**WEB DEVELOPER**

**Linux Server**

**Docente: Wolfgang Cecchin**

**Titolo argomento: SSH, Secure Shell**

**SSH (Secure Shell)**

SSH è un servizio (ma anche un protocollo) che consente la comunicazione sicura via rete (sicura perché crittografata) tra un client e un server.

Attraverso SSH un utente può inviare comandi a un computer remoto.

Precedentemente per collegarsi alle macchine si utilizzava Telnet: servizio che è stato abbandonato, perché la comunicazione tra client e server avveniva in chiaro.

Approfondimenti:

<https://en.wikipedia.org/wiki/Secure_Shell>

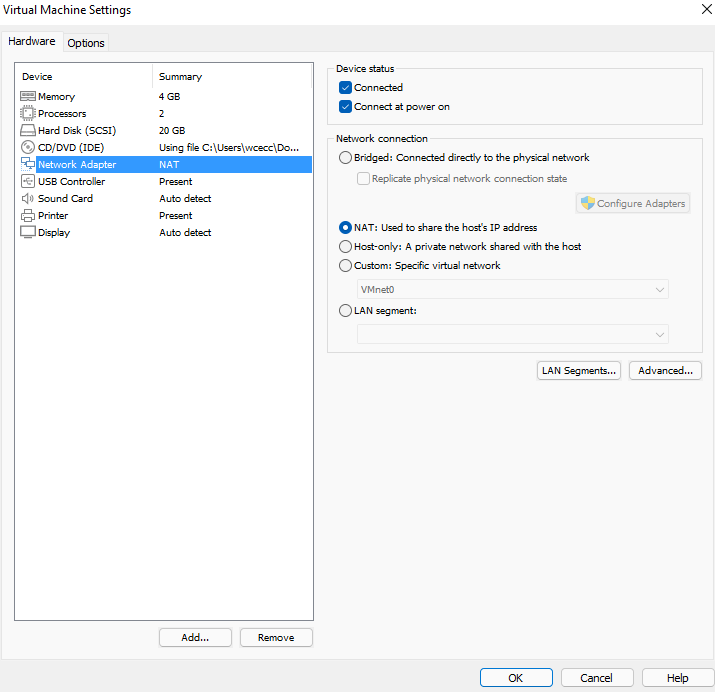
**Utilizziamo VM Workstation con NAT**

Per evitare di avere conflitti con altre macchine (e con la rete di ITS) utilizziamo VM Ware Workstation con NAT (“Network Address Translation”)

**Soluzione per Virtual Box:**

Utilizzare **scheda solo host,** eventualmente aggiungendo una seconda scheda.

<https://www.slideshare.net/powerhan96/networking-between-host-and-guest-v-ms-in-virtual-box>



**Installiamo su Debian il server SSH**

Aggiorniamo i repositories:

$ sudo apt update

$ sudo apt install openssh-server

Controlliamo di avere installato:

$ sudo systemctl status sshd

Controlliamo che sia in ascolto sulla porta 22:

$ netstat -tulpn | grep 22

Impostiamo il server SSH perché parta all’avvio:

$ sudo systemctl enable ssh

Nel caso in cui sia installato un firewall, dobbiamo consentire l’ingresso per ssh:  
  
$ sudo ufw allow ssh

Il file di configurazione di ssh si trova all’interno di /etc

Attenzione:

/etc/ssh/ssh\_config 🡪 è il file di configurazione del client ssh del sistema

/etc/ssh/ssh**d**\_config 🡪 è il file di configurazione del server ssh

Invece:

/etc/ssh/ssh\_config**.d** 🡪 è una directory. Vengono includi tutti i files di configurazione del client ssh del sistema

/etc/ssh/ssh**d**\_config**.d** 🡪 è una directory. Vengono includi tutti i files di configurazione del server ssh del sistema

A noi, se vogliamo modificare le configurazioni di ssh, interessa modificare il file:  
/etc/ssh**d**\_config

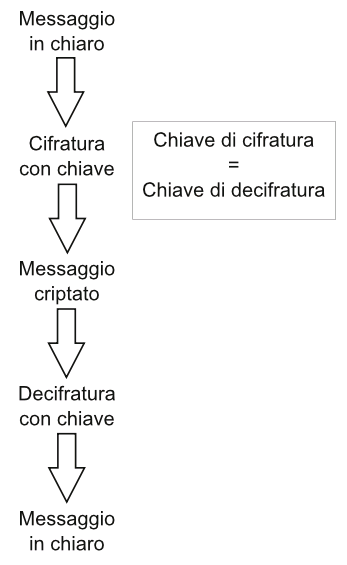
Individiuamo l’IP della macchina

$ hostname -I

Dalla macchina Windows (cioè la macchina host) possiamo utilizzare un client ssh per connettersi alla macchina:  
  
$ ssh its-user@ip-della-macchina-guest

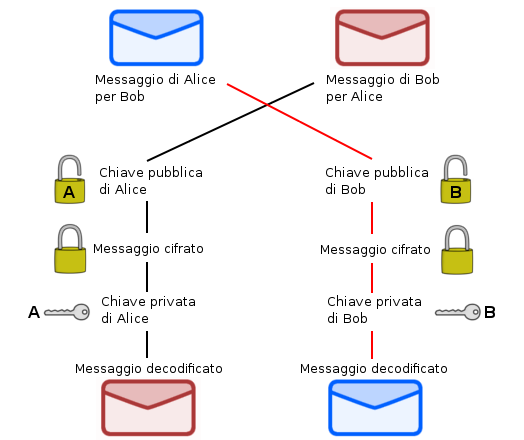
**Crittografia simmetrica**

<https://it.wikipedia.org/wiki/Crittografia_simmetrica>



**Crittografia asimmetrica**

<https://it.wikipedia.org/wiki/Crittografia_asimmetrica>



**Connessione tramite SSH**

SSH utilizza **crittografia simmetrica** per crittografare la connessione tra client e server. La crittografia del canale in modalità asimmetrica sarebbe troppo onerosa (troppo lenta) a livello di calcolo.

Tuttavia **la fase di autentificazione** può avvenire attraverso crittografia asimmetrica e chiave pubblica.

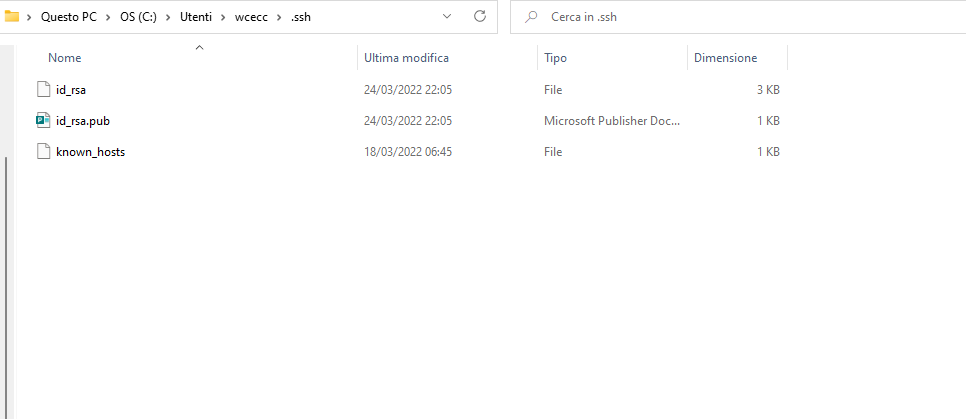
Nella powershell di Windows generiamo una coppia di chiavi pubblica/privata (non specificando nulla verrà usato l’algoritmo RSA):

> ssh-keygen

Immagine che contiene testo

Descrizione generata automaticamente

Nella home dell’utente è stata creata una cartella .ssh con le chiavi pubbliche e private.



In Debian andiamo a copiare la chiave pubblica nella cartella

/root/.ssh

Ci sono molti modi per farlo, ad esempio da Windows:  
  
> scp .\id\_rsa.pub [its-user@192.168.206.128:/home/its-user](mailto:its-user@192.168.206.128:/home/its-user)

> ssh [its-user@192.168.206.128](mailto:its-user@192.168.206.128)

E poi nella macchina Debian:

$ cat id\_rsa.pub >> ~/.ssh/authorized\_keys

Il contenuto del file **authorizes\_keys** è una lista di chiavi pubbliche:

Immagine che contiene testo

Descrizione generata automaticamente