**/etc/ssh/ssh\_host\_ecdsa\_key.pub**

File della chiave pubblica dell’utente

4. **Connettersi ad un pc:**

ssh testssh@indirizzo\_ip

**6. Verificare il funzionamento del comando “scp” (Secure Copy) creando un file sulla macchina locale e trasferendolo sulla macchina remota:**

sudo scp /home/5agr6/cane.txt testssh@indirizzo\_ip:/path/../..

**7. Mettere in atto le politiche di hardening per rendere più sicura la connessione SSH (tralasciate per ora l’autenticazione chiave pubblica/privata):**

* sudo nano /etc/ssh/sshd\_config
* disabilitare l'accesso tramite SSH come utente root: **PermitRootLogin no**
* limitare il numero di tentativi di accesso: **MaxAuthTries** **3**
* impostare il tempo a disposizione di un utente per completare l'autenticazione dopo la connessione iniziale al server SSH: **LoginGraceTime 20**

Impostando il numero a meno secondi, è vantaggioso contro attacchi Ddos

* Disabilitare l'autenticazione di password: **PasswordAuthentication no**
* Stessa cosa di prima ma con le password vuote: **PermitEmptyPasswords no**

https://www.digitalocean.com/community/tutorials/how-to-harden-openssh-on-ubuntu-20-04

**8. Configurate l’autenticazione a chiave pubblica/privata. Utilizzate il comando “ssh-copy-id” per installare sul server la chiave pubblica dell’utente:**

* skey-gen
* ssh-copy-id username@indirizzo\_ip

https://www.digitalocean.com/community/tutorials/how-to-configure-ssh-key-based-authentication-on-a-linux-server?authuser=1

**9. Reinstallate (prima apt purge, poi apt install SSH sulla macchina server) e verificate come viene gestita la richiesta di un client che già si connetteva al server di riconnettersi.**

**10. Fate in modo che solo 2 macchine remote possano collegarsi al vostro server SSH. Le macchine remote saranno specificate tramite indirizzo IP:**

* sudo nano /etc/ssh/sshd\_config
* implementare liste consentite di indirizzi IP utilizzando la direttiva di configurazione **AllowUsers**, che limita le autenticazioni degli utenti in base al nome utente e/o all'indirizzo IP

Limitare a solo due indirizzi IP: AllowUsers \*@10.0.3.6 \*@10.0.3.9

C’è un file chiamato “known che contiene tutte le chiavi pubbliche. Controllare le impronte digitali se sono giuste.

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!

Someone could be eavesdropping on you right now (man-in-the-middle attack)!

It is also possible that a host key has just been changed.

The fingerprint for the ECDSA key sent by the remote host is

SHA256:bLYX9VTS0MOSFfJCWrxOOsYY2GqoTOkAacr1QhFf2vI.

Please contact your system administrator.

Add correct host key in /home/testssh/.ssh/known\_hosts to get rid of this message.

Offending ECDSA key in /home/testssh/.ssh/known\_hosts:1

remove with:

ssh-keygen -f "/home/testssh/.ssh/known\_hosts" -R "10.0.3.4"

ECDSA host key for 10.0.3.4 has changed and you have requested strict checking.

Host key verification failed.