Step by step guide for settings up a simple networked project

Used software:

- Oracle Virtualbox
- Putty
- Ubuntu 20.04-live-server-amd64

Setting up the virtual machine

1. Download Oracle VirtualBox and install it
2. Create new virtual machine (CTRL+N)
3. Give it a name and a desired destination folder
4. Choose which type and which version
    a. Type: Linux
    b. Version: Ubuntu 64Bit
5. Choose RAM
6. Create disk space
7. Choose default data type VDI (VirutalBox Disk Image)
8. Choose dynamic allocation
9. Choose how the size of the virtual disk
10. Launch newly created virtual machine
11. It will ask for a medium -> choose your Distribution (Ubuntu server)
12. Server setup starting…
13. Choose desired language
14. If you have a older version of the installer choose update, else continue the setup process
15. Choose keyboard layout
16. Set up network connections, here you have to wait for short period of time. After that you will have the option “Done” on the bottom to continue the setup process
17. Leave “Proxy address” blank
18. Leave “Mirror address” by default
19. Leave “Guided storage configuration” by default
20. Leave “Storage configuration“ as it is and proceed
21. After that it will ask you to confirm the destructive action. Hit “Continue”
22. Set up your profile
23. In “SSH Setup” choose “Install OpenSSH server” and leave “Import SSH identity” by default (“No”)
24. Choose “Featured Server Snaps”. (I like to choose powershell, wormhole and keepalived. This is optional!)
25. Server starts installing the system…
26. After it is finish press “Reboot”
27. Log into the server with the username and the password
28. Check if ssh server is running by typing *sudo systemctl status ssh*
29. If it is does not say “running” then type *sudo service ssh start*
30. Type *sudo ufw allow ssh* to allow ssh for the firewall
31. Type *sudo apt install net-tools* for helping purpose. With *ifconfig -a* you can see the ip address of the server
32. Type *sudo nano /etc/ssh/sshd_config* and find “#Port 22” and “PubkeyAuthentication Yes” and uncomment both. Here you can change the port (be careful which port you choose, because it might have a different purpose)
33. Type *sudo service ssh restart*

34. Open the VirutalBox Settings and go to “Network”
35. Add a new NAT-Netwerk
36. Edit the new NAT-Network and click on “port forwarding”
37. Add a new rule
    a. Host: (the ip address of your pc)
    b. Host-Port: (you can choose, for example 2222)
    c. Guest: (the ip address of the server)
    d. Guest-Port: (the port you’ve changed perviously)
38. Shutdown the server
39. In the VirtualBox Manager click on the virtual machine and select “network” on the right
40. The option “connected to” has to be “nat-network” and then choose the NAT-Network you previously created
41. Open putty.exe and enter the ip address and the port of the host you previously defined in the rules
42. Check connection type “SSH” and press “open”
43. Putty client will connect to the ssh server and you will have to enter the username and the password to access

Public key authentification

1. Open PuttyGen and generate a key
2. Give it a password for safety reasons. This password is stored localy and won’t be sent, hence it’s safe against network sniffing!
3. Safe the private and public key on your local pc.
4. Start putty.exe and log onto the ssh server via username and password
5. Create a directory with *mkdir .ssh*
6. Create a file with the authorized keys *vi .ssh/authorized_keys*
7. Copy the public key
8. Go back to your putty client, press “i” and paste it into the terminal editor via right mouse click
9. To safe the changes press “esc” and then type *:wq*
10. Type in the client *sudo nano /etc/ssh/sshd_config*
11. Search for “#PubkeyAuthentication Yes” and uncomment it
12. Search for “#PasswordAuthentication Yes”, uncomment it and replace “Yes” with “No”
13. Type in the client *service ssh restart*
14. Type in the client *exit*
15. Open putty.exe and type in the host ip addresse and the port
16. Under “Saved Sessions” give your connection a name and head to the catogories
17. In “Xatorgories -> Connection -> SSH -> Auth” you will find “Private key file for authentication:”, here you have to choose the private key you saved earlier
18. After that, head back to the category “Sesssion” and save the session
19. Click on the saved session and it will open up the client and it will connect to the server

After that you will be asked for a username and the public key password. Don’t worry this password is local and won’t be send through the network. It prevents traffic sniffing and adds an additional layer for safety reasons.