SSH

Topics Covered

Command to log into from your personal liniux based OS to the lab machine:

1. ssh into seis: `ssh <USERNAME>@seis.bris.ac.uk` Seis is a proxy server that allows you to connect to a private network via the internet
2. seis to lab-machine: `ssh rd-mvb-linuxlab.bristol.ac.uk` This allows you to connect to a local lab machine that is currently running.

Setting up SSH Keys

- The keys that SSH uses cimes as pairs of files :
  - A private key called id_CIPHER
  - A public key in a file called id_CIPHER.pub, where the .pub stands for public
- Both keys need a copy, the private key should be stores somehere only you have access to and the public key can be stored in the File system in the lab machines and seis.

Creating a Key Pair:

- To generate a key; `ssh-keygen -t ed25519`. The ed25519 is a method of creating a key signature. Basically gets unique key signature in 128 bits of data. The -t flag tells the ssh program to use the ed25519 crypographic method to generate the key

▼ Where the key is stored on m local machine (Mac Desktop)

(/Users/admin/.ssh/id_ed25519)

- Using this we have not creatd two keys, one private and one public and stored them on our local machine. The hosts that we have already got access to are stored in the knownhosts file in the ./ssh directory
- Think of the key pairs as a contract. The paper is the machine you want access to, the pubic key is the dotted line and the private key is the unique siganture giving you access to the contract. Whnever you want to access via ssh using keys, the ssh on the host machines send a challange to your local machines which is filled by your private key signature, this is then sent back to the host machine for verfication.

Setting up Key Access on SSH : Uplaoding public key to seis

- Now that we have our public key we need to copy it across to seis to allow seis to have acces to the key thus allowing us to log into seis without needing a password everytime.
- There needs to be a /.seis folder on seis, if there is not one make one via the command `mkdir ~./ssh`
- Now we need to copy the public key from the local compute to the seis /.ssh folder :

`scp ~/.ssh/id_ed25519.pub "` `USERNAME@seis.bris.ac.uk` `:~/.ssh/"`

- note the command is similiar to the cp command on linux but you are using scp to copy a file between hosts. in this case we are copying the public key from our local computer to the seis host machine
- The double quotation marks are to stop our machines expanding the `~` character
- The `:` is to specify a specific directory on the host machine are copying the file to
- The final step is to copy the public key in seis into a file called **authorized_keys**
- If we do `cat id_25519.pub >> authorized_keys` This will append the authorized keys file (if it already exists), or create one if it did not

- Now to change the permissions of the authorized keys folder using chmod:
  `chmod 600 authorized_keys`

To preform a action on the Host machine after shell:

```
$ ssh -t lab "cd Desktop/ #<or any other command># && exec $SHEl
```

- This will force a command prompt to open up in the Host machine after executing the ssh action

Setting up Key Access on SSH : Uplaoding public key to lab machine

- To log into seis withouht needing a passoword, you had a private key on your local machines and a public key on the seis machine
- Logically then it would make sense to connect seis to the lab machine without needing a password you need to have a private key on seis and a public key on the lab machined
- However we do not want to upload our private key onto seis for secrutiy reasons.
- SSH has a feature called agent forwarding that will allow you to ssh into one machine and ssh into another from there. The way we do this is using the - A flag.
-