Born2BeRoot Guide

This guide has 8 Parts:

- Part 1 - Downloading Your Virtual Machine
- Part 2 - Installing Your Virtual Machine
- Part 3 - Starting Your Virtual Machine
- Part 4 - Configurating Your Virtual Machine
- Part 5 - Connecting to SSH
- Part 6 - Continue Configurating Your Virtual Machine
- Part 7 - Signature.txt
- Part 8 - Your Born2BeRoot Defence Evaluation with Answers

Part 1 - Downloading Your Virtual Machine

1. Click on this link **https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/**
2. Scroll to the bottom of the website and click `debian-11.3.0-amd64-netinst.iso` (3rd from the bottom), if that doesn't work, then you can try either `debian-edu-11.3.0-amd64-netinst.iso` or `debian-mac-11.3.0-amd64-netinst.iso`

Part 1.1 - Sgoingfre (Only 42 Adelaide Students)

1. Head over to iTerm2

```
lread@F2N057 ~ % ls
Cleaner_42.sh   Downloads       Music           sgoinfre
Desktop         Library         Pictures
Documents       Movies          goinfre
lread@F2N057 ~ %
```

1. Then type `cd sgoinfre/students`

```
lread@F2N057 ~ % cd sgoinfre
lread@F2N057 sgoinfre % ls
lost+found      students
lread@F2N057 sgoinfre % cd students
lread@F2N057 students % ls
lread
lread@F2N057 students %
```

1. Then type `mkdir <your intra username>`

```
lread@F2N057 students % mkdir lread
```

1. Then type `chmod 700 <your intra username>`

```
laread@iMac-2 students % chmod 700 lread
laread@iMac-2 students %
```

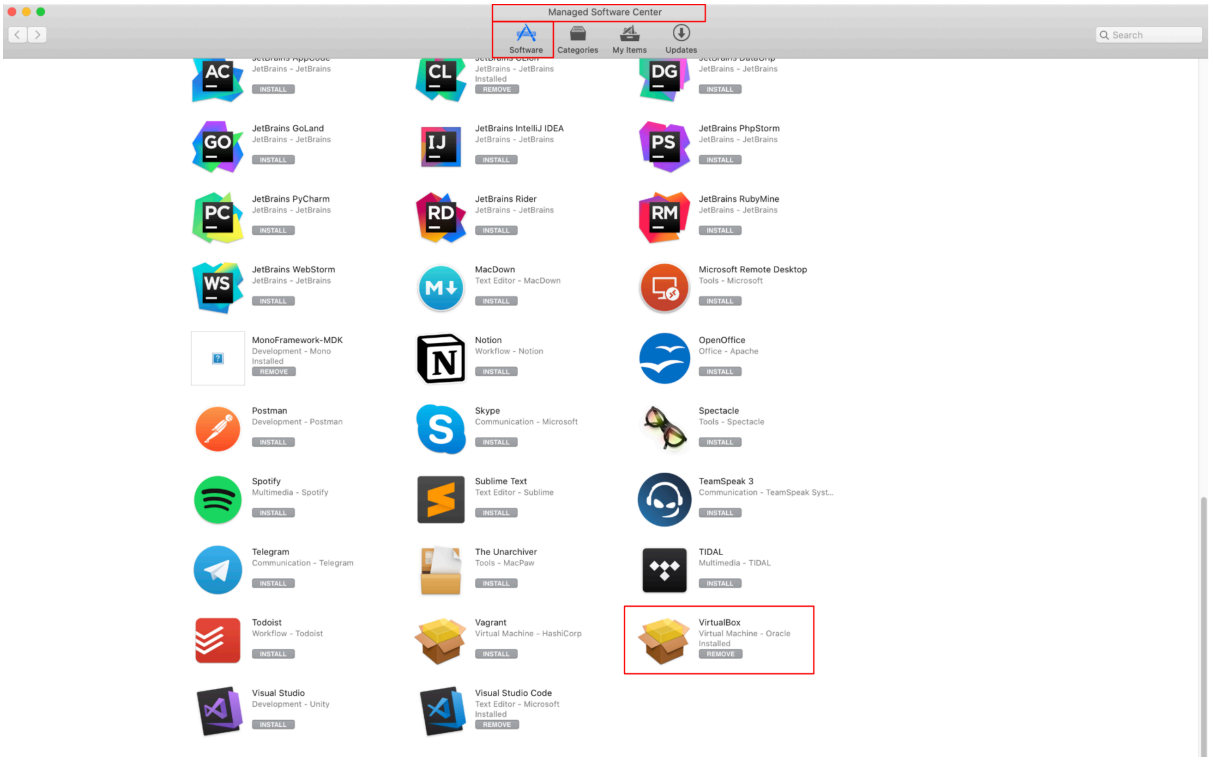
1. Find your Debian Download from Part 1 - Downloading Your Virtual Machine and put that download in this sgoinfre folder that you have just created.

Part 1.2 - Virtual Box

Now head over to Virtual Box to continue on.

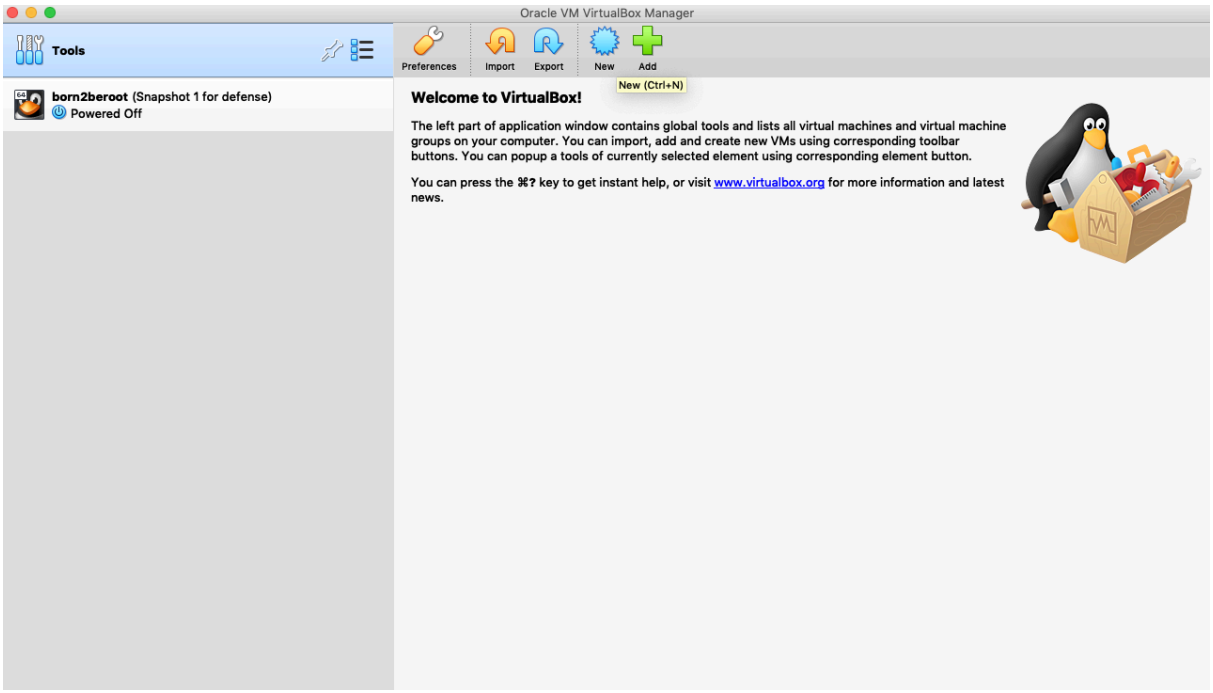
Don't have Virtual Box Installed?

Download it from Managed Software Center on an Apple Computer/Laptop.

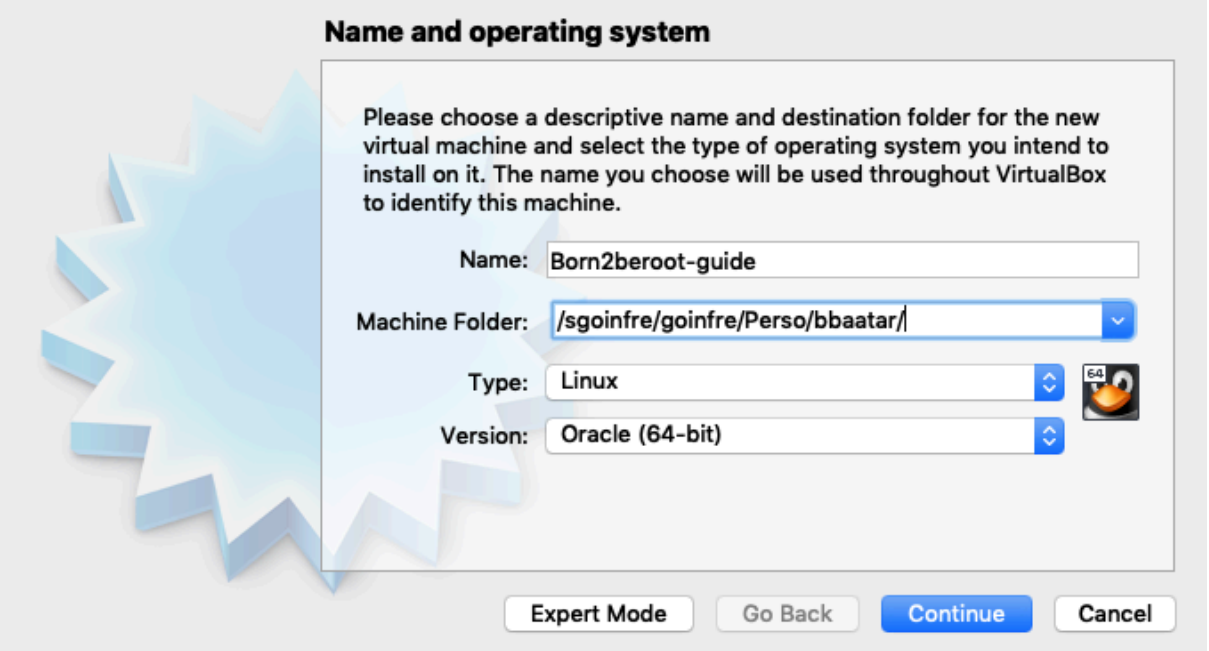


Part 2 - Installing Your Virtual Machine

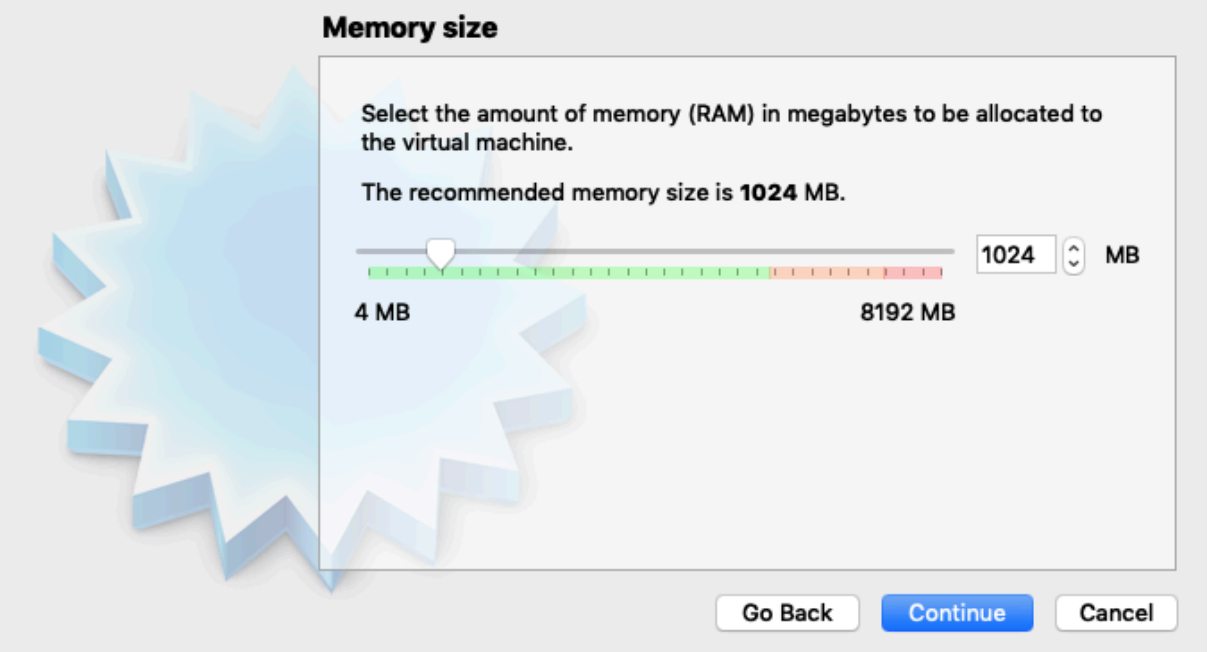
1. Click on `New`



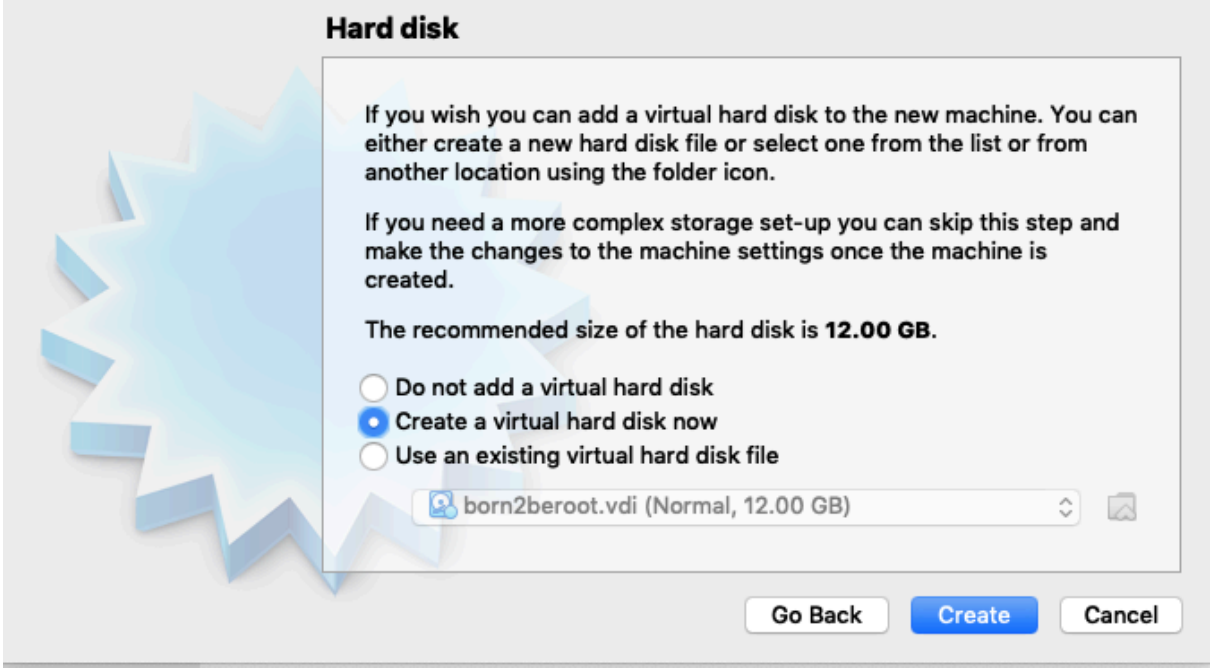
1. Change Machine Folder to `sgoinfre/students/your_intra_login/Virtual Machine Name` and then click `continue` to move to the next step.



1. Set Memory Size as `1024 MB` and click continue.

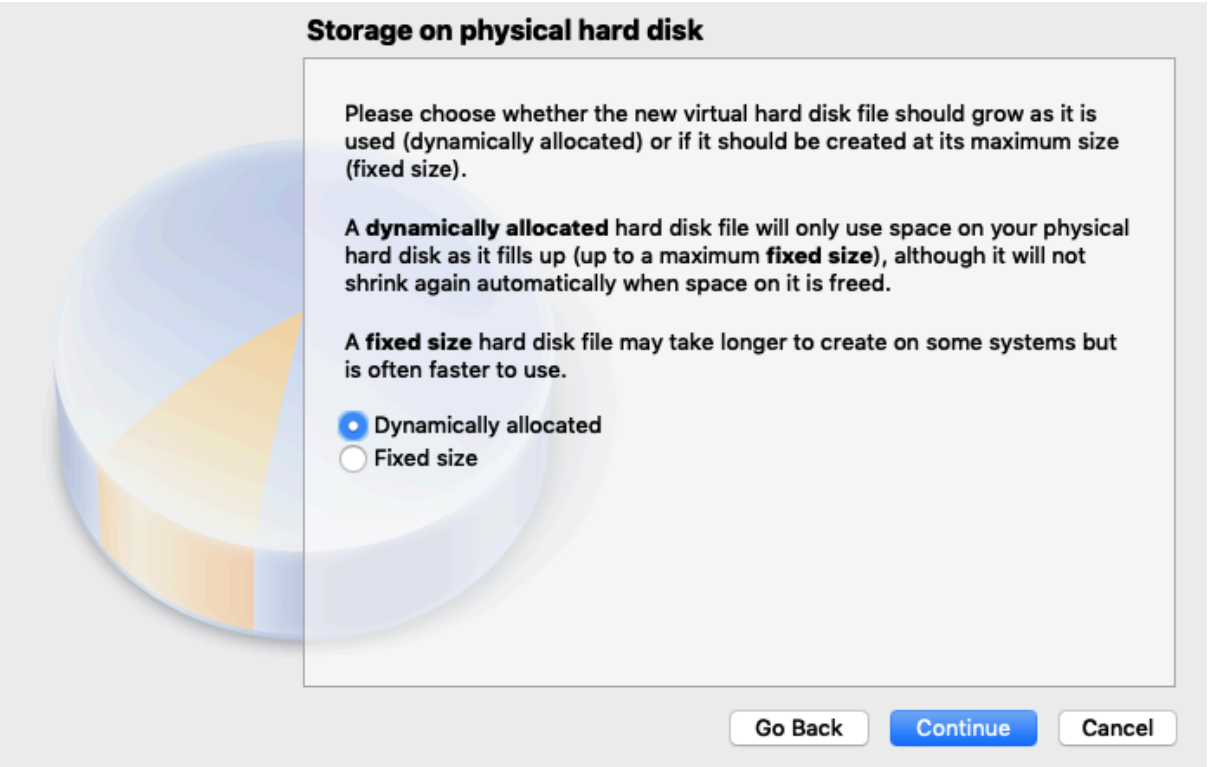


1. Click `Create a Virtual Hard Disk Now` and then click `Create` to create the Hard Disk.

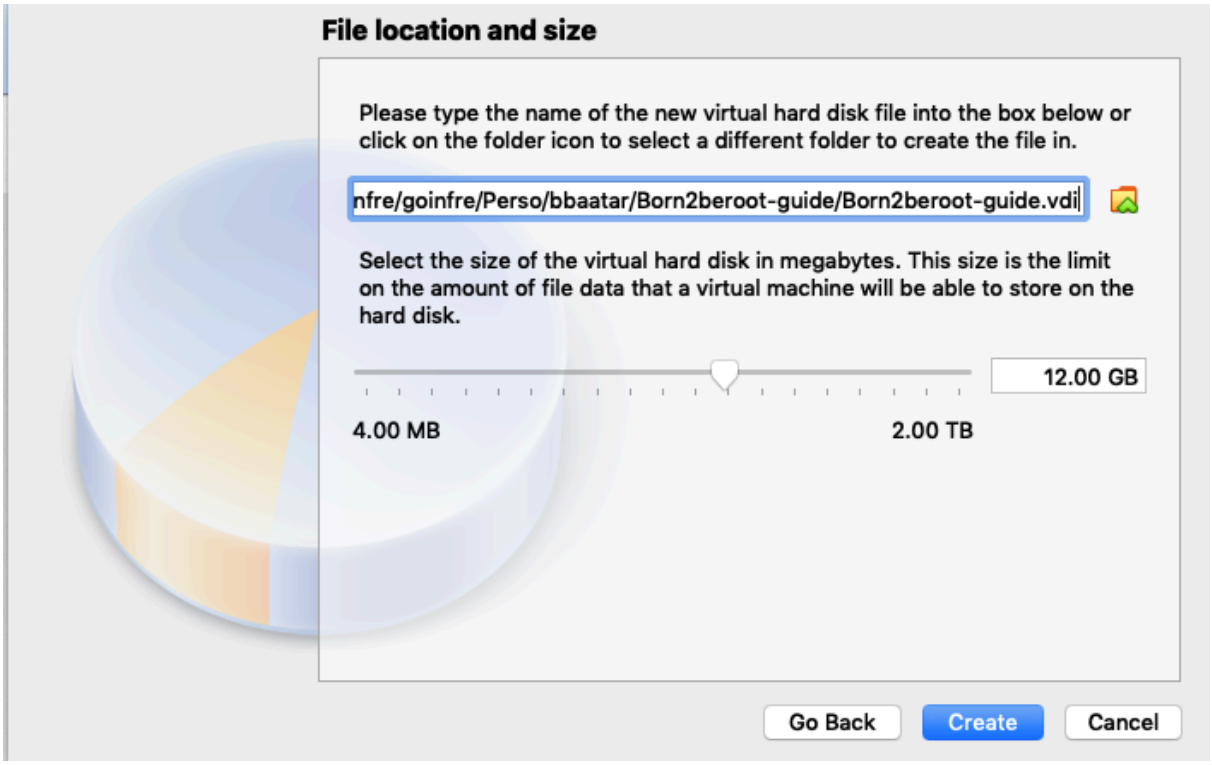


1. Click `VDI (VirtualBox Disk Image)` and then click `Continue` to select VDI.

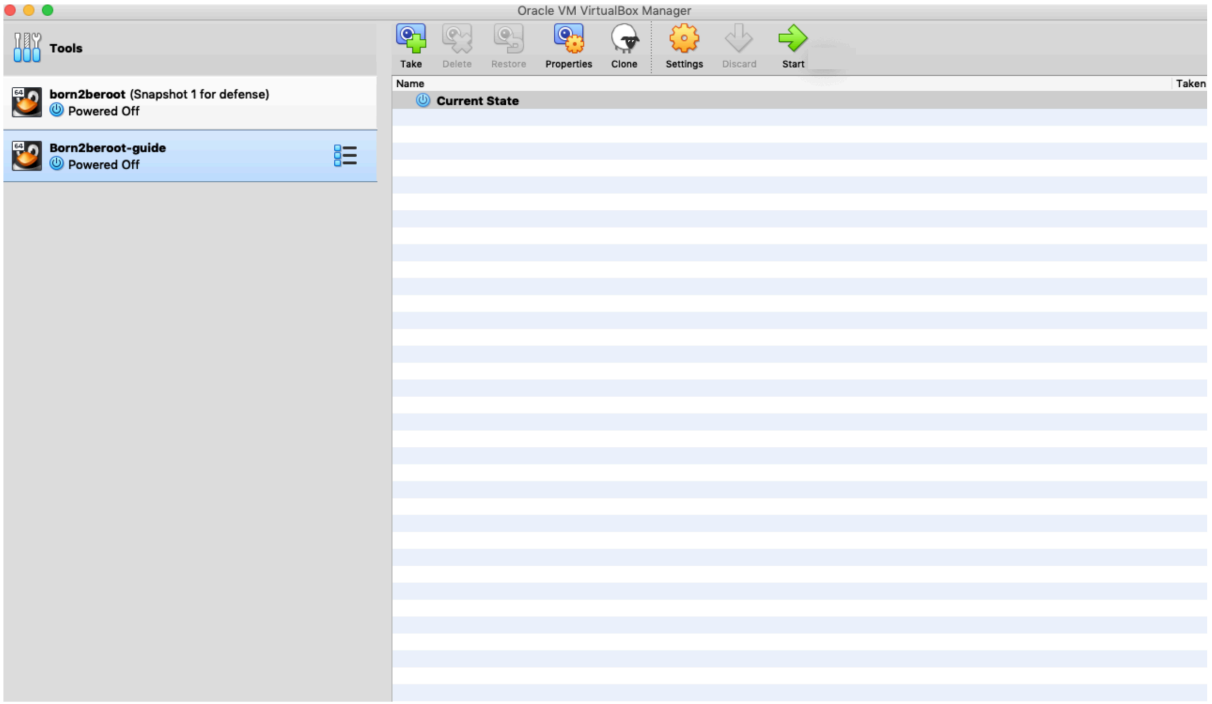
1. Click `Dyamically Allocated` and then click `Continue` to only use space on your Hard Disk.



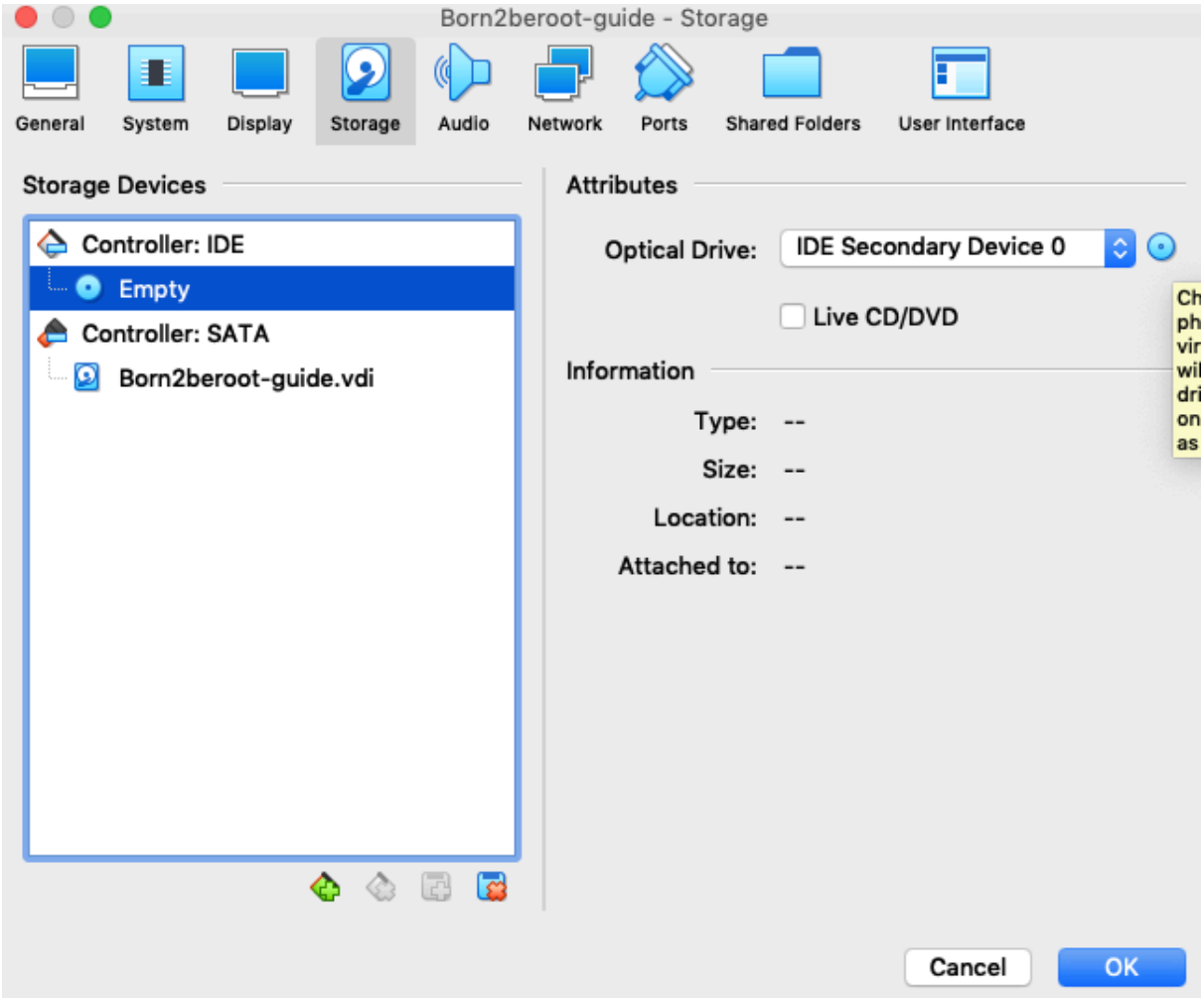
1. Set Size as `12.00 GB` and then click `Continue` this should be enough for this project.



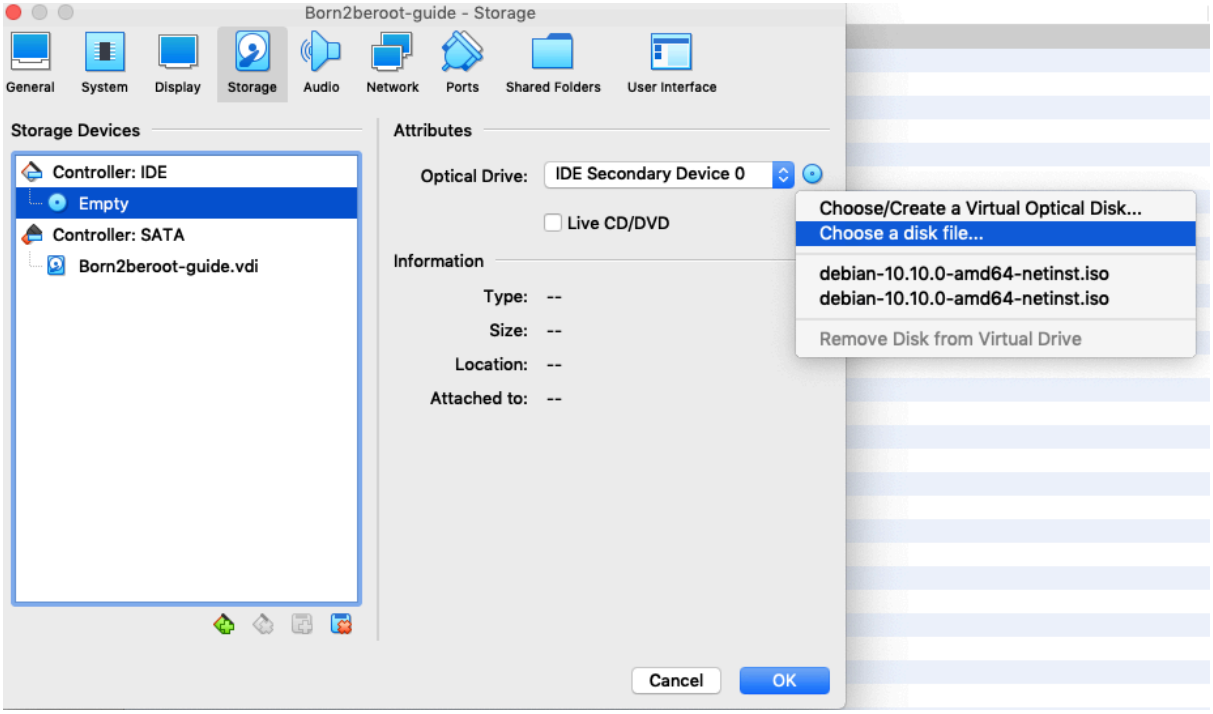
1. Click `Settings` and then click `Storage` to view your Virtual Machine Storage.



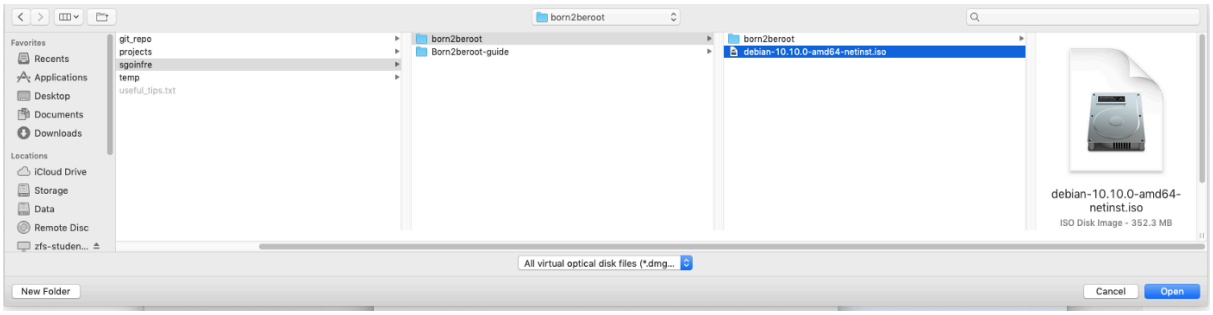
1. Click on `Optical Drive` (Optical Drive - far right blue small box).



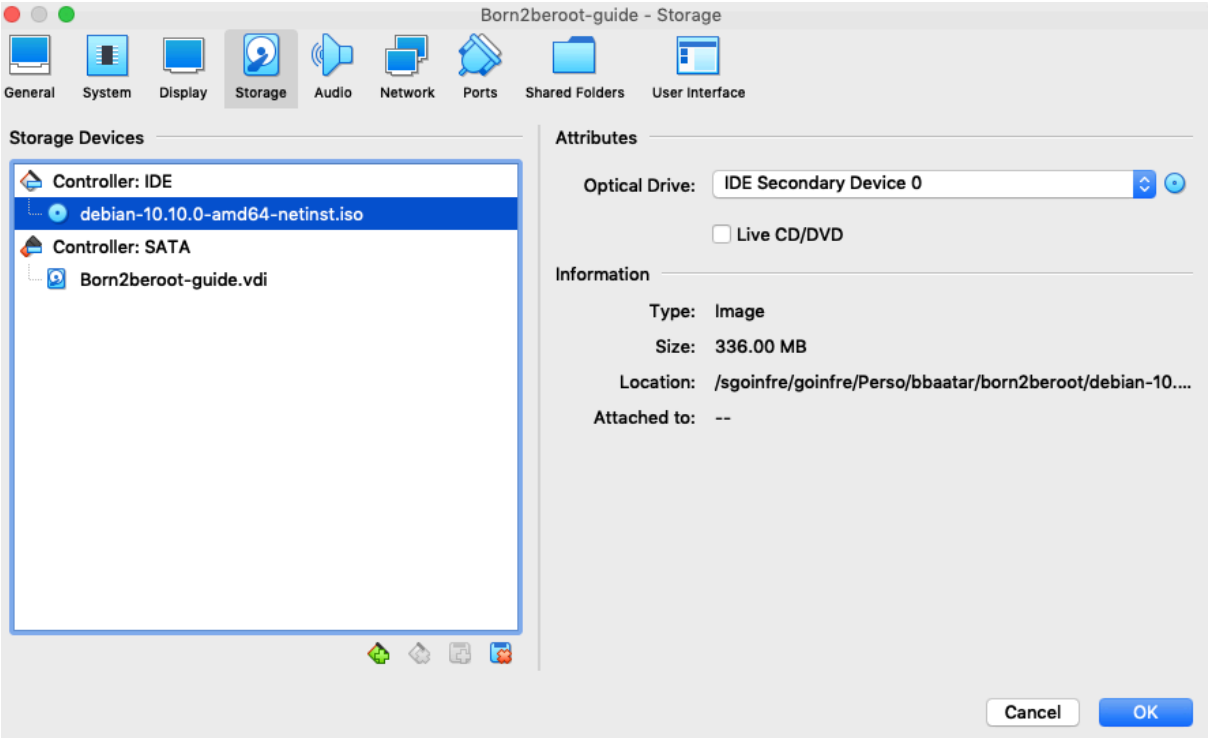
1. Click on `Choose a disk file...` (2nd option in the drop down).



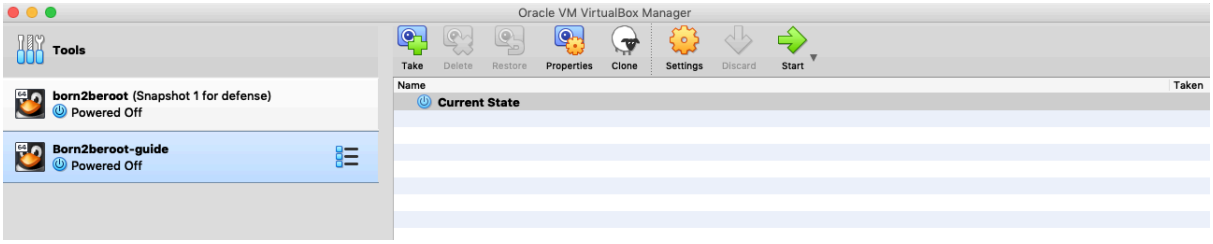
1. Then click on the Virtual Machine file (.iso).



1. Click on your `Virtual Machine` and then click `'ok` to confirm you Virtual Machine Storage.



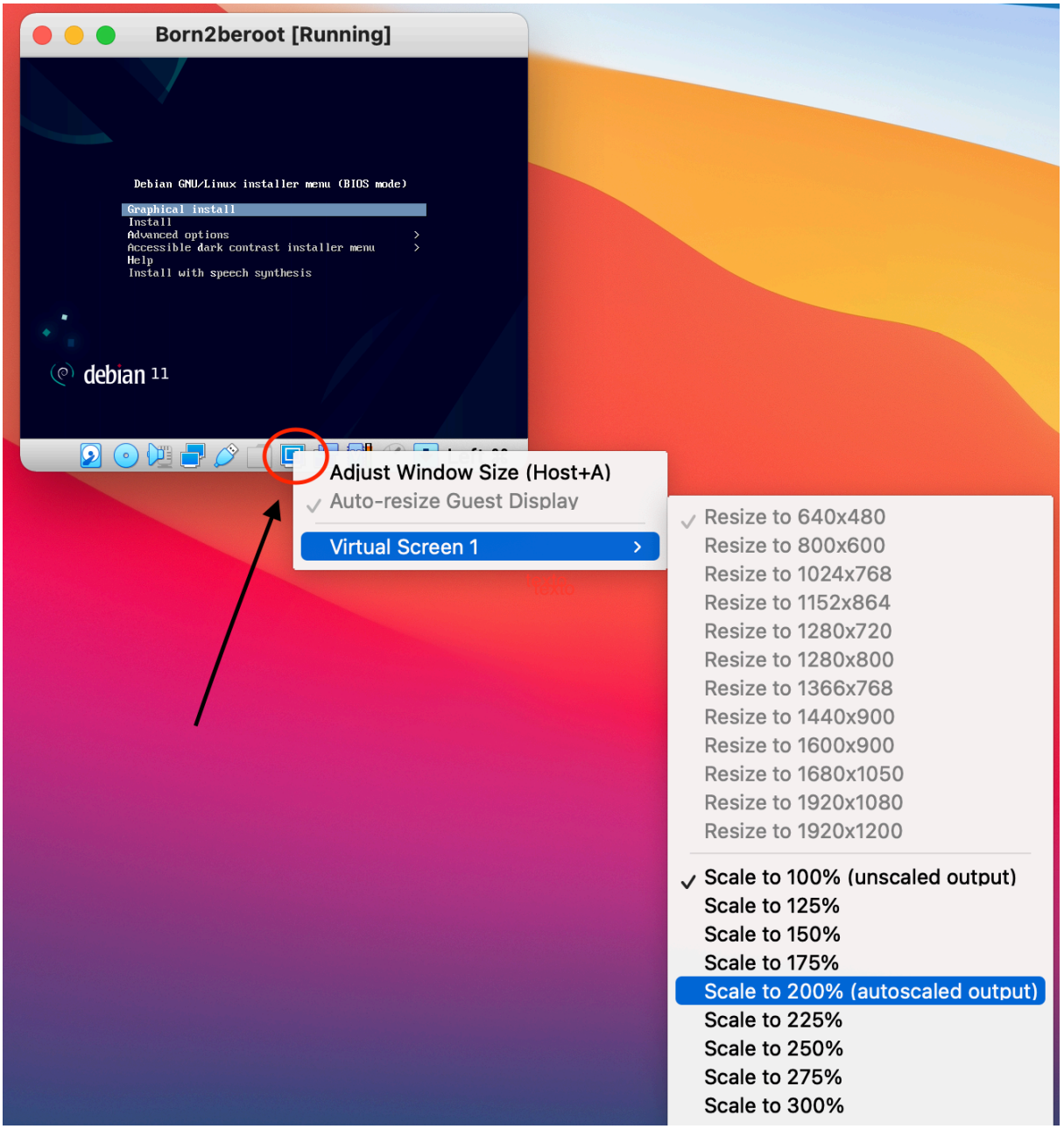
1. Click `Start` (The Green Arrow ➡️) to start your Virtual Machine.



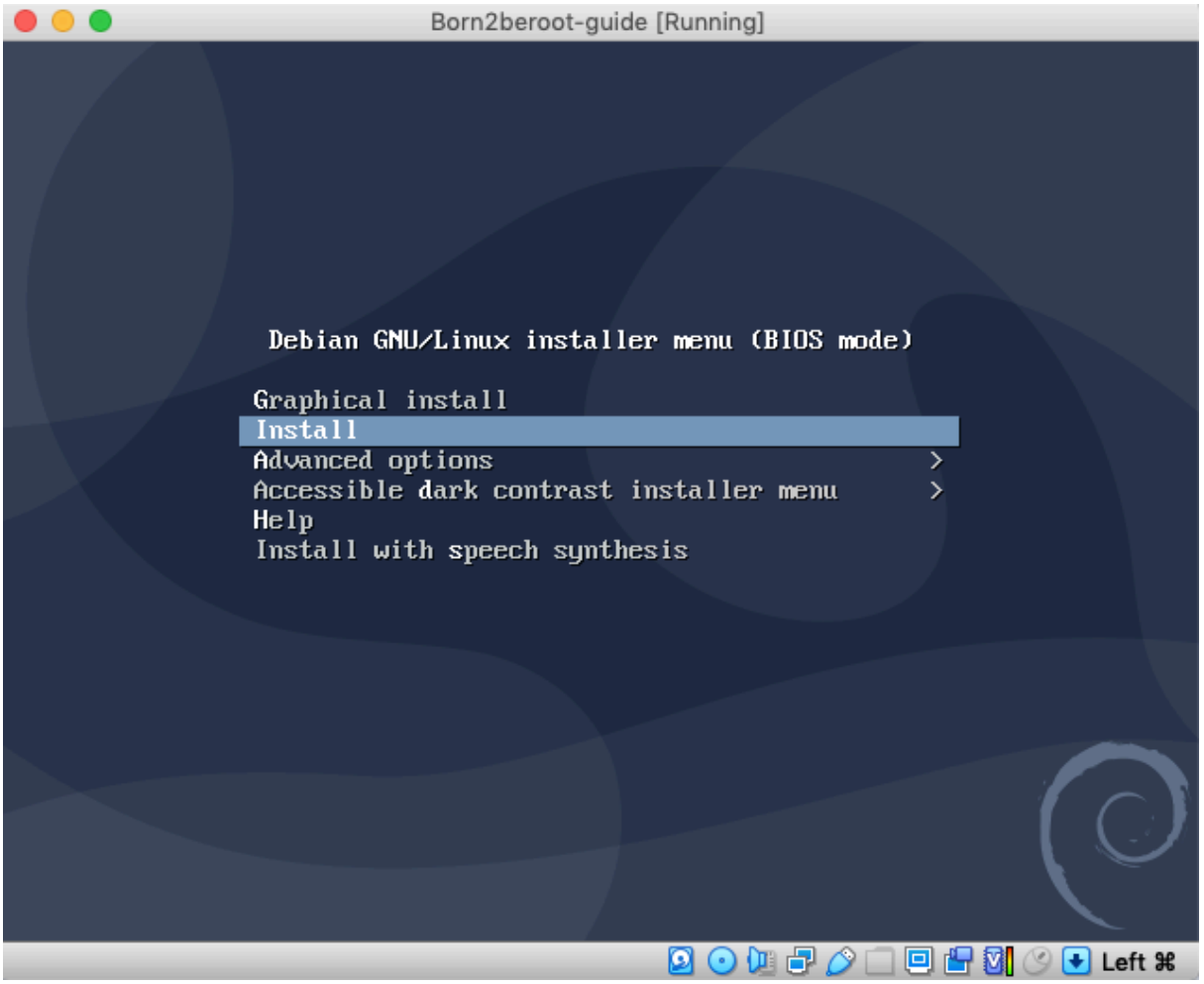
Part 3 - Accessing Your Virtual Machine

In the Virtual Machine, you will not have access to your mouse and will only use your Keyboard to operate your Virtual Machine.

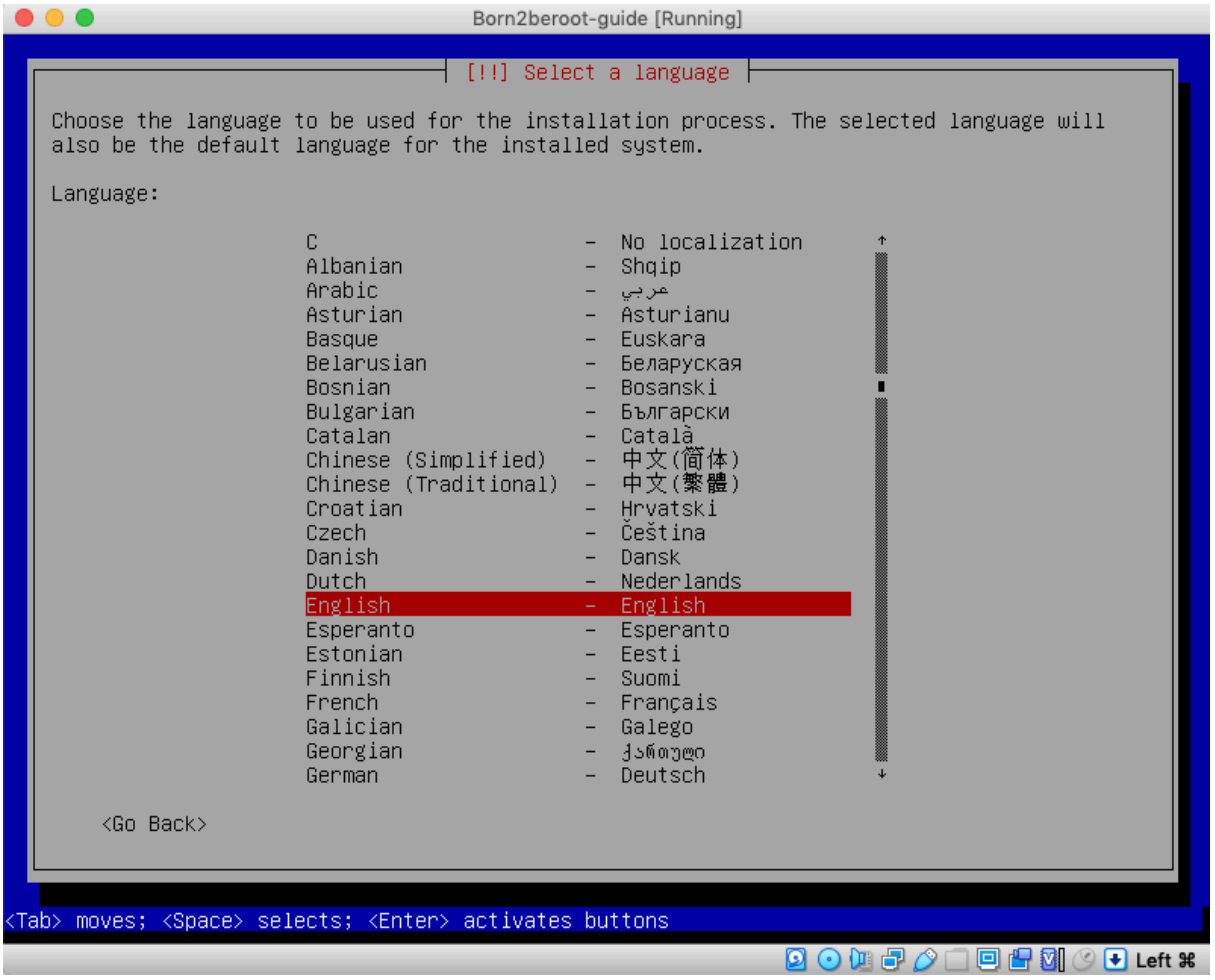
1. To increase your Virtual Machine size, press `command` + `c` on your Apple Keyboard at the same time and then use your mouse to drag the screen to the size you wish or do the following:



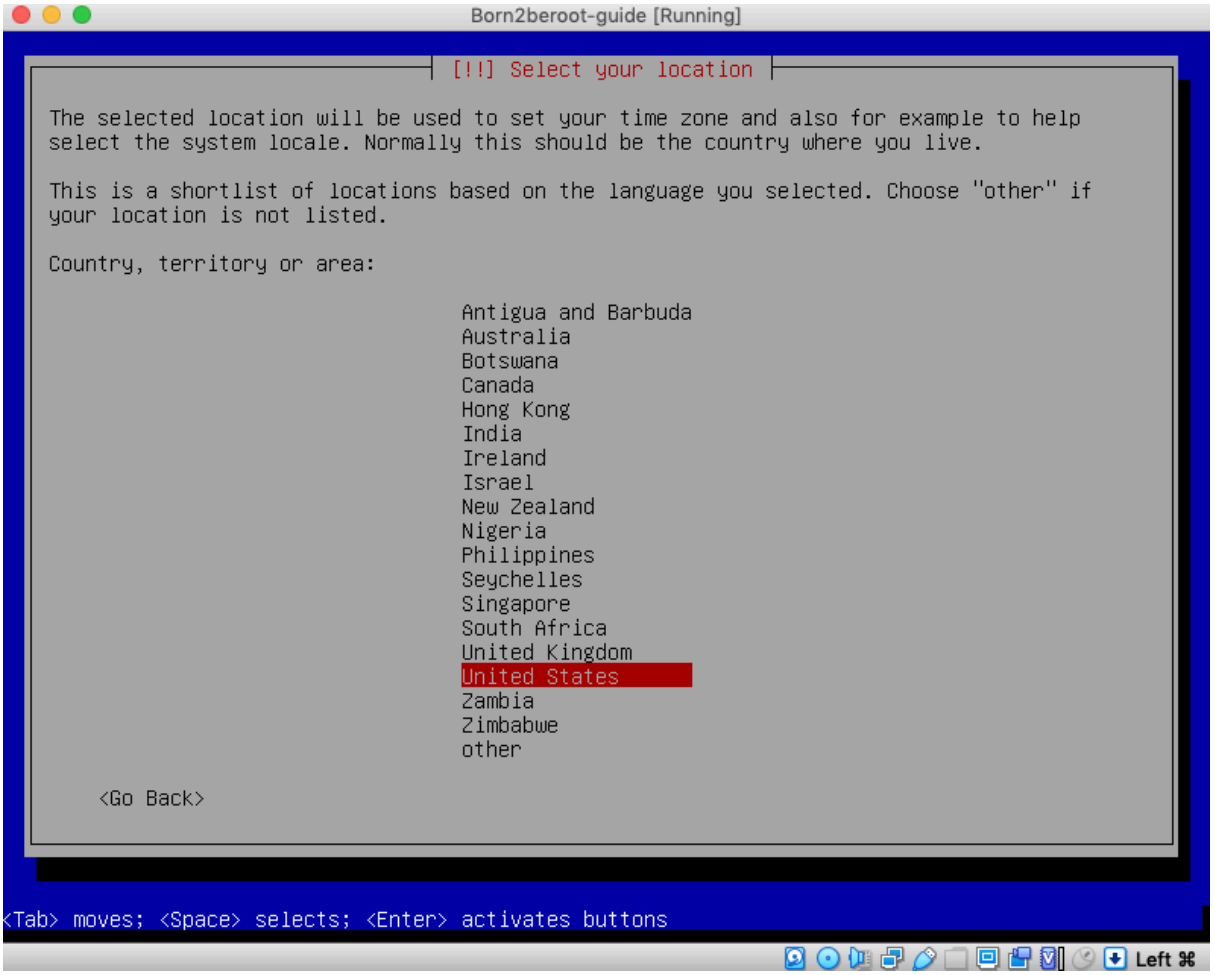
1. Use the arrow keys on your keyboard 🔼🔽 and press `Enter` on `Install` (This will start the installation proccess).



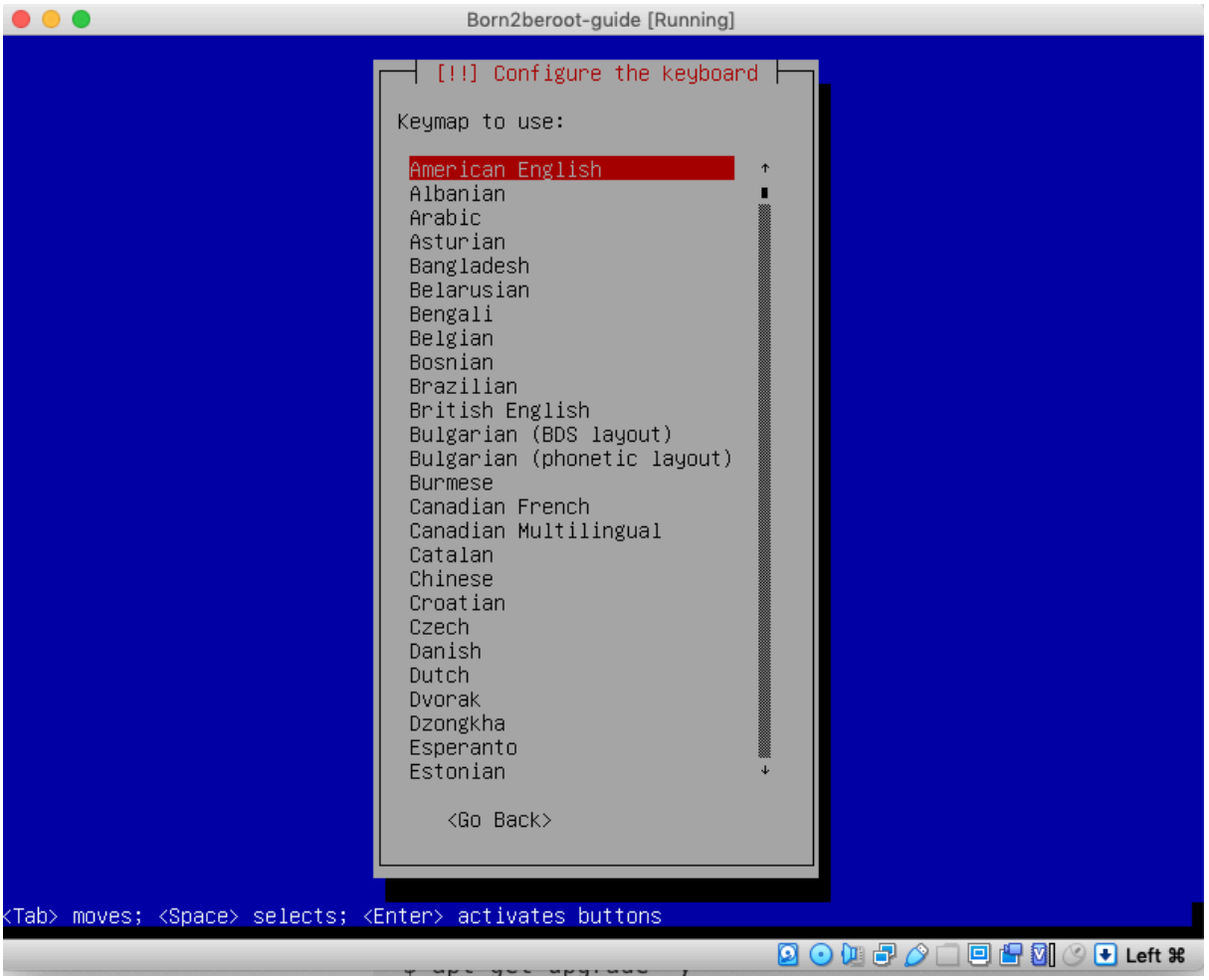
1. Press `enter` on `English - English` or your language of preference.



1. Press enter on Australia or the country your installing this Virtual Machine.

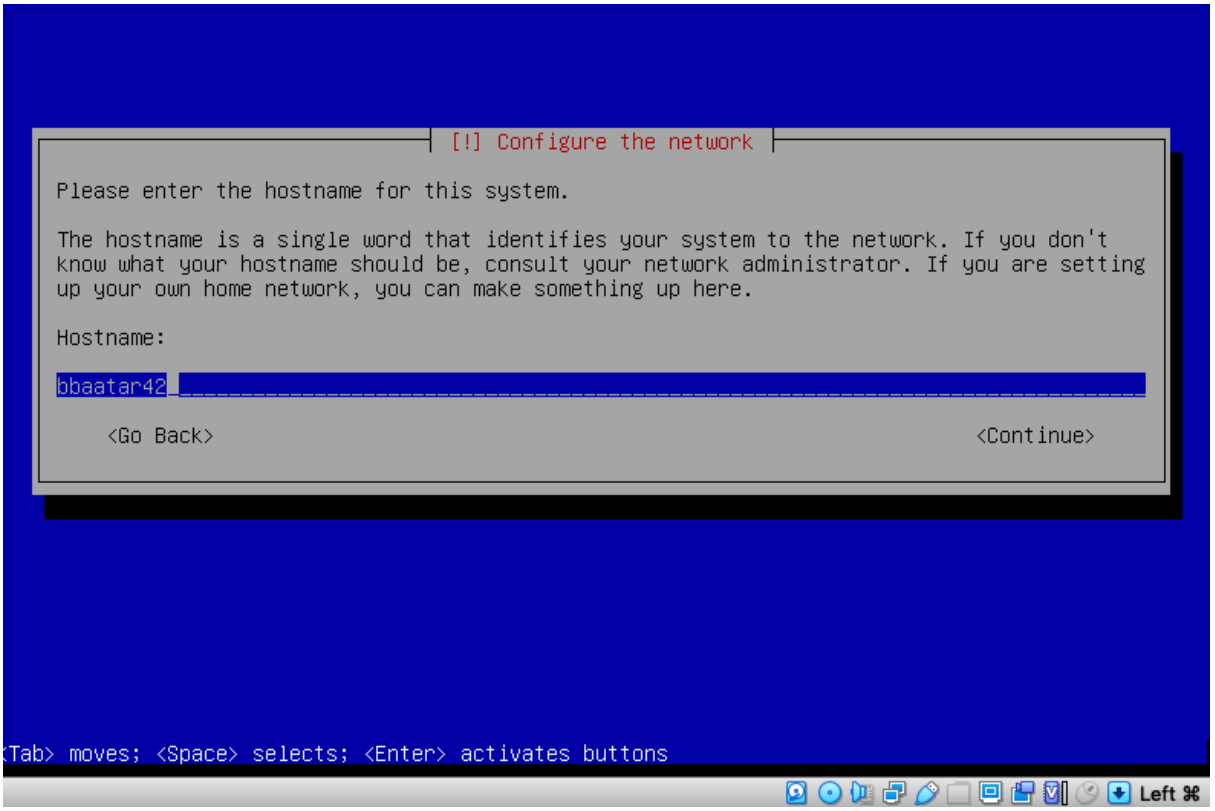


1. Press `enter` on `American English` or your keyboard of preference.

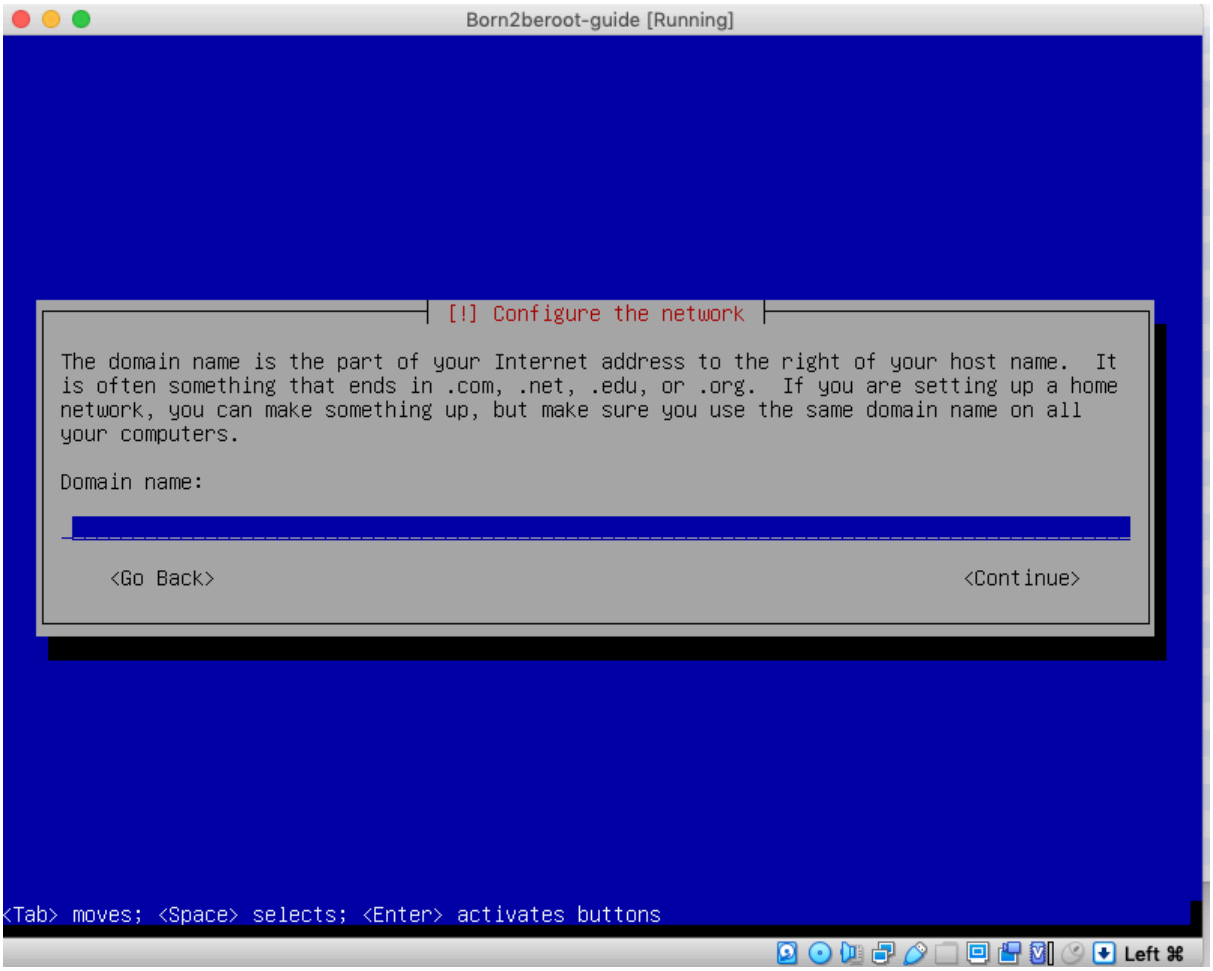


⚠️ NOTE: Whenever you are told to create a password, use the same password as everything.

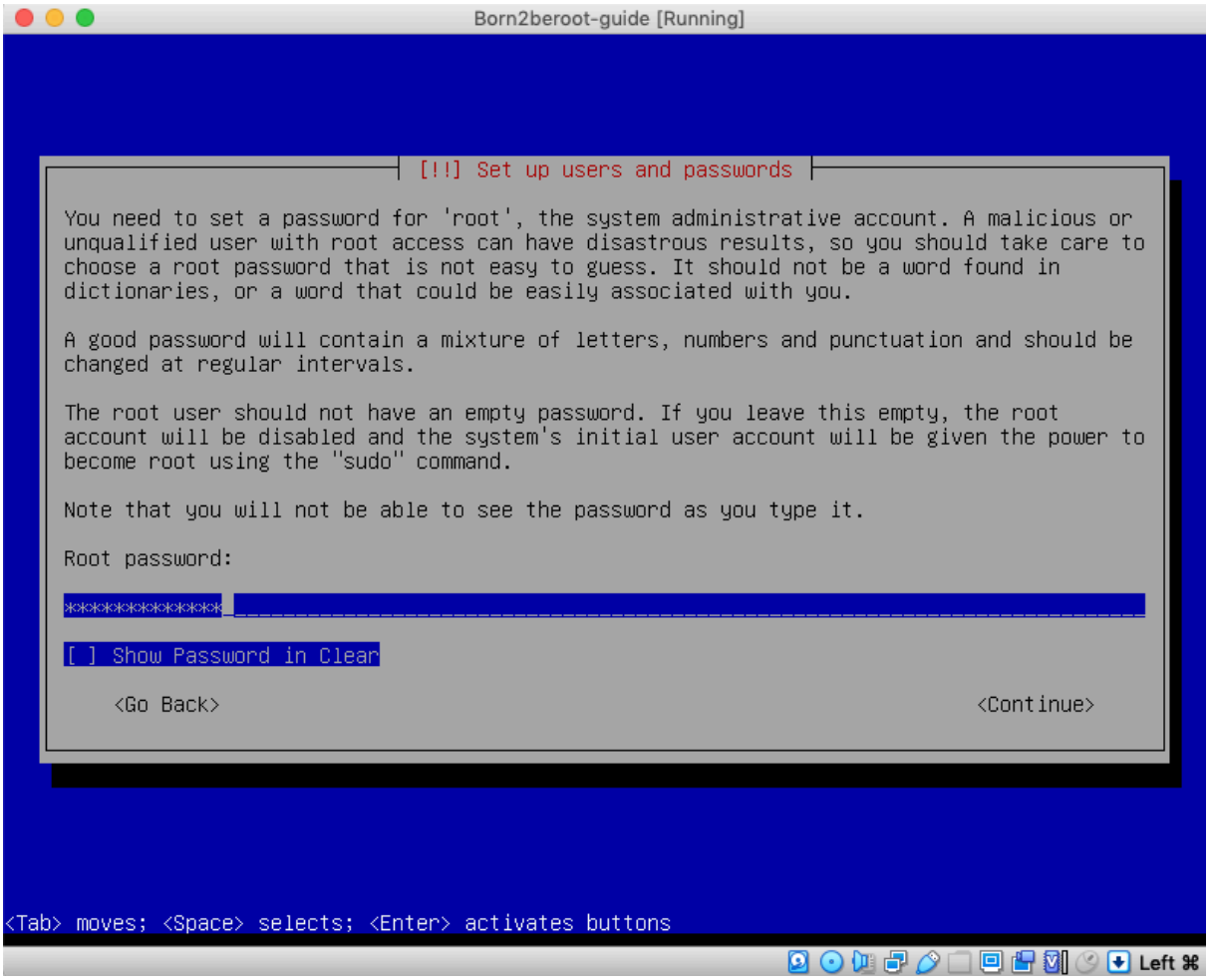
1. Create a Host Name as your login, with 42 at the end (eg. prossi42) - write down your Host Name, as you will need this later on.



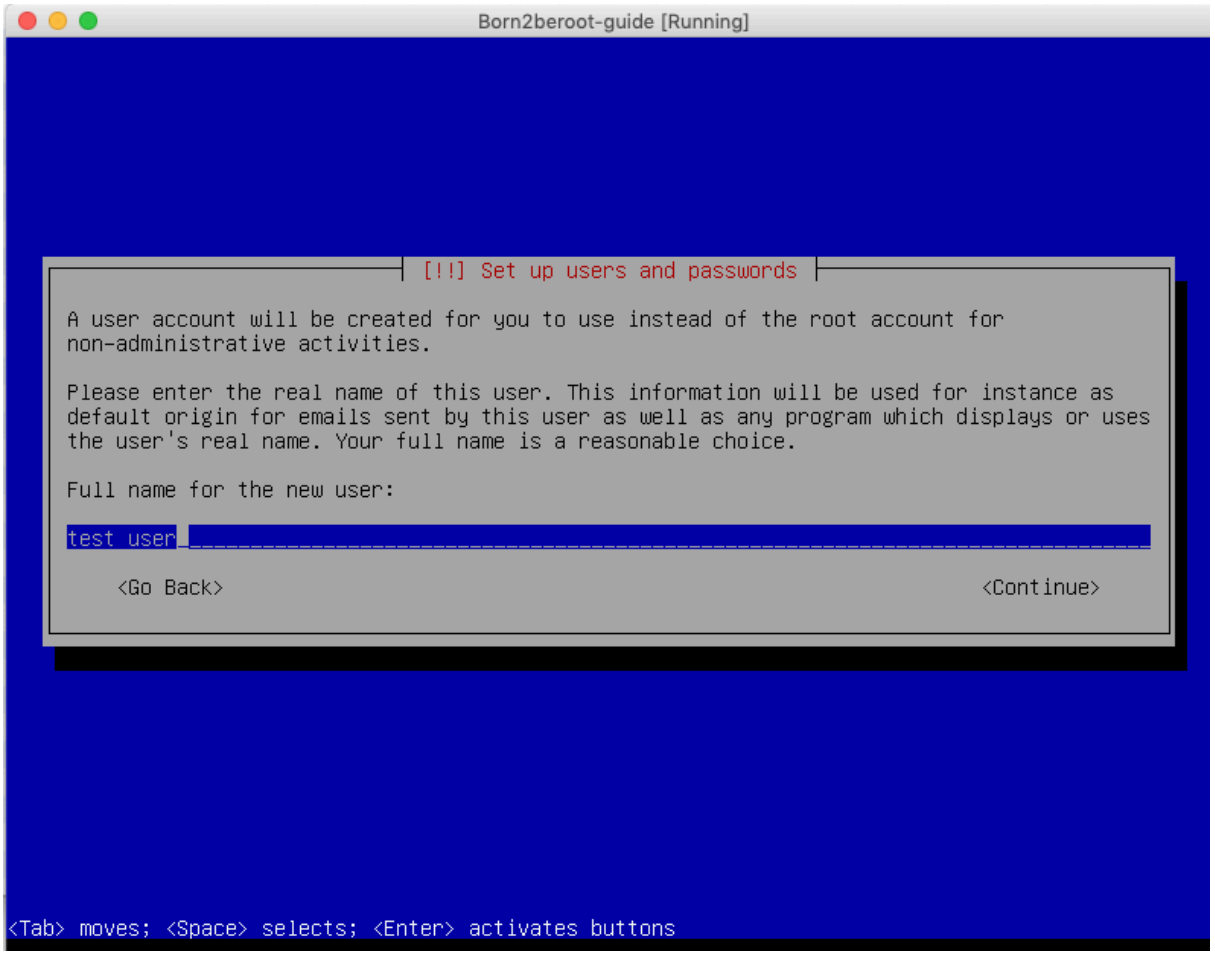
1. Leave this blank, press `enter` on Continue.



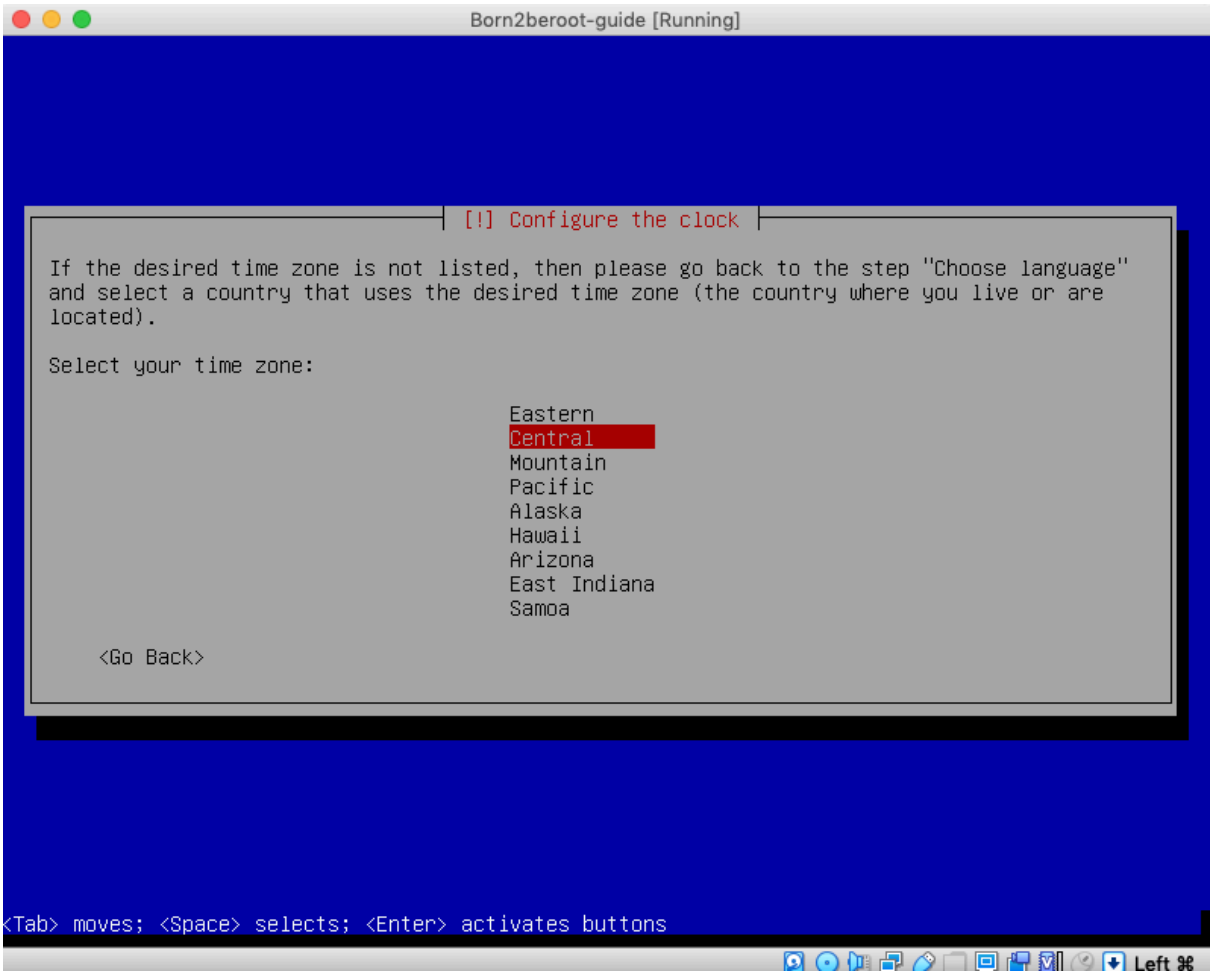
1. Create a Password for the Host Name - write this down as well, as you will need this later on.



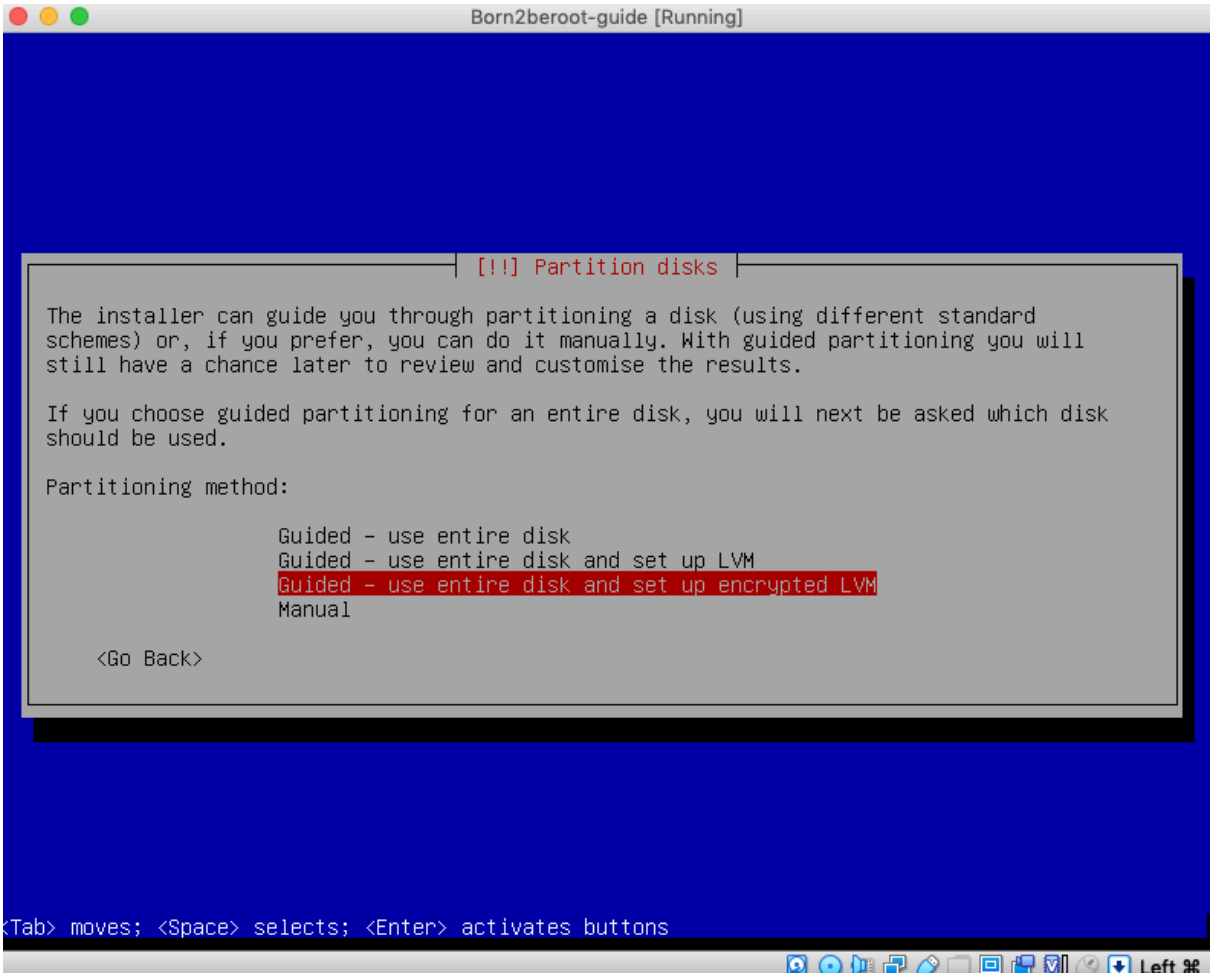
1. Create a User Name without 42 at the end (eg. prossi) - write down your Host Name, as you will need this later on.



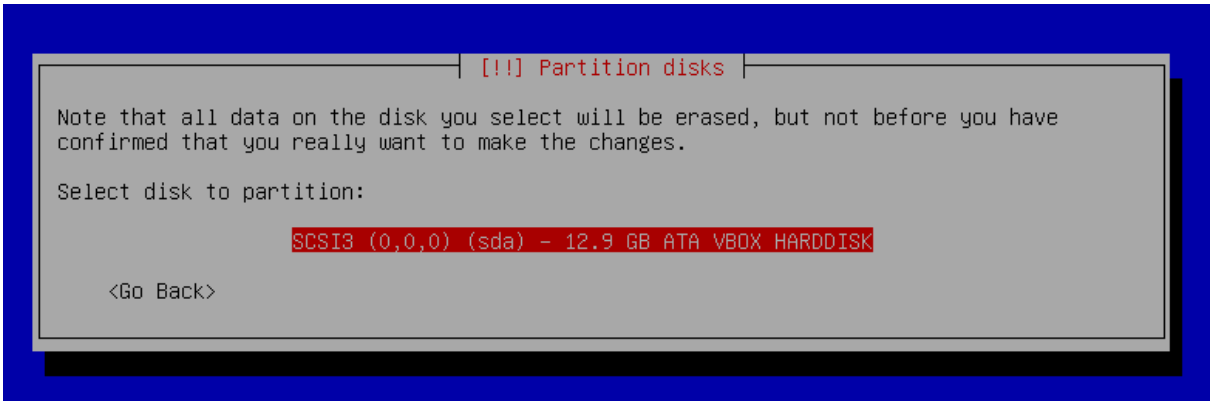
1. Create a Password for the User Name (you might as well use the same password as your Host Password) write this down as well, as you will need this later on.
2. Press `enter` on your `Timezone` (The timezone your currently doing this project in).



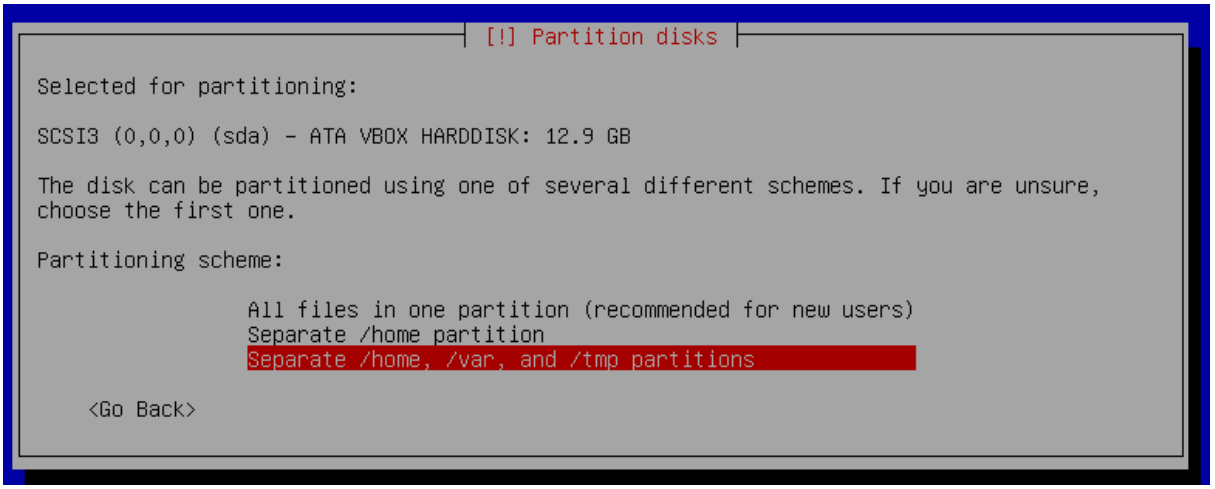
1. Press `enter` on `Guided - use entire disk and set up encrypted LVM` (Second to last option from the list).



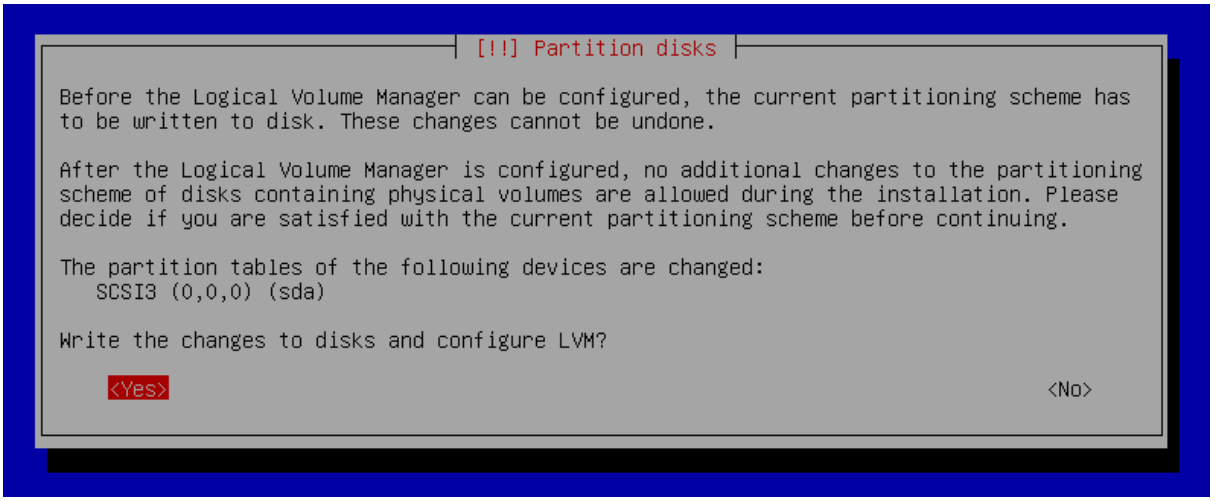
1. Press `enter` on Select Disk to Partition.



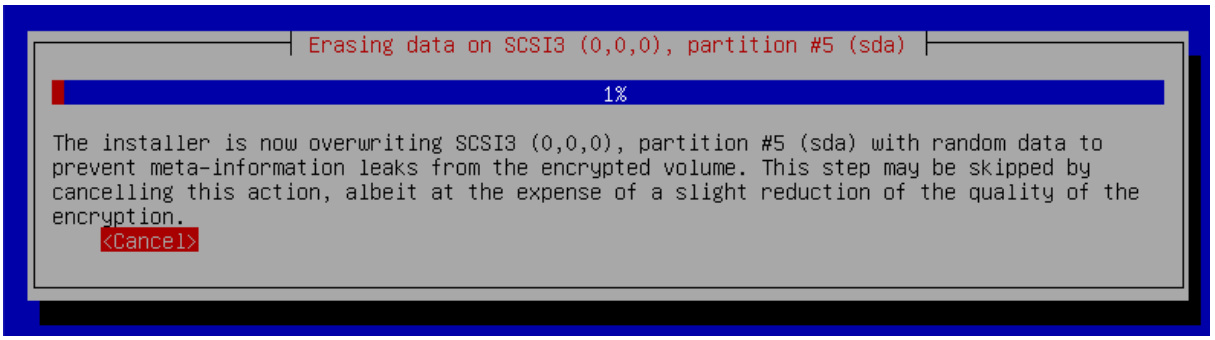
1. Press `enter` on Select `Separate /home, /var, and /tmp paritions` (Last option from the list).



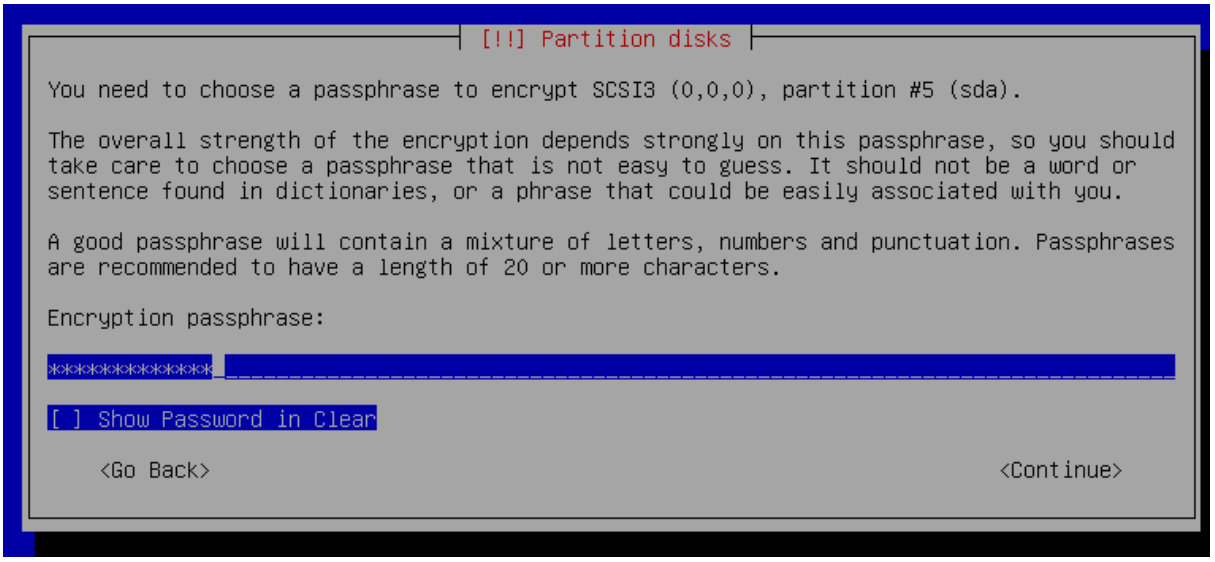
1. Select `Yes` and press `Enter` to write the changes to disks and configure LVM.



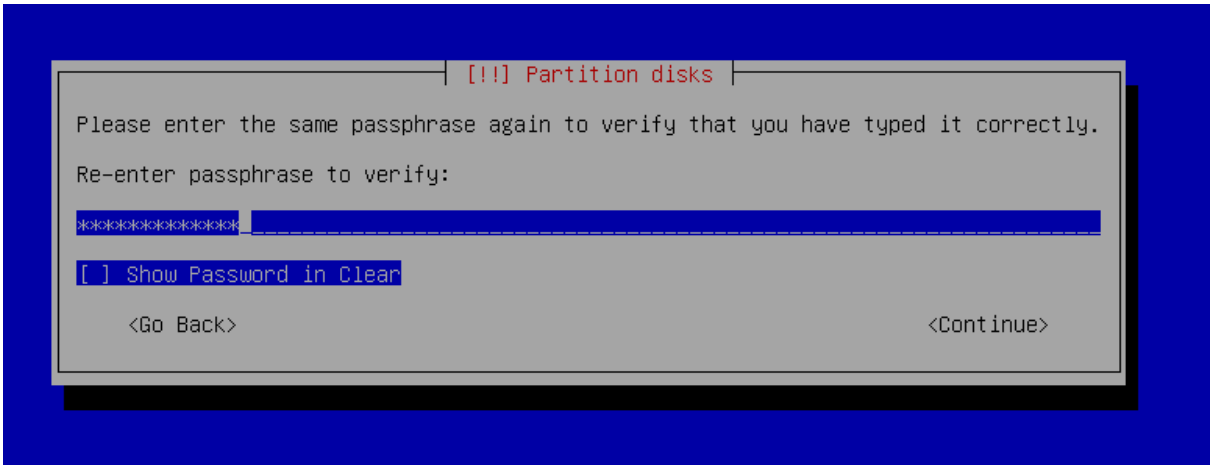
1. Press `Enter` to `cancel` Erasing data as you won't need this for your Virtual Machine.



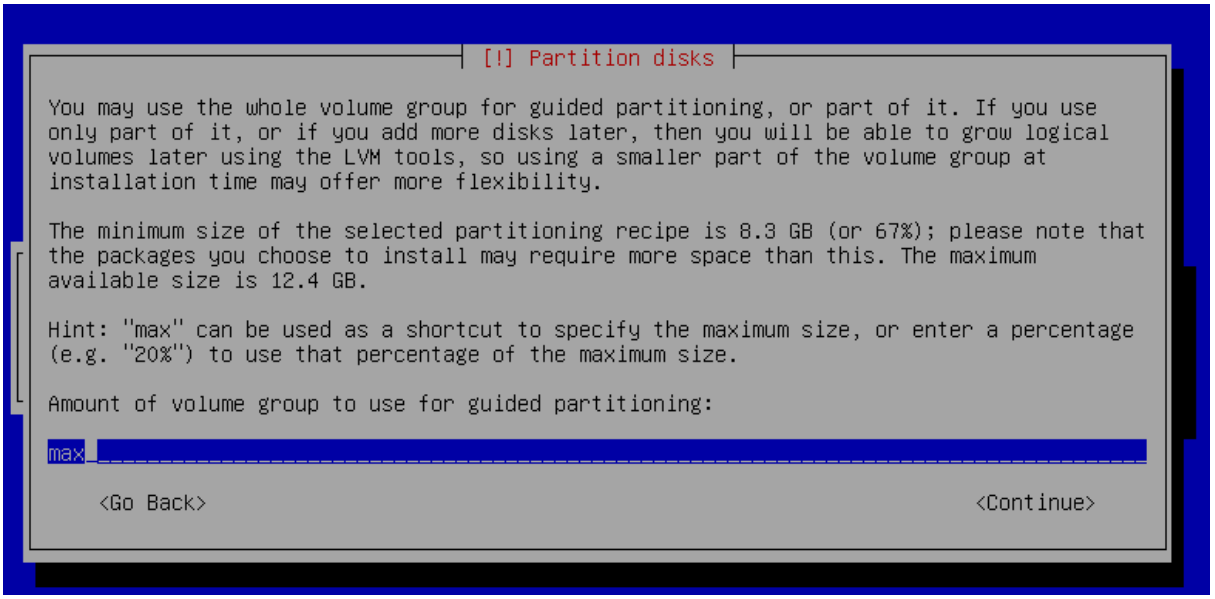
1. Create a Encryption passphrase - write this down as well, as you will need this later on.



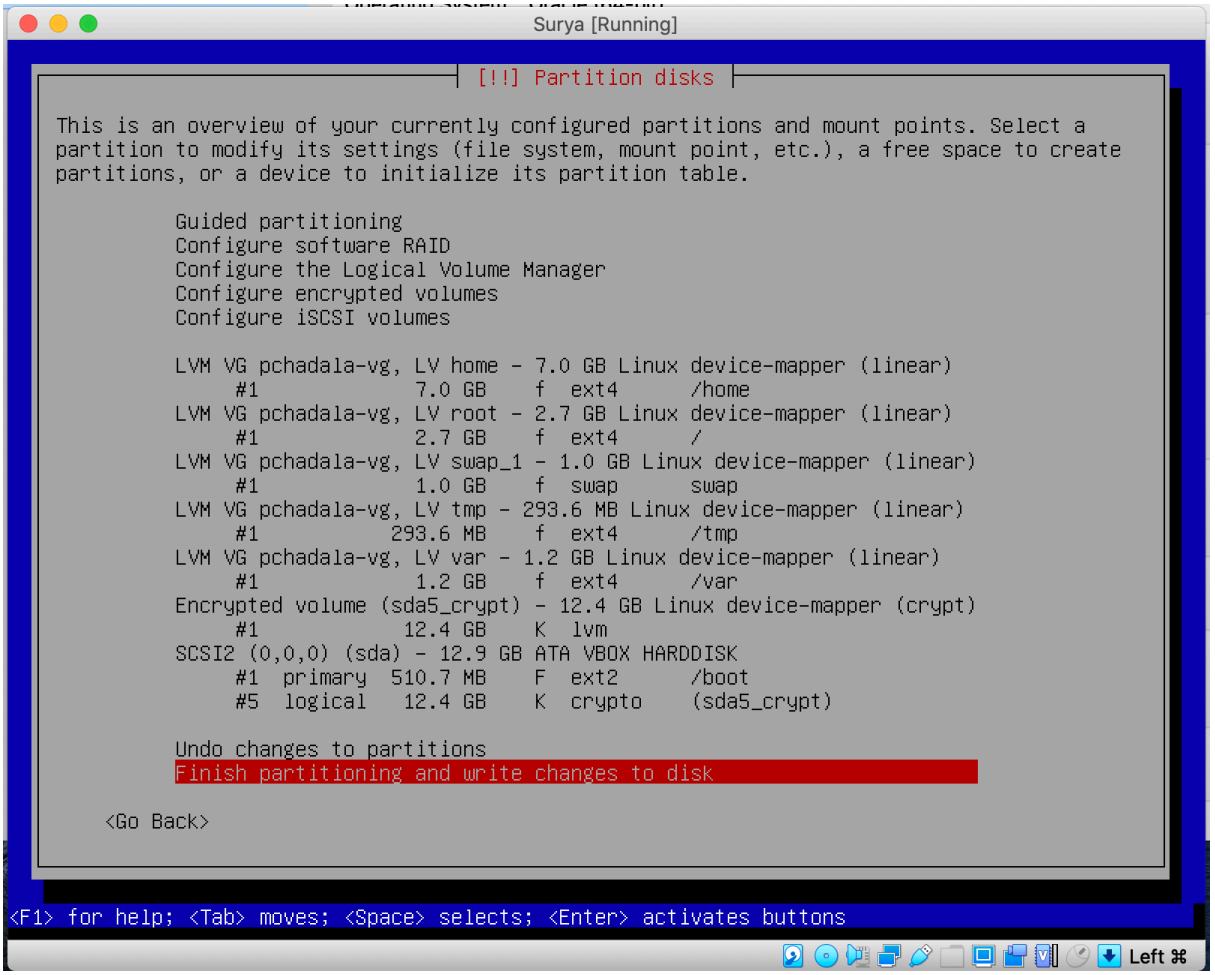
1. Retype the Encryption passphrase you just created.



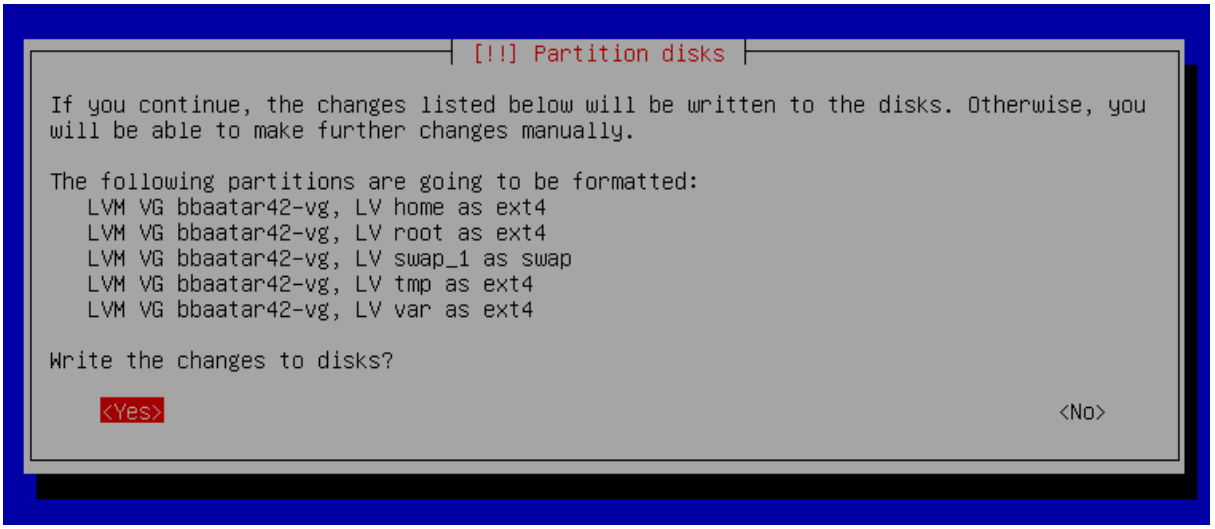
1. Type in `max` and press enter on `Continue` to assign the amount of volume group to use for guided partitioning.



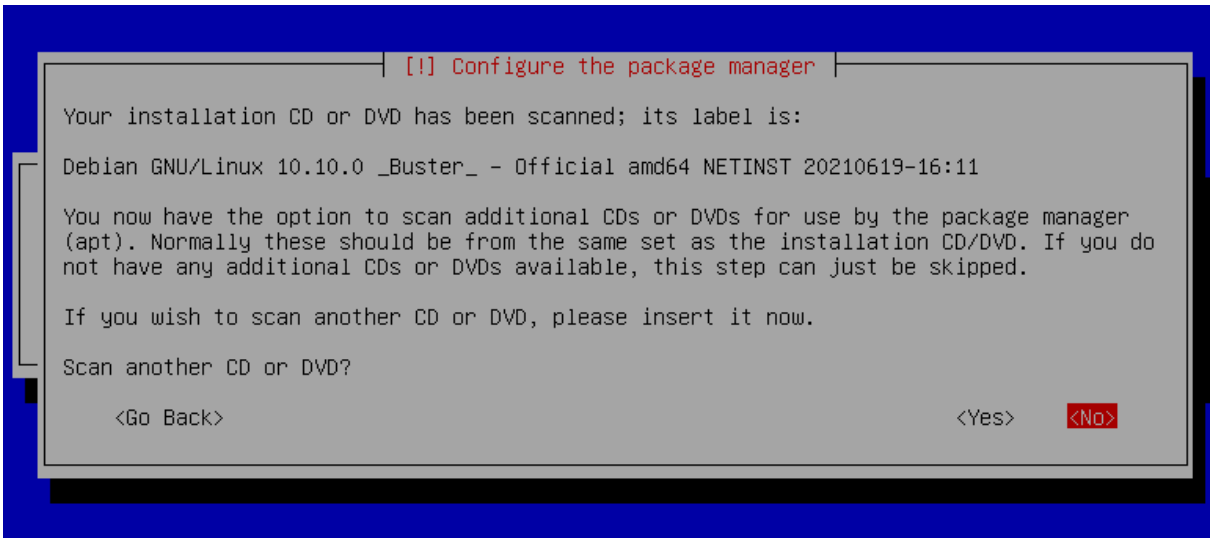
1. Press enter on `Finish partitioning and write changes to disk`.



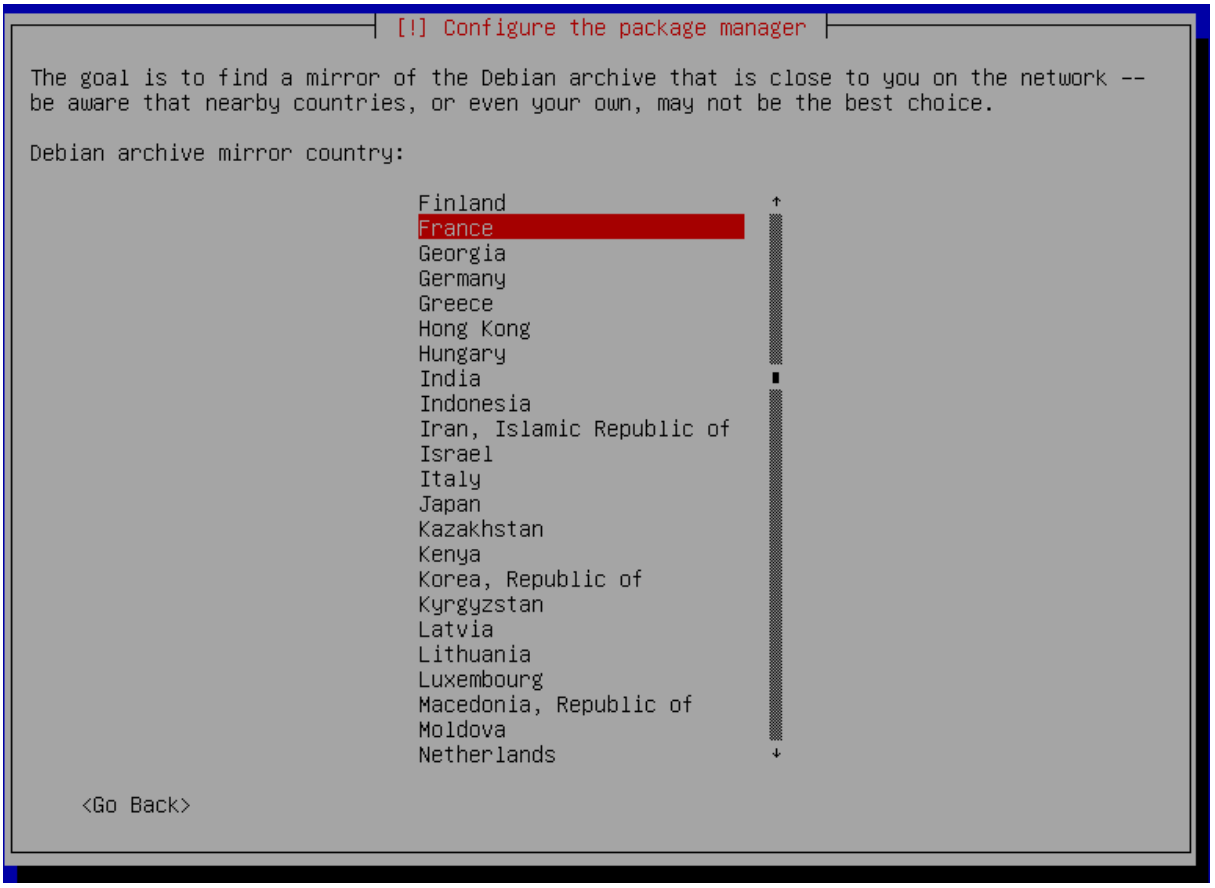
1. Press enter on `Yes` for Partition Disks.



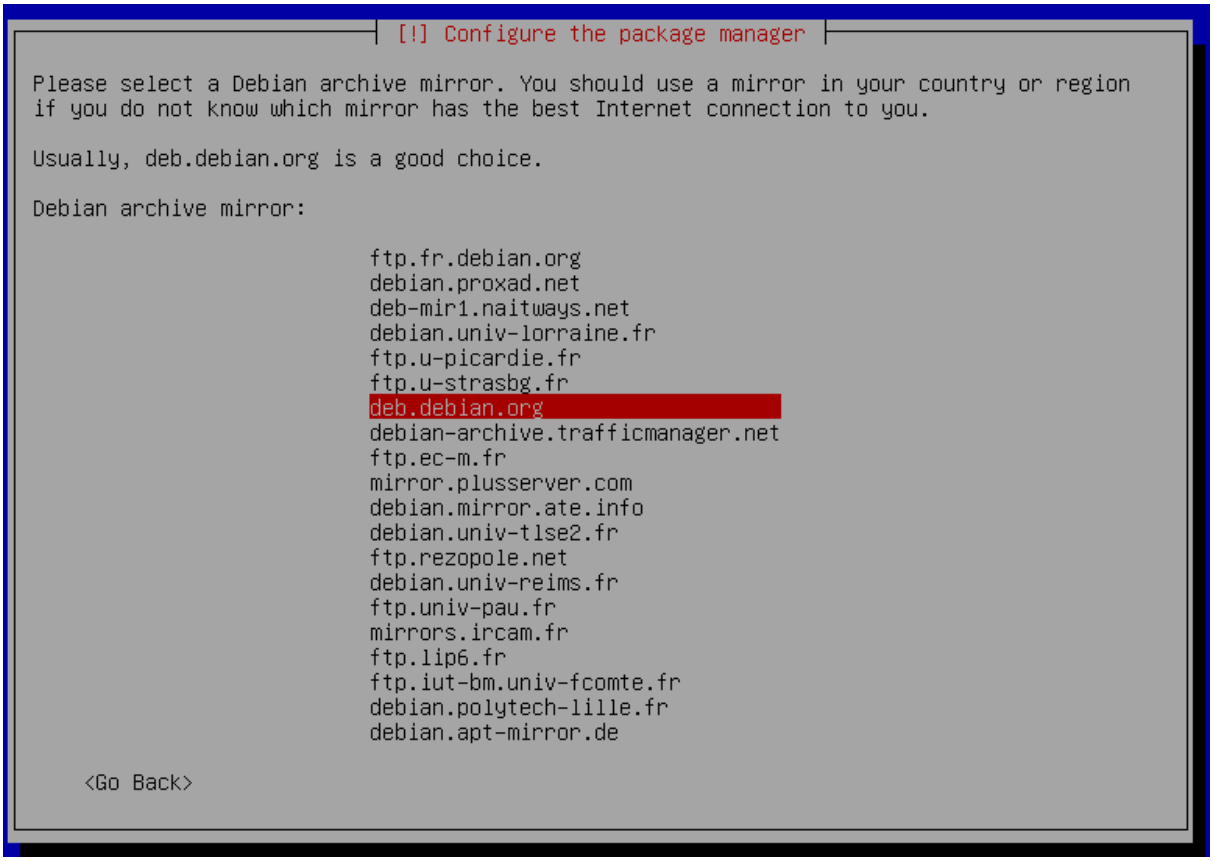
1. Press enter on `No` for Configure the package manager.



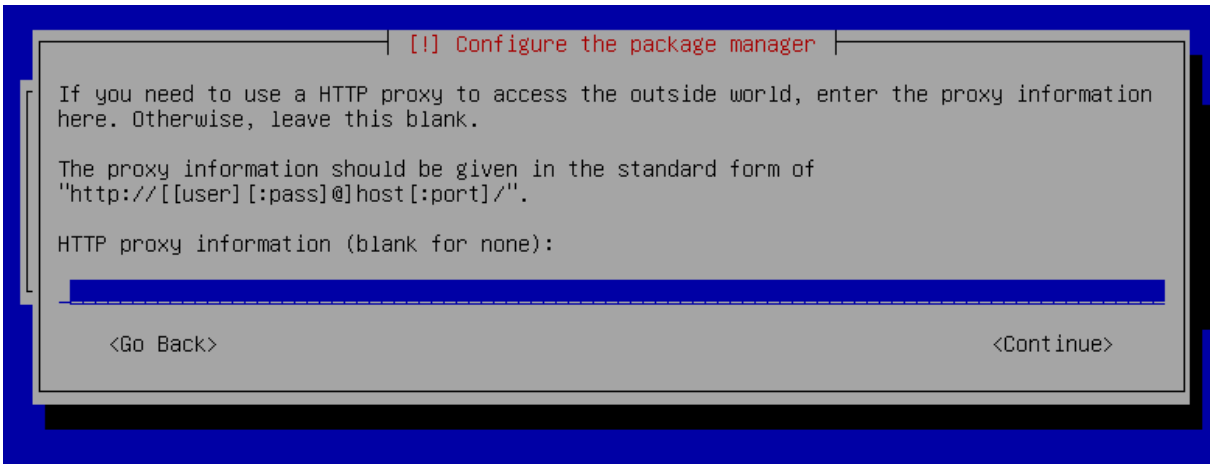
1. Press `enter` in the country that your in.



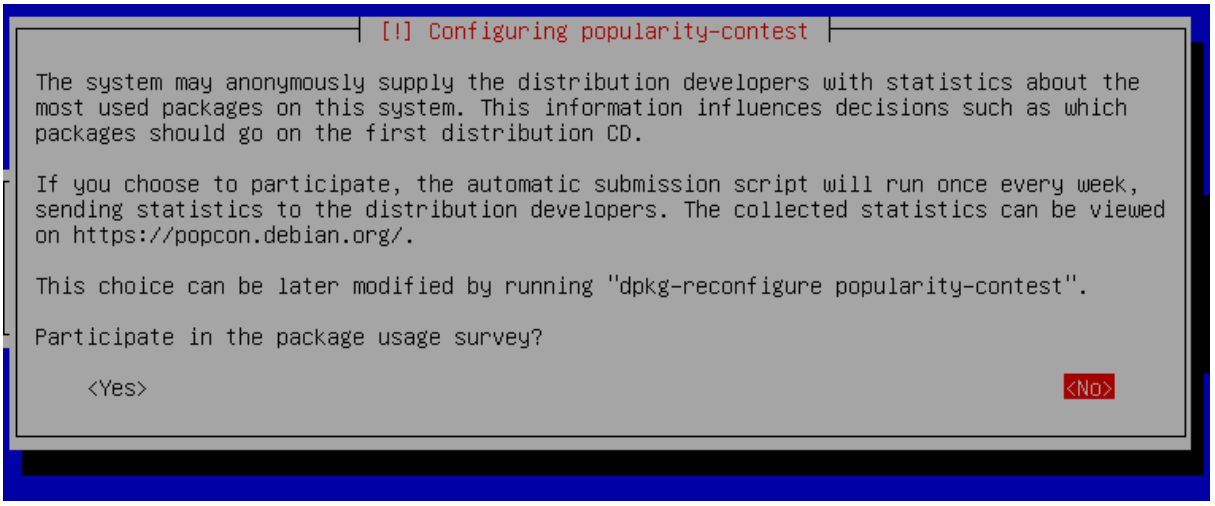
1. Press `enter` on deb.debian.org.



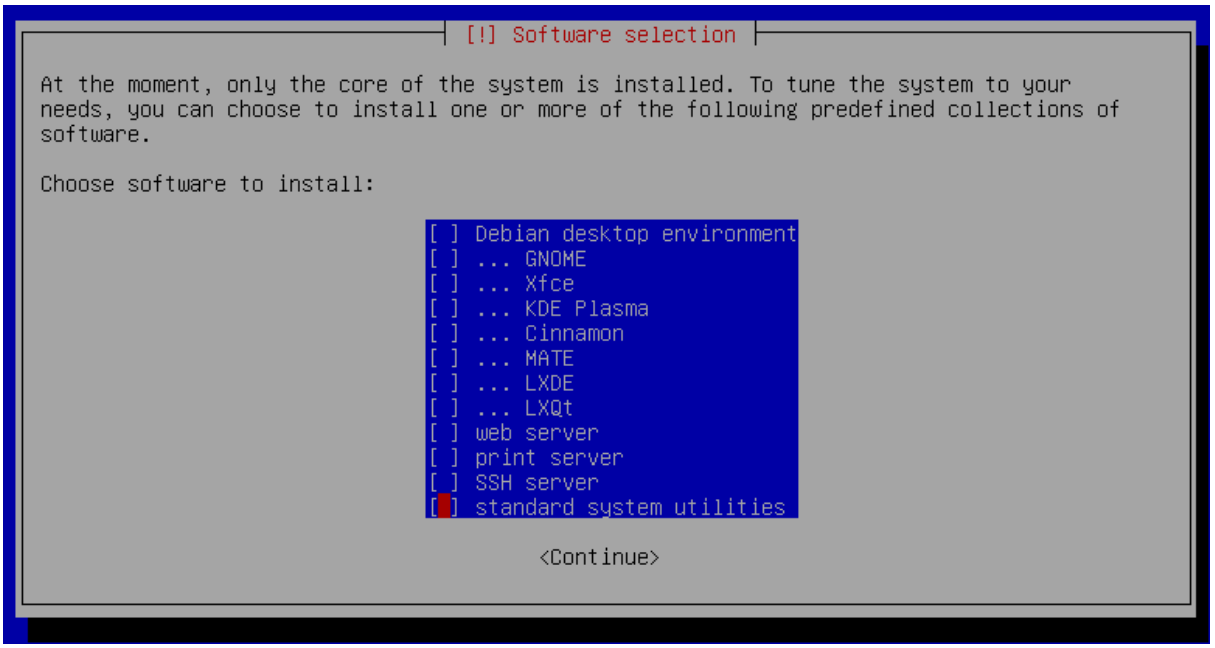
1. Leave this blank and press `enter` on continue.



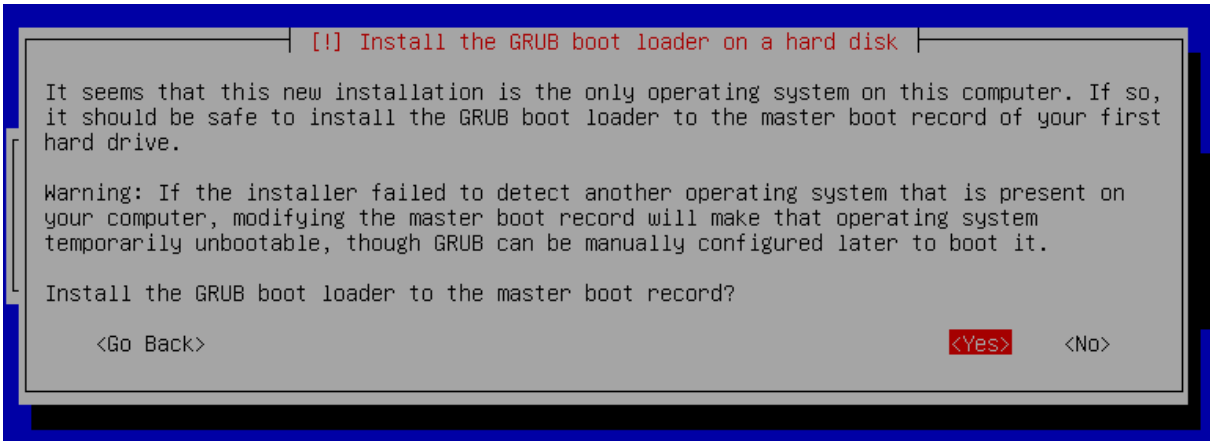
1. Press `enter` on `no` for Configuring popularity-contest.



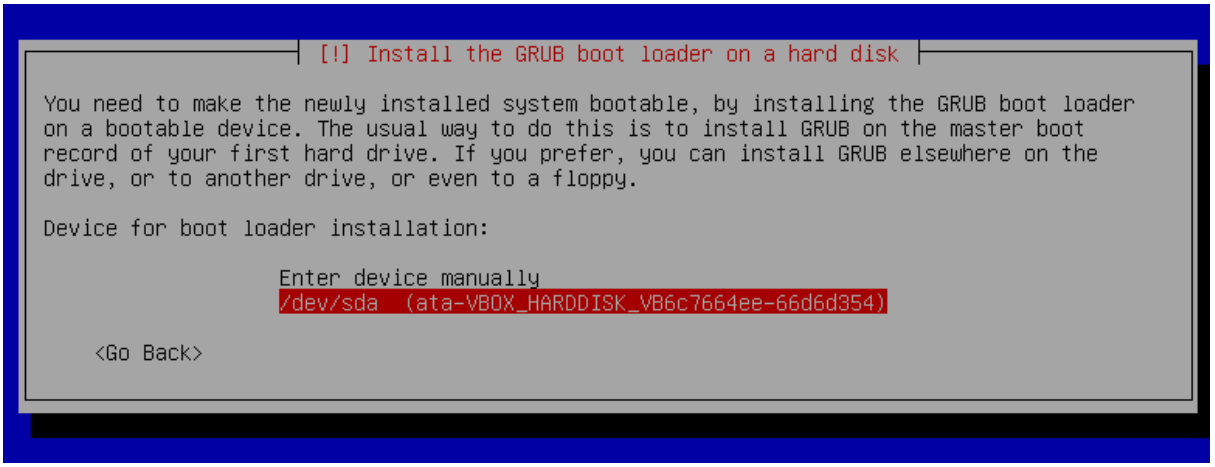
1. Deselect `SSH server` and `standard system utilities` by pressing the `Space key` and then press `enter` on `Continue`.



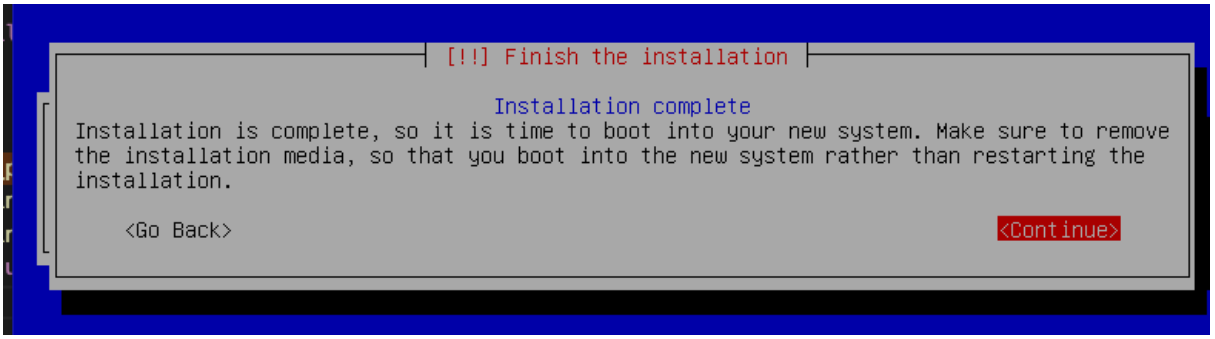
1. Press `enter` on `Yes` to Install the GRUB boot loader on a hard disk.



1. Press `enter` on /dev/sda



1. Press `enter` on `continue` to finish the installation.



1. Before we move onto starting your Virtual Machine, make sure you have your Host, Username and Password/s saved or written down somewhere.

Part 3.1 - Starting Your Virtual Machine

1. Press enter on `Debian GNU/Linux`
2. Enter your encryption password you had created before

3. Login in as the your_username you had created before
4. Type `lsblk` in your Virtual Machine to see the partition

Part 4 - Configurating Your Virtual Machine

Part 4.1 - Installing Sudo

1. First type `su -` to login in as the root user.
2. Then type `apt-get update -y`
3. Then type `apt-get upgrade -y`
4. Then type `apt install sudo`
5. Then type `su -`
6. Then type `usermod -aG sudo your_username` to add user in the sudo group (To check if user is in sudo group, type `getent group sudo`)
7. Type `sudo visudo` to open sudoers file
8. Lastly find - # User privilege specification, type `your_username  ALL=(ALL) ALL`

Part 4.2 - Installing Git and Vim

1. First type `apt-get update -y`
2. Then type `apt-get upgrade -y`
3. Then type `apt-get install git -y` to install Git
4. Then type `git --version` to check the Git Version
5. Then Type `sudo apt-get install wget` to get wget, a free and open source tool for downloading files from web repositories
6. Lastly type `sudo apt-get install vim` to install Vim

Part 4.3 - Installing and Configuring SSH (Secure Shell Host)

1. First type `sudo apt-get update`
2. Type `sudo apt install openssh-server`
3. Type `sudo systemctl status ssh` to check SSH Server Status
4. Type `sudo vim /etc/ssh/sshd_config`
5. Find this line `#Port22`
6. Change the line to `Port 4242` without the # (Hash) in front of it

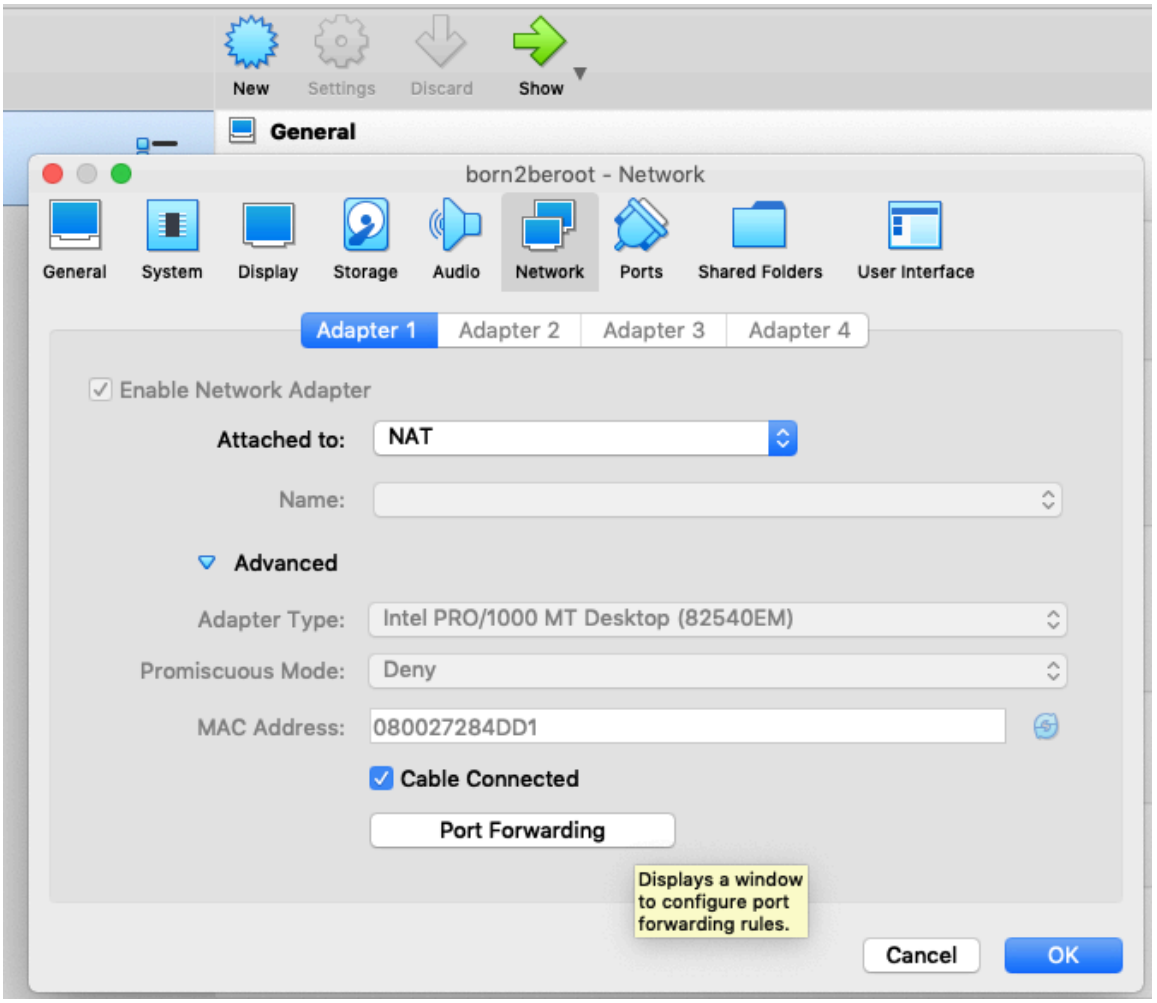
7. Save and Exit Vim
8. Then type `sudo grep Port /etc/ssh/sshd_config` to check if the port settings are right
9. Lastly type `sudo service ssh restart` to restart the SSH Service

Part 4.4 - Installing and Configuring UFW (Uncomplicated Firewall)

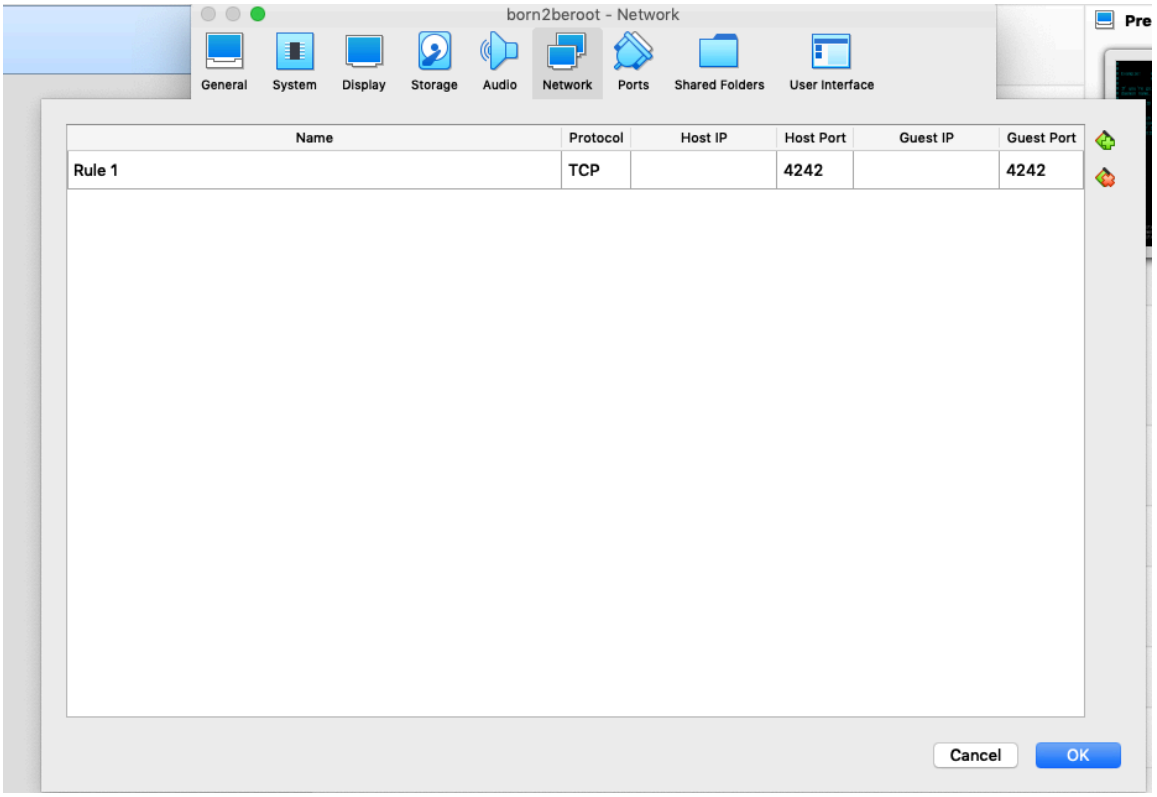
1. First type `apt-get install ufw` to install UFW
2. Type `sudo ufw enable` to inable UFW
3. Type `sudo ufw status numbered` to check the status of UFW
4. Type `sudo ufw allow ssh` to configure the Rules
5. Type `sudo ufw allow 4242` to configure the Port Rules
6. Lastly Type `sudo ufw status numbered` to check the status of UFW 4242 Port

Part 5 Connecting to SSH

1. To exit your Virtual Machine and use your mouse, press `command` on your Apple Keyboard and your mouse should appear
2. Go to your Virtual Box Program
3. Click on your Virtual Machine and select `Settings`
4. Click `Network` then `Adapter 1` then `Advanced` and then click on `Port Forwarding`



5. Change the Host Port and Guest Port to `4242`



6. Then head back to your Virtual Machine
7. Type `sudo systemctl restart ssh` to restart your SSH Server
8. Type `sudo service sshd status` to check your SSH Status
9. Open an iTerm and type the following `ssh your_username@127.0.0.1 -p 4242`
10. In case an error occurs, then type `rm ~/.ssh/known_hosts` in your iTerm and then retype `ssh your_username@127.0.0.1 -p 4242`
11. Lastly type `exit` to quit your SSH iTerm Connection

Part 6 - Continue Configurating Your Virtual Machine

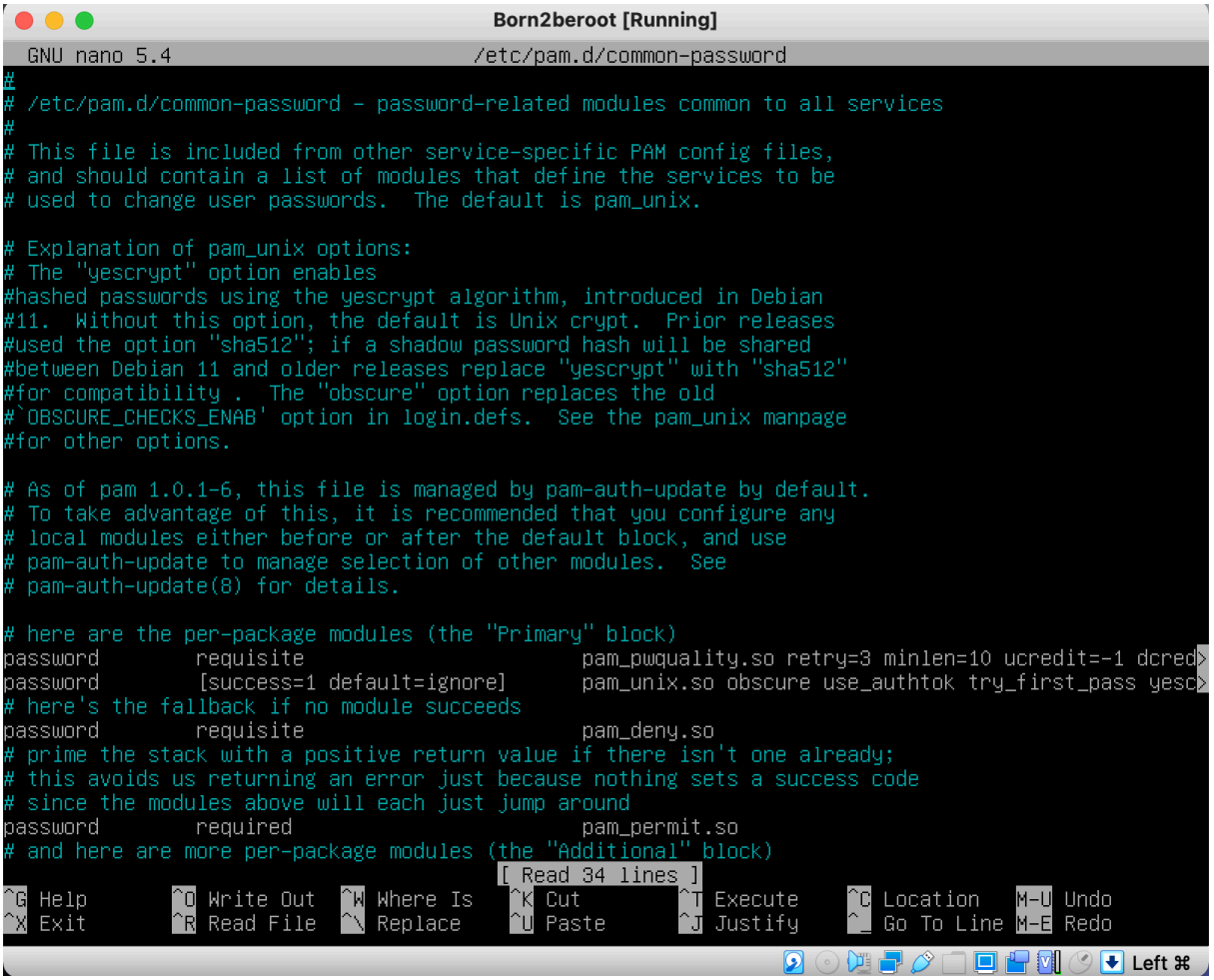
Part 6.1 - Setting Password Policy

1. First type `sudo apt-get install libpam-pwquality` to install Password Quality Checking Library
2. Then type `sudo vim /etc/pam.d/common-password`
3. Find this line

```
password        requisite                       pam_pwquality.so retry=3
```

4. Add this to the end of that line `minlen=10 ucredit=-1 dcredit=-1 maxrepeat=3 reject_username difok=7 enforce_for_root`

- 4.1 The line should now look like this - `password requisite pam_pwquality.so retry=3 minlen=10 ucredit=-1 dcredit=-1 maxrepeat=3 reject_username difok=7 enforce_for_root`



1. Save and Exit Vim
2. Next type in your Virtual Machine `sudo vim /etc/login.defs`
3. Find this part `PASS_MAX_DAYS 9999` `PASS_MIN_DAYS 0` `PASS_WARN_AGE 7`
4. Change that part to `PASS_MAX_DAYS 30` and `PASS_MIN_DAYS 2` keep `PASS_WARN_AGE 7` as the same
5. Lastly type `sudo reboot` to reboot the change affects

Part 6.2 - Creating a Group

1. First type `sudo groupadd user42` to create a group
2. Then type `sudo groupadd evaluating` to create an evaluating group
3. Lastly type `getent group` to check if the group has been created

Part 6.3 - Creating a User and Assigning Them Into The Group

1. First type `cut -d: -f1 /etc/passwd` to check all local users
2. Type `sudo adduser new_username` to create a username - write down your new_username, as you will need this later on.

- 2.1 Type `sudo usermod -aG user42 your_username`
- 2.2 Type `sudo usermod -aG evaluating your_new_username`

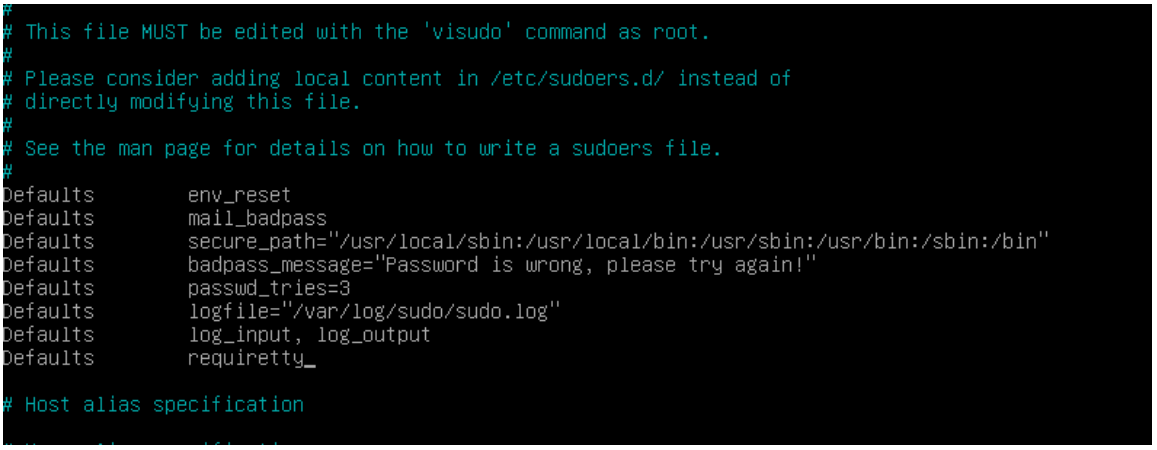
1. Type `getent group user42` to check if the user is the group
2. Type `getent group evaluating` to check the group
3. Type `groups` to see which groups the user account belongs to
4. Lastly type `chage -l your_new_username` to check if the password rules are working in users

Part 6.4 - Creating sudo.log

1. First type `cd ..`
2. Type `cd ..` again.
3. Type `cd ..` again for the 3rd time.
4. Then type `cd var/log`
5. Then type `mkdir sudo` (if it already exists, then continue to the next step).
6. Then type `cd sudo && touch sudo.log`
7. Then type `cd ..`
8. Then type `cd ..`
9. Then type `cd ..` again for the 3rd time.

Part 6.4.1 - Configuring Sudoers Group

1. First type `sudo vim /etc/sudoers` to go the sudoers file
2. Now edit your sudoers file to look like the following by adding in all of the defaults in the image below -




```
Defaults  env_reset
Defaults  mail_badpass
Defaults  secure_path="/usr/local/sbin:/usr/local/bin:/usr/bin:/sbin:/bin"
Defaults  badpass_message="Password is wrong, please try again!"
Defaults  passwd_tries=3
Defaults  logfile="/var/log/sudo/sudo.log"
Defaults  log_input, log_output
Defaults  requiretty
```

Part 6.5 - Crontab Configuation

1. First type `sudo apt-get update -y`
2. Then type `sudo apt-get install -y net-tools` to install the netstat tools
3. Then type `cd /usr/local/bin/`
4. Then type `touch monitoring.sh`
5. Lastly type `chmod 777 monitoring.sh`

Part 6.5.1 - Copy Text Below onto Virtual Machine

1. Copy this text (To copy the text below, hover with your mouse to the right corner of the text below and a copy icon will appear).

```
#!/bin/bash
arc=$(uname -a)
pcpu=$(grep "physical id" /proc/cpuinfo | sort | uniq | wc -l)
vcpu=$(grep "^processor" /proc/cpuinfo | wc -l)
fram=$(free -m | awk '$1 == "Mem:" {print $2}')
uram=$(free -m | awk '$1 == "Mem:" {print $3}')
```

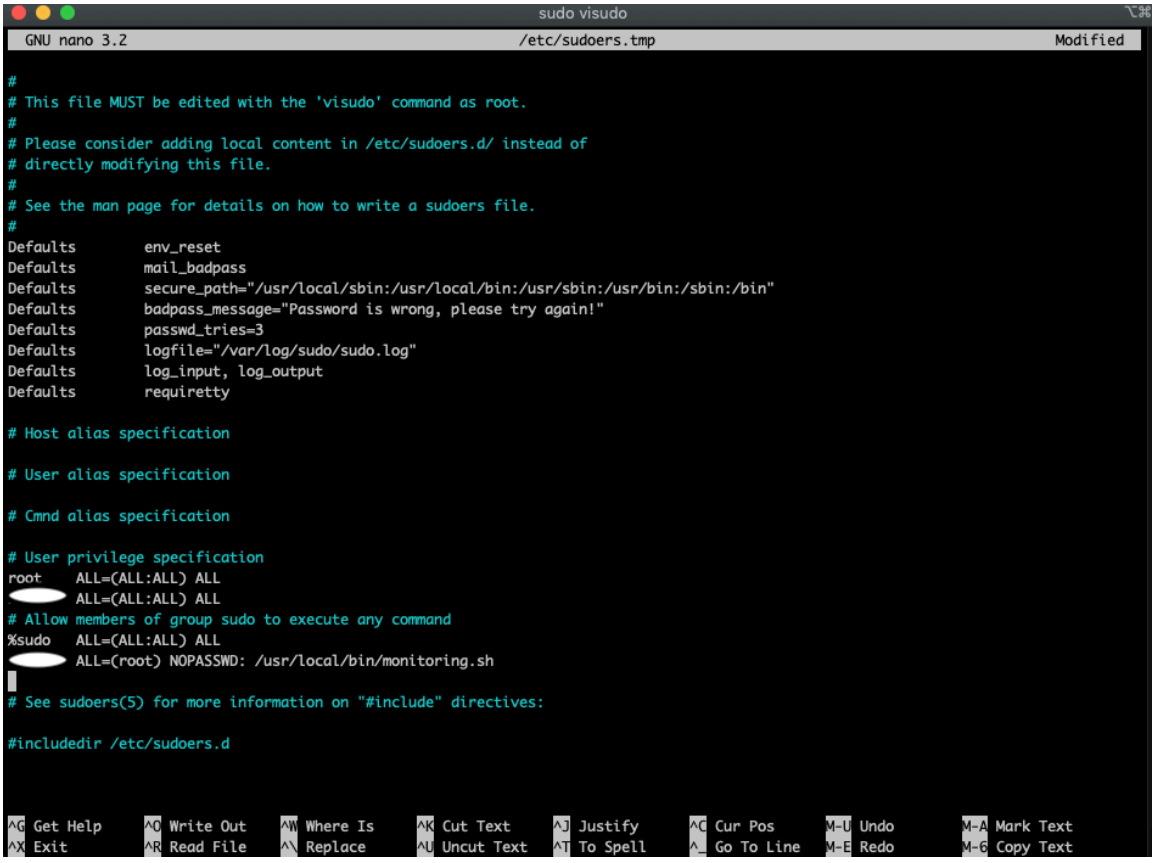
```
pram=$(free | awk '$1 == "Mem:" {printf("%.2f"), $3/$2*100}')
fdisk=$(df -BG | grep '^/dev/' | grep -v '/boot$' | awk '{ft += $2} END {print
ft}')
udisk=$(df -BM | grep '^/dev/' | grep -v '/boot$' | awk '{ut += $3} END {pri
nt ut}')
pdisk=$(df -BM | grep '^/dev/' | grep -v '/boot$' | awk '{ut += $3} {ft+= $2}
END {printf("%d"), ut/ft*100}')
cpul=$(top -bn1 | grep '^%Cpu' | cut -c 9- | xargs | awk '{printf("%.1f%%"),
$1 + $3}')
lb=$(who -b | awk '$1 == "system" {print $3 " " $4}')
lvmu=$(if [ $(lsblk | grep "lvm" | wc -l) -eq 0 ]; then echo no; else echo ye
s; fi)
ctcp=$(ss -neopt state established | wc -l)
ulog=$(users | wc -w)
ip=$(hostname -I)
mac=$(ip link show | grep "ether" | awk '{print $2}')
cmds=$(journalctl _COMM=sudo | grep COMMAND | wc -l)
wall "   #Architecture: $arc
    #CPU physical: $pcpu
    #vCPU: $vcpu
    #Memory Usage: $uram/${fram}MB ($pram%)
    #Disk Usage: $udisk/${fdisk}Gb ($pdisk%)
    #CPU load: $cpul
    #Last boot: $lb
    #LVM use: $lvmu
    #Connections TCP: $ctcp ESTABLISHED
    #User log: $ulog
    #Network: IP $ip ($mac)
    #Sudo: $cmds cmd"
```

1. Then open up a iTerm2 seperate from your Virtual Machine and type in iTerm `ssh your_host_name42@127.0.0.1 -p 4242` and then type your password, when it asks for it.
2. Then type `cd /usr/local/bin`.
3. Then type `vim monitoring.sh` and paste the text above into the vim monitoring.sh you just created, by doing `command` + `v` on your Apple keyboard.

4. Save and Exit your `monitoring.sh`

- 5.1 - Then type `exit` to exit the iTerm SSH Login.
- 5.2 - Then go back to your Virtual Machine (not iTerm) and continue on with the steps below.

1. Then type `sudo visudo` to open your sudoers file
2. Add in this line `your_username ALL=(ALL) NOPASSWD: /usr/local/bin/monitoring.sh` under where its written %sudo ALL=(ALL:ALL) ALL
3. It should look like this



4. Then exit and save your sudoers file
5. Now type `sudo reboot` in your Virtual Machine to reboot sudo
6. Type `sudo /usr/local/bin/monitoring.sh` to execute your script as su (super user)
7. Type `sudo crontab -u root -e` to open the crontab and add the rule
8. Lastly at the end of the crontab, type the following `/10 * * * *` `/usr/local/bin/monitoring.sh` this means that every 10 mins, this script will show

Part 7 - Signature.txt (Last Part Before Defence)

⚠️ Warning: before you generate a signature number, please power off your Virtual Machine. ⚠️

1. Open iTerm and type `cd`
2. Then type `cd sgoinfre/students/<your_intra_username>/VirtualBox VMs`
3. Then type `shasum VirtualBox.vdi` or whatever your Virtual Machine .vdi file is called.
4. After a few mins, you should see an output similar to this - 6e657c4619944be17df3c31faa030c25e43e40af
5. Copy your signature number and create a .txt file and paste your number in the .txt file you just created, ready for submission.

🥳 **CONGRATULATIONS! YOU HAVE NOW FINISHED! NEXT IS THE EVALUATION** ⬇️