verificar la seguretat de les contrasenyes dels usuaris d'una màquina és una tècnica comuna en el testing de penetració i en la auditoria de seguretat. Aquest mètode es basa en l'ús de llistes predefinides de paraules (diccionaris) que es consideren possibles contrasenyes. Aquestes paraules poden incloure paraules comunes, frases fetes, contrasenyes popularment utilitzades, i variacions complexes d'elles.
Existeixen nombrosos diccionaris disponibles en línia, que varien en complexitat i en l'idioma. La selecció d'un bon diccionari és crucial, ja que un diccionari més complet pot millorar les possibilitats d'èxit de l'atac.
Una vegada tenim el diccionar utilitzem “john --wordlist=/path/to/dictionary.txt <fitxer>.txt”.
Evidència d'ús: 1-2.txt
Bibliografia:man john

2- Servei SSH

Accions i requeriments

- Implementa un servidor i un client SSH.
- L'usuari entel hi té accés mitjançant usuari i contrasenya.
- L'usuari root hi té accés mitjançant una parella de claus privada/pública.
- Configura els paràmetres d'informació, xifrat, accés i manteniment de la sessió.
- Fes captures de xarxa amb un servidor i un client per validar els resultats.

Qüestions a respondre

- Com s'instal·la el servidor de SSH?

Per instal·lar el servidor SSH en un sistema Debian, en la terminal s'han d'executar les següent comandes per actualitzar la llista de paquets i instal·lar el servidor ssh en la màquina.

root@seax1:~# apt update
root@seax1:~# apt install openssh-server

En una altre màquina instal·lar s'haura d'instalar el openssh-client, respost en la pregunta 2.8 i preguntes següents.

Evidència d'ús: 2-1.txt
Es pot veure l'execució de les comandes anteriors.

Bibliografia: Web debian servidor ssh: https://wiki.debian.org/SSH

- Com es configura el servidor de SSH?

Per configurar els diferents paràmetres del servidor ssh, el que s'ha de fer és modificar el fitxer: /etc/ssh/sshd_config depenen de les característiques que es vulguin per començar posarem:

- que el port sigui el 22 i
- que l'usuari root puguin accedir per parella de claus pública/privada descomentant la línea: PermitRootLogin prohibit-password
- que qualsevol usuari (entel) entri per usuari i contrasenya descomentant la línea: PasswordAuthentication yes
- Configurar el manteniment de la sessió: deixar que el servidor comprovi cada 900 segons si el client està actiu: ClientAliveInterval 900
- Configurar el manteniment de la sessió: el màxim de clients connectats alhora: ClientAliveCountMax 3

Podem fer-ho executant: root@seax1:~# nano /etc/ssh/sshd_config

Per guardar els canvis, a part de guardar correctament el fitxer, també hem de reiniciar el servei ssh per aplicar els canvis executant: root@seax1:~#systemctl restart ssh

Fitxers involucrats: /etc/ssh/sshd_config
Per configurar manualment la configuració del servidor

Evidència d'ús: 2-2.txt
Es pot veure l'execució de les comandes anteriors.

Bibliografia: Web debian servidor ssh: https://wiki.debian.org/SSH

- Com es verifica el funcionament del servidor de SSH?

Per veure el funcionament actual del servidor podem fer-ho amb status ssh, que ens retorna una sèrie de la informació del servei com el seu estat, on s'executa, les tasques que té i la memòria i la cpu que utiliza.

Podem fer-ho executant: root@seax1:~# systemctl status ssh
Aquest estarà actiu si i només si té l'apartat de 'Active:' com a active.
Es pot parar el servei executant: root@seax1:~# systemctl stop ssh que deixarà inactive el servei
I per tornar a activar el servei s'ha d'executar: root@seax1:~# systemctl enable ssh i root@seax1:~# systemctl start ssh i retornarà al seu sistema actiu.

Evidència d'ús: 2-3.txt
Es pot veure l'execució de les comandes anteriors.

Bibliografia: Web debian servidor ssh: https://wiki.debian.org/SSH

- Com es genera una parella de claus privada/pública?

Per generar les claus, s'ha de fer executant keygen en el servidor, fent això es generarà una id_rsa.pub en la màquina la pública i una fitxer id_rsa serà la clau privada.
MI
root@seax1:~# ssh-keygen -t rsa -b 4096
Especificant que el tamany sigui de 4096 bytes
root@seax1:~# cat /root/.ssh/id_rsa.pub
Es pot veure que la clau privada ha sigut creada correctament.

Podem fer un ls de /root/.ssh/ per veure si s'han creat la clau privada: id_rsa i la clau pública: id_rsa.pub

Es pot fer un cat /root/.ssh/id_rsa.pub per veure la clau pública.

Evidència d'ús: 2-4.txt
Es pot veure l'execució de les comandes anteriors.

Bibliografia: Web debian servidor ssh: https://wiki.debian.org/SSH

- Com es permet l'accés per SSH amb una parella de claus privada/pública?

Per permetre l'accés en la connexió ssh a través d'una parella de claus privada i pública s'ha de configurar correctament el fitxer de configuració del servidor, descomentant i modificant tots els paràmetres necessaris.
En aquest cas, com hem explicat en la pregunta 2.2, descomentarem els següents paràmetres per seguir les especificacions donades:

- que el port sigui el 22 descomentant la línea: Port 22
- que l'usuari root puguin accedir per parella de claus pública/privada descomentant la línea: PermitRootLogin yes
- que qualsevol usuari (entel o test) entri per usuari i contrasenya descomentant la línea: PasswordAuthentication yes

Fitxers involucrats: /etc/ssh/sshd_config
Per configurar la configuració de les claus del servidor ssh

Evidència d'ús: 2-5.txt
Es pot veure l'execució de les comandes anteriors.
Podem veure que per l'usuari root s'ha de enviar la clau privada utilitzant: ssh-copy-id root@192.168.1.25 i després també demanaran la contrasenya del usuari root.
Després si es vol connectar amb un usuari no root, com el test, només es necessita entrar la contrasenya d'aquest usuari.

Bibliografia: Web debian servidor ssh: https://wiki.debian.org/SSH

- Com es distribueix una parella de claus privada/pública?

Per distrubuir les claus, és un procés ben senzill si la configuració de les màquines és la adecuada, en el nostre cas amb dues màquines virtuals hem activat dos interfícies bridge perquè es puguin connectar entre elles:

- màquina 1 (seax1): 192.168.1.26
- màquina 2 (seax2): 192.168.1.25

Això es pot mirar executant:root@seax1:~# ip addr show enp0s9 , en les dues màquines

Una vegada sabem les ips, podem enviar les claus a través de la comanda:
root@seax1:~# ssh-copy-id usuari@ip_servidor
En el nostre cas enviarem de la màquina 1 a la màquina 2:
root@seax1:~# ssh-copy-id entel@192.168.1.25

Al acabar la còpia correctament, ens donarà com connectar-nos a la màquina, utilitzant la comanda: ssh 'entel@192.168.1.25
I si ens connectem podem veure que s'estableix correctament la connexió dins de la màquina client (seax2) i podem veure els seus fitxers, com el del nostre cas a /home_seax2/dins_seax2.txt
Que ens verifica que estem a dins, ja que la màquina servidor (seax1) no té aquest fitxer creat.

Evidència d'ús: 2-6.txt
Es pot veure l'execució de les comandes anteriors.

Bibliografia: Web debian servidor ssh: https://wiki.debian.org/SSH

- Com cal configurar les carpetes dels usuaris?

Per configurar correctament les carpetes d'usuari, sobretot les utilitzades en la connexió ssh, és molt important per mantenir una seguretat correcte en el sistema.

- Propietari tingui permisos complerts, llegir escriure i executar mentre que els altres només poden llegir i executar: chmod 755 /carpeta
- Llegibles per qualsevol usuari però només modificable pel propietari: chmod 644
- Per restringir permisos d'una fitxer fins que el només el seu propietari pugui llegir, escriure i executar: chmod 700
- Només el propietari pot llegir i escriure el fitxer: chmod 600

En un servei ssh, necessitarem posar seguretat en els fitxers de les claus privades i en la carpeta ssh en general:
Dins de la màquina client executar:
root@seax1:~#chmod 700 /root/.ssh/
root@seax1:~#chmod 600 /root/.ssh/id_rsa
root@seax1:~ chmod 644 /root/.ssh/id_rsa.pub
Des de la màquina client hem de comprovar que els usuaris tampoc puguin accedir als fitxers dels altres usuaris, en la màquina server hi han dos usuaris: entel i test i des de entel hem de comprovar que no pot accedir al /home del test

Evidència d'ús: 2-7.txt
Es pot veure l'execució de les comandes anteriors.
Podem mirar els usuaris de la màquina server utilitzant getnet passwd i en el llistat trobarem el test i el entel, i com /home/test és un fitxer de l'usuari test.

Bibliografia: Web debian servidor ssh: https://wiki.debian.org/SSH

- Com s'instal·la el client de SSH?

Des de una altre màquina, s'ha d'instal·lar els paquets de openssh però ara el paquet específic de client.
Ara la màquina client serà seax2 i el servidor seax1.
Per fer-ho instal·lar el paquet necessari per tenir les opcions de ser un client ssh.

root@seax2:~# apt install openssh-server

Evidència d'ús: 2-8.txt
Es pot veure l'execució de les comandes anteriors.

Bibliografia: Web debian servidor ssh: https://wiki.debian.org/SSH

- Com es configura el client de SSH?

Per permetre l'accés en la connexió ssh amb un client s'ha de configurar correctament el fitxer de configuració de d'aquest , descomentant i modificant tots els paràmetres necessaris.
En aquest cas, com hem explicat en la pregunta 2.2, descomentarem els següents paràmetres per seguir les especificacions donades:

- que el port sigui el 22 descomentant la línea: Port 22
- indicar la ubicació de la clau privada: IdentityFile ~/.ssh/id_rsa
- que qualsevol usuari (entel o test) entri per usuari i contrasenya descomentant la línea: PasswordAuthentication yes

Fitxers involucrats: /etc/ssh/ssh_config
Per configurar la configuració del client ssh

Evidència d'ús: 2-9.txt
Es pot veure l'execució de les comandes anteriors.

Bibliografia: Web debian servidor ssh: https://wiki.debian.org/SSH

- Com es verifica el funcionament del client de SSH?

Per poder verificar el correcte funcionament del client ssh, es pot provar de diferents maneres, una de els maneres és sense connectar-se rebre la informació de la connexió executant: root@seax2:~# ssh -vvv test@192.168.1.25
Aixi podem veure la informació amb gran detall de la connexió entre les màquines.
També ho podem fer executant una comanda com: root@seax2:~# ssh test@192.168.1.25 "whoami"
Si aquesta comanda és executada correctament i la connexió ssh esta establerta retornarà el nom d'usuari, en el nostre cas sera l'usuari test.

Evidència d'ús: 2-10.txt
Es pot veure l'execució de les comandes anteriors.

Bibliografia: Web debian servidor ssh: https://wiki.debian.org/SSH

- Com es verifica l'empremta SSH d'un servidor?

L'empremta digital d'un servidor és un resum únic generat a partir de la clau pública del servidor, aquesta es pot obtenir utilitzant ssh-keyscan i la ip del servidor.
En el nostre cas seria: root@seax1:~#ssh-keyscan 192.168.1.26
I utilitzar per obtenir l'empremta clau:
root@seax1:~# ssh-keyscan 192.168.1.26 | ssh-keygen -lf -

Evidència d'ús: 2-11.txt
Es pot veure l'execució de les comandes anteriors.

Bibliografia: Web debian servidor ssh: https://wiki.debian.org/SSH

- Com es poden generar túnels SSH?

Evidència d'ús: 2-12.txt

Es pot veure l'execució de les comandes anteriors.

Bibliografia: Web debian servidor ssh: https://wiki.debian.org/SSH

- Com es verifica el funcionament dels túnels SSH?

Evidència d'ús: 2-13.txt

Es pot veure l'execució de les comandes anteriors.

Bibliografia: Web debian servidor ssh: https://wiki.debian.org/SSH

3- Servei SFTP.

Accions i requeriments

- Implementa un servidor i un client SFTP.
- Defineix les accions tant pel servidor com pel client.
- Comparteix la carpeta home de l'usuari.
- L'usuari no podrà accedir a la resta de disc.
- Defineix les regles del tallafocs adients per a aquest servei.
- Fes proves mitjançant captures de xarxa amb un servidor i un client.

Qüestions a respondre

- Com s'instal·la un servidor de fitxers amb SFTP?

Al instal·lar openssh-server aquest ve instal·lat automàticament. Per comprovar-ho podem mirar el fitxer de configuració "/etc/ssh/sshd_config", i buscar la línia "Subsystem sftp /usr/lib/openssh/sftp-server".
També podem intentar fer una connexió i comprovar si aquesta funciona, fent des del client "sftp usuari@ip".
Si no està instal·lat es pot fer seguint les comandes anomenades anteriorment:

```
root@seax1:~#  apt update
root@seax1:~#  apt install openssh-server
```

Per comprovar la connexió entre dues màquines:

- servidor (seax1): 10.0.3.4
- client (seax2):10.0.3.7

Podem executar un tcpdump per veure que realment estan connectats i s'intercanvien fitxers.

```
root@seax1:~#tcpdump -i enp0s8 -w sftp.pcap
```

Evidència d'ús: 3-1.txt
Es pot veure l'execució de les comandes anteriors.

Bibliografia: man ssh
Web debian oficial sftp: https://manpages.debian.org/stretch/openssh-client/sftp.1.en.html

- Com es configura un servidor de fitxers amb SFTP?

Per configurar un servidor SFTP, hem de modificar el fitxer "/etc/ssh/sshd_config".
Nosaltres afegirem les següents variacións al fitxer.

1. Limitar Usuaris a SFTP

```
"Match User entel
   ChrootDirectory %h
   ForceCommand internal-sftp
   AllowTcpForwarding no
   X11Forwarding no"
```

Això engabiarà (chroot) els usuaris especificats al seu directori home i només els permetrà utilitzar SFTP.

2. Desconnectar Automàticament els Usuaris Inactius

```
"ClientAliveInterval 300
```

ClientAliveCountMax 0”
Aquí, un usuari seria desconnectat si ha estat inactiu durant 300 segons (5 minuts). ClientAliveCountMax indica el nombre de comprovacions de vida del client que el servidor SSH envia sense rebre cap resposta del client abans de tancar la connexió. Posar-lo a 0 desconnectarà el client si el temps de vida supera el ClientAliveInterval sense activitat.

3. Limitar el Nombre d'Intents d'Inici de Sessió

“MaxAuthTries 3”
Això limita l'usuari a 3 intents d'autenticació fallits abans de tancar la connexió.

4. Desactivar Inici de Sessió com a Root

“PermitRootLogin no”

5. Canviar el Port per Defecte

“Port 2222”
Canviar el port SSH del port per defecte (22) a un altre pot ajudar a reduir els atacs de força bruta.

6. Limitar el Nombre d’usuaris actius

“MaxSessions 10”
Això limita a 10 el nombre d’usuaris que és poden conectar per sftp a la vegada.

Per últim reiniciem el ssh per a que tots els canvis tinguin efecte.
“systemctl restart sshd”

Fitxers involucrats: /etc/ssh/sshd_config
Per configurar la configuració del client ssh

Evidència d'ús: 3-2.txt
Es pot veure l’execució de les comandes anteriors.

Bibliografia: man ssh
Web debian oficial sftp: https://manpages.debian.org/stretch/openssh-client/sftp.1.en.html

- Com es verifica un servidor de fitxers amb SFTP?

Per confirmar que la connexió ha estat configurada correctament podem fer-ho conectant-se al servidor a través d’un client SFTP utilitzant la comanda: sftp -P 22222 <nom_usuari>@<direccio_ip>”
En el nostre cas serà des del client:root@seax2:~# sftp -P 2222 entel@192.168.1.26

Evidència d'ús: 3-3.txt
Es pot veure l’execució de les comandes anteriors.
Com podem veure des del client seax2, entrem amb l’usuari entel al servidor seax1, on podem entrar a la seva carpeta /home/entel i podem entrar a la carpeta /home_seax1/ on hi ha un document .txt únic del servidor seax1, que verifica que es veu correctament

Bibliografia: man ssh

- Com es pot compartir un directori amb SFTP?

Per poder compartir un directori amb sftp, primer hem de crear aquest directori dins del servidor, aquesta l’anomenarem: /root/directori_sftpcomp

Des del servidor li donarem permisos pels usuaris poder connectar-se en la carpeta executant:
Ara en el fitxer de configuració hem de especificar que l'usuari entel, començarà en la carpeta creada posant:

Ara si entrem executant el sftp i mirem el directori actual, executant pwd dins de sftp, ens retornarà /, que serà el directori base d'aquest usuari (la carpeta /directori_sftpcomp)

```
Match User entel
        ChrootDirectory /root/directori_sftpcomp
        ForceCommand internal-sftp
        AllowTcpForwarding no
        X11Forwarding no
```

Fer un reboot del servei per guardar els canvis: root@seax1:~# systemctl restart sshd

Fitxers involucrats: /etc/ssh/sshd_config
Per configurar la configuració del servidor sftp

Evidència d'ús: 3-4.txt
Es pot veure l'execució de les comandes anteriors.
Podem veure que entra correctament a la carpeta si podem veure que en el servidor (seax1) hi ha un fitxer anomenat hola.txt, i al connectar nos amb el client (seax2) amb l'usuari entel, veu aquest fitxer en la seva carpeta "/", justificant que s'ha enllaçat correctament les carpetes.

Bibliografia: man ssh

- Com es pot engabiar un usuari (chroot) amb SFTP ?

Per engabiar un usuari chroot, primer s'ha de crear aquest usuari en el servidor, utilitzant:root@seax1:~# useradd chroot , després s'ha de crear un grup d'usuaris, anomenat sftpgrup utilitzant la comanda:root@seax1:~# groupadd sftpgrup
Després enllaçar el usuari dins del nou grup creat: root@seax1:~# usermod -aG sftpgrup chroot
Ho podem verificar executant: root@seax1:~# getent group sftpgrup, veient que està l'usuari chroot
Ara crear una carpeta específica per el usuari i donar-li privilegis:
root@seax1:~# mkdir -p /home/chroot/
root@seax1:~#chmod 755 /home/chroot/

En el fitxer de configuració de ssh, posar en específic el grup creat amb la carpeta creada:

```
Match Group sftpgrup
        ChrootDirectory /home/chroot
        ForceCommand internal-sftp
        AllowTcpForwarding no
        X11Forwarding no
```

Fer un reboot del servei per guardar els canvis: root@seax1:~# systemctl restart sshd

(Si dona problemes en la connexió amb sftp de possibles contrasenyes, és important establir una contrasenya per l'usuari chroot, des de servidor executar: root@seax1:~# passwd chroot i establir una contrasenya)

Fitxers involucrats: /etc/ssh/sshd_config
Per configurar la configuració del servidor sftp

Evidència d'ús: 3-5.txt
Es pot veure l'execució de les comandes anteriors.
Podem dir que esta engabiat, perquè només té accés a la seva carpeta de /home/chroot, les altres carpetes del servidor com / home_seax1 o /scripts no pot entrar

Bibliografia: man ssh

- Com es securitza un servidor de fitxers SFTP?

Per fer més segur el servidor sftp, sha de fer a través de la modificació del fitxer de configuració, aquest es l'hem modificat segons:

1. Port personalitzat: S'ha canviat el port SSH al 2222 per millorar la seguretat.
2. Accés root permès: Malgrat ser una pràctica de seguretat desaconsellada, s'ha permès l'accés SSH per l'usuari root.
3. Autenticació per contrasenya habilitada: S'ha permès l'autenticació amb contrasenya, en lloc de limitar-se només a claus SSH.
4. Ús de PAM: S'ha habilitat l'ús de PAM per a autenticació i processament de sessió, proporcionant flexibilitat en els mètodes d'autenticació.
5. Configuració SFTP per usuaris específics: S'han definit directrius per restringir usuaris SFTP a directoris específics i permetre només l'ús de SFTP.
6. Configuració de Client Alive: S'ha configurat per mantenir connexions vives durant 5 minuts.

I amb tots els usuaris i grups d'usuaris especificats perquè tinguin el seu propi directori compartit.

Fitxers involucrats: /etc/ssh/sshd_config
Per configurar la configuració del servidor sftp

Evidència d'ús: 3-6.txt
Es pot veure l'execució de les comandes anteriors.

Bibliografia: man ssh

- Com s'instal·la un client de fitxers amb SFTP?

Per instal·lar un client de fitxers amb suport per a SFTP en un sistema Debian, pots utilitzar la línia d'ordres i el paquet openssh-client
Continuarem tenint la màquina client seax2 i el servidor seax1.
Per fer-ho instal·lar el paquet necessari per tenir les opcions de ser un client ssh.
root@seax2:~# apt update
root@seax2:~# apt install openssh-server

Evidència d'ús: 3-7.txt

Es pot veure l'execució de les comandes anteriors.

Bibliografia: man ssh

- Com es configura un client de fitxers amb SFTP?

Per permetre l'accés en la connexió d'un client amb SFTP s'ha de configurar correctament el fitxer de configuració de d'aquest , descomentant i modificant tots els paràmetres necessaris.
Descomentarem els següents paràmetres del fitxer /etc/ssh/ssh_config

- que el port sigui el 22 descomentant la línea: Port 22
- indicar la ubicació de la clau privada: IdentityFile ~/.ssh/id_rsa
- que qualsevol usuari (entel o test) entri per usuari i contrasenya descomentant la línea: PasswordAuthentication yes

Fitxers involucrats: /etc/ssh/ssh_config
Per configurar la configuració del client sftp

Evidència d'ús: 3-8.txt
Es pot veure l'execució de les comandes anteriors.

Bibliografia: man ssh

- Com es verifica un client de fitxers amb SFTP?

Per verificar un client de fitxers amb SFTP, generalment voldràs assegurar-te que el client pot connectar-se amb èxit al servidor SFTP i transferir fitxers de manera segura. Això implica:

Comprovar la Connexió:
Utilitza el comandament sftp seguit de l'identificador d'usuari i l'adreça del servidor (p. ex., sftp usuari@servidor.com). Hauries d'entrar al mode SFTP si la connexió és exitosa.
Si és la primera vegada que et connectes, se't demanarà que verifiquis l'empremta digital del servidor.

Transferència de Fitxers:
Un cop dins de la sessió SFTP, prova de pujar (put fitxer) i baixar (get fitxer) fitxers per assegurar que la transferència de fitxers funciona com s'espera.

Sortir de la Sessió:
Utilitza el comandament exit o bye per sortir de la sessió SFTP.

Evidència d'ús: 3-9.txt
Es pot veure l'execució de les comandes anteriors.
Ho podem mirar executant: :root@seax2:~# sftp -P 2222 root@10.0.3.7 i executant les opcions anteriors.
Com podem veure, el usuari root pot entrar a qualsevol carpeta i fitxer (com les del usuari chroot), mentre que com hem vist anteriorment a la pregunta 3-9 l'usuari chroot només pot llegir la seva única carpeta.
O mirant els diferents paquets que s'intercanvien amb el tcpdump

Bibliografia: man ssh

- Com es pot muntar automàticament (fstab) un recurs compartit amb SFTP?

Primer de tot haurem d'instal·lar:
root@seax2:~# apt install sshfs
Copiem la clau pública de la màquina que utilitzem com a client a la màquina que utilitzem com a servidor amb la comanda "ssh-copy-id <usuari@ip>.
Afegim la següent línia al /etc/fstab
usuari@<ip>:/directori/destí /punt/muntatge fuse.sshfs defaults,_netdev,allow_other,reconnect,IdentityFile=/home/usuari/.ssh/id_rsa 0 0
Reiniciem l'equip o muntem el fstab amb "mount -a",

Evidència d'ús: 3-10.txt
Es pot veure l'execució de les comandes anteriors.
I podem veure els fitxers intercanviats utilitzant el tcpdump.

Bibliografia: man ssh

- Com es pot muntar manualment un recurs compartit amb SFTP?

Amb el paquet ssgfs instal·lat utilitzem la següent comanda
"sshfs usuari@servidor.com:/directori/destí ~/directori/muntatge -o allow_other,reconnect,IdentityFile=/home/usuari/.ssh/id_rsa
Per desmontar utilitzarem la comanda "fusermount -u /directori/muntatge"
En el nostre cas seria:
root@seax2:~# sshfs entel@10.0.3.4:/home/entel /seax1manual/ -o allow_other,reconnect,IdentityFile=/root/.ssh/id_rsa

Evidència d'ús: 3-11.txt
Es pot veure l'execució de les comandes anteriors.
Podem veure que abans de l'execució de la comanda sshft, el fitxer de /seaxmanual estava buit, i després té el fitxer de laltre màquina en la seva carpeta.
I podem veure els fitxers intercanviats utilitzant el tcpdump.

Bibliografia: man ssh

- Lliura els resultats mitjançant Atenea (2 fitxers).
- Fitxer 1: Redactar l'informe de la pràctica p2_s1_cognom1_nom.txt.
- Fitxer 2: Realitzar les proves necessàries per justificar els resultats i encapsular els fitxers necessaris en el fitxer p2_s1_cognom1_nom.zip.
