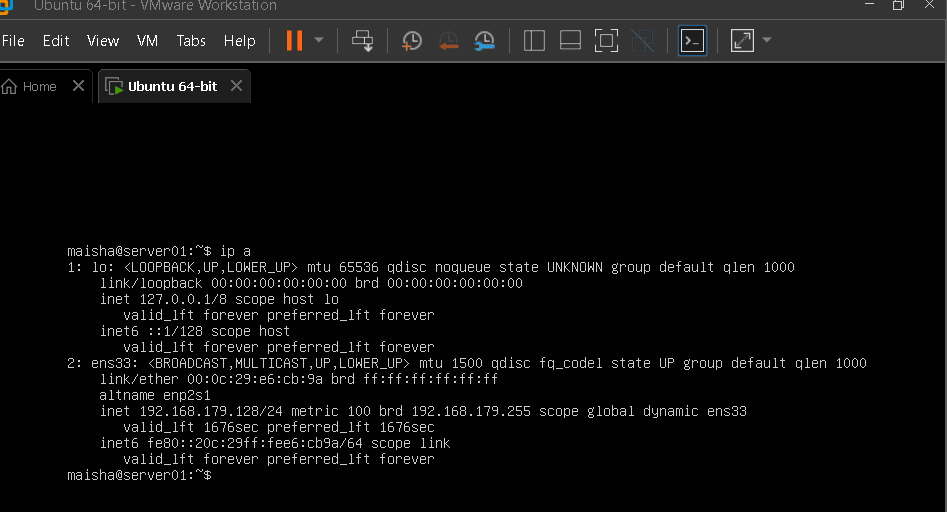
|  |  |
| --- | --- |
| **Durham College** | |
| **Course** | **INFT1103** |
| **Professor** | **Ida Leung** |
| **Student Name** | **Maisha Khatoon | #100899259** |
| **Lab#5.2 Linux System (UFW/ Banner / ClamAV)** | |

# Part 1: Create a pair rsa key to login to your Linux Server

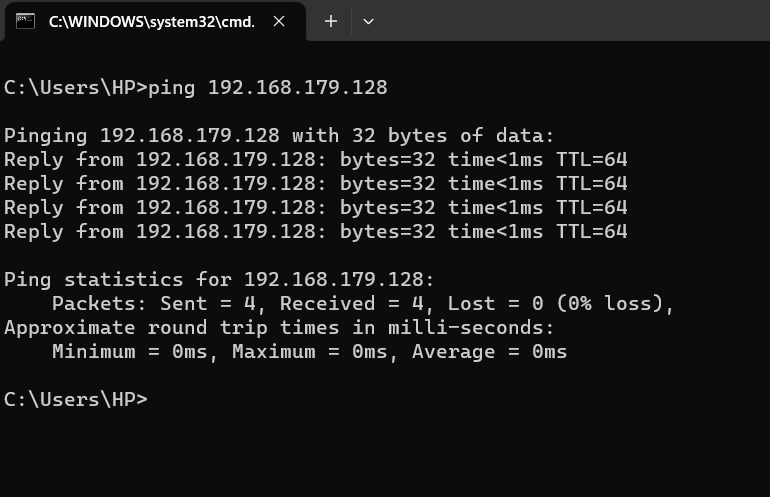
1. Use the command *ip a* to confirm your server’s IP address

a. Take a screenshot of your Ubuntu server’s IP address and paste it here

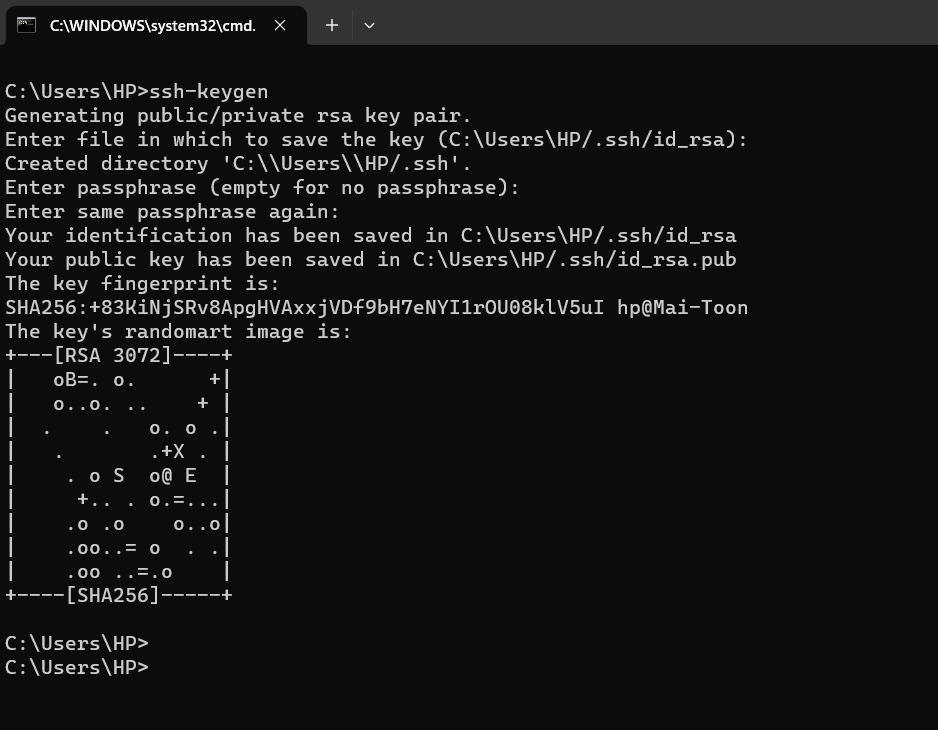


1. Ping the IP from your Windows host computer

a. Take a screenshot of the successful pings and paste it here



1. On your local Windows computer (NOT your ubuntu machine) create an ssh keypair: open command prompt and type: *ssh-keygen*
   1. Take a screenshot of the confirmation message, including the fingerprint, and paste it here



1. Once the keypair is created, copy the public key to a safe directory. Use the command: *copy C:\Users\yourUserName\.ssh\id\_rsa.pub*

*C:\Users\yourUserName\authorized\_keys Command may varies if you are using MacOS.*

1. Go back to your Ubuntu server

1. Start the SSH service using the commands:
   1. *sudo apt install openssh-server*
   2. *sudo ufw allow ssh mkdir -p ~*

1. Create an ssh directory with the command: *mkdir ~/.ssh/ , you may already have the folder exists*

**

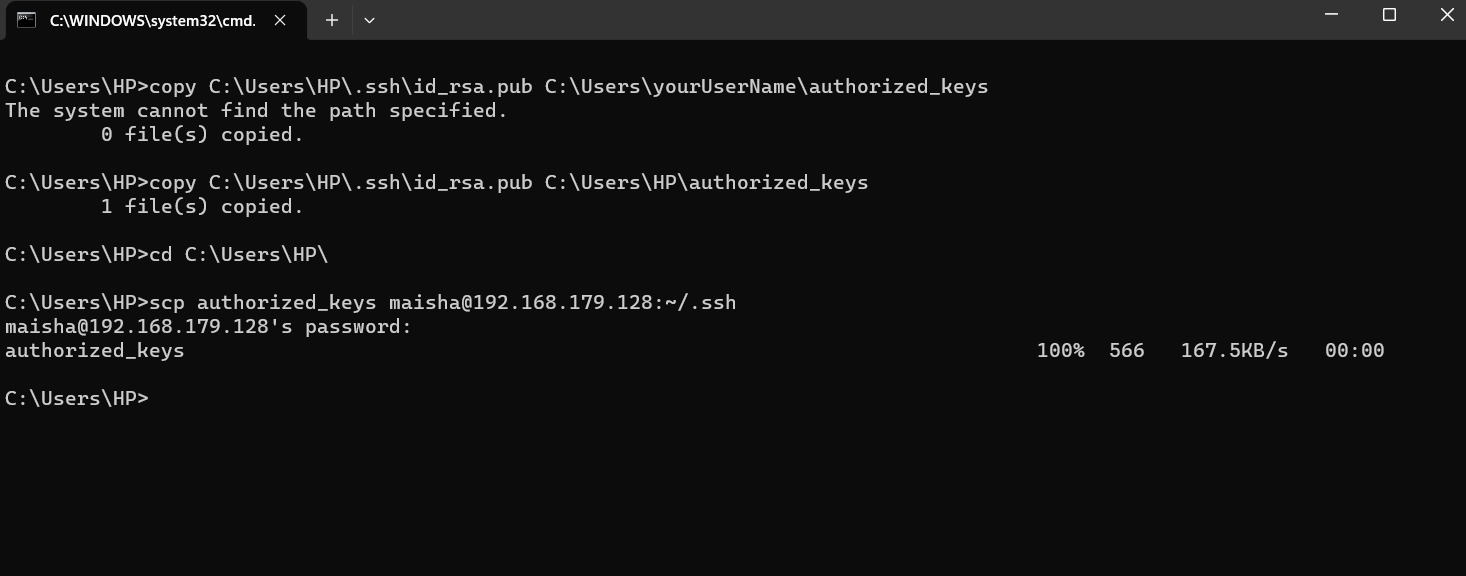
1. Go back to your Windows host computer.

1. Open command prompt and use the command: 
   * 1. *cd C:\Users\yourUserName\*

* + 1. Copy your public ssh key to the ubuntu server using the command: *scp authorized\_keys username@UbutnuServerIP:~/.ssh*

*For Linux server hosts in AWS environment, you may experience problem by using other username. Keep the “ubuntu” username for what the key pairs for.*

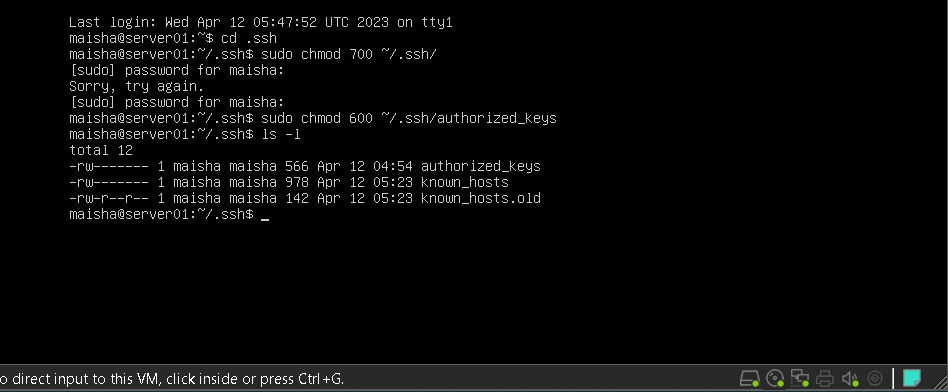
* + 1. Take a screenshot to confirm the authorized\_keys file has been copied to the correct directory and paste it here



1. Go back to your Ubuntu server

1. Adjust the permission settings for the ssh share and public ssh key file:
   * 1. *chmod 700 ~/.ssh*
     2. *chmod 600 ~/.ssh/authorized\_keys*

* + 1. Run the *-ls -l* command on the /.ssh directory to ensure the changes were made. *Take a screenshot and paste it here*



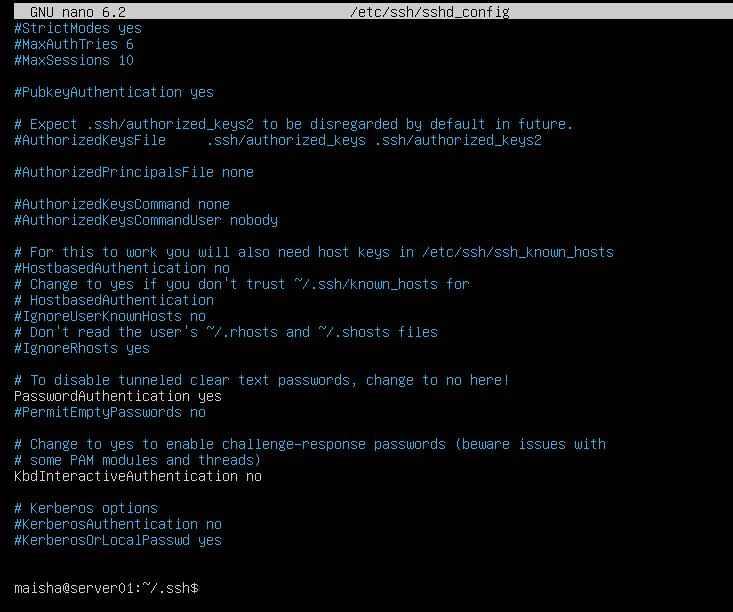
1. Go back to your Windows host computer
2. Test your login by using password authentication. sudo nano /etc/ssh/sshd\_config

Ensure PasswordAuthentication is “yes”.

Restart the sshd process: systemctl restart sshd

Then ssh username@UbuntuServerIP (for AWS, you may need to add the .pem file together)

*i.* Paste your screenshot here



1. Modify the sshd\_config file to deny password authentication but allow public key authentication.

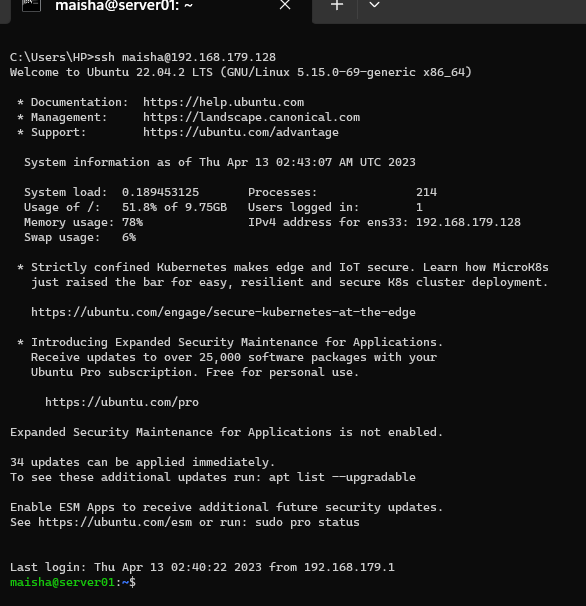
*Ensure that PasswordAuthentication is “no” and PubkeyAuthentication yes and not in comment.*

## sudo nano /etc/ssh/sshd\_config

***# add the line “PubkeyAuthentication yes” if it does not exist!***

## #uncomment line “PasswordAuthentication” and set to “no” systemctl restart sshd

1. Log into your Ubuntu machine from the Windows command prompt with the command: *ssh username@UbuntuServerIP* 
   1. You should not be prompted for a password
   2. Take a screenshot showing both the ssh login command and the ubuntu terminal (expand the command prompt window if necessary)
      * 1. Example:
        2. Paste your screenshot here



1. Create a banner message for your SSH service
   1. *sudo nano /etc/ssh/ssh\_banner.net*
   2. In the text editor enter the following information:
      * 1. Your Name:
        2. Your student number: iii. The course number:

iv. Welcome message

* 1. Close the text editor with Ctrl +X

1. Add the banner message to the SSH config file
   1. *sudo nano /etc/ssh/sshd\_config*
   2. Find the line that says “Banner” and add the following information:

*i. Banner /etc/ssh/ssh\_banner.net*

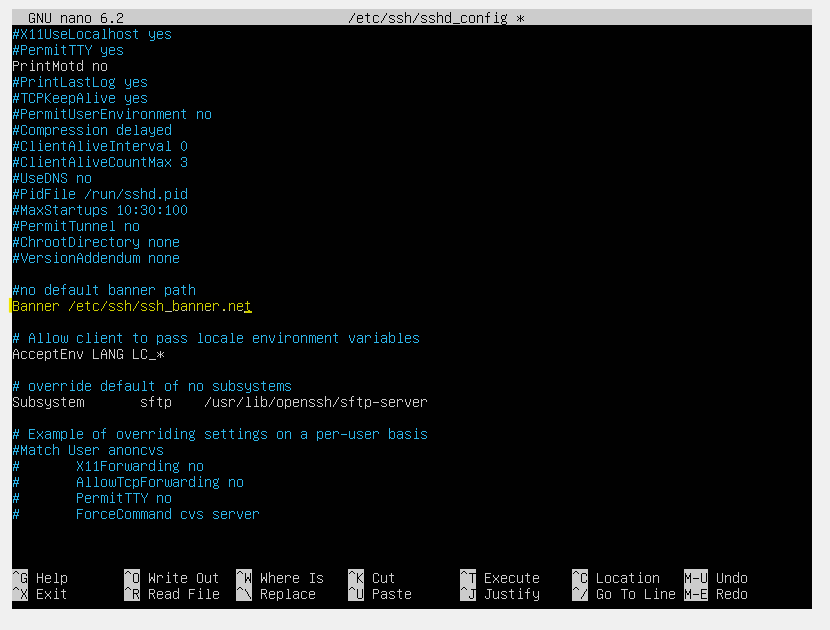
***Replace ‘Banner none’ with ‘Banner /etc/ssh/ssh\_banner.net’***

* 1. Close the text editor using CTRL + X
  2. Restart the SSH service

*i. sudo systemctl restart ssh*

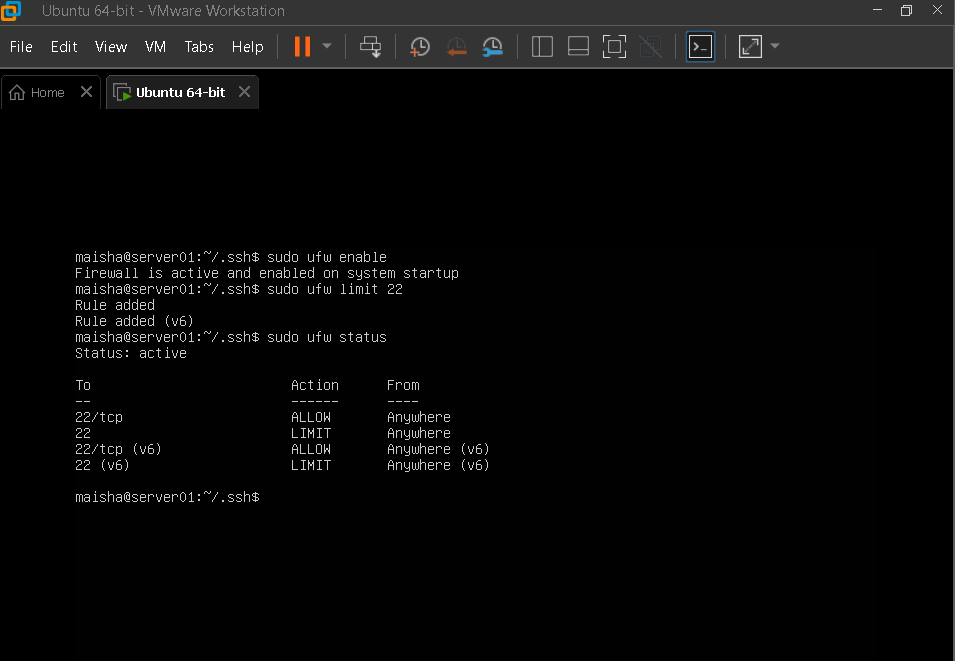
1. Log out of the SSH terminal session completely
2. Log back in using SSH

a. Take a screenshot of your banner message and paste it here.

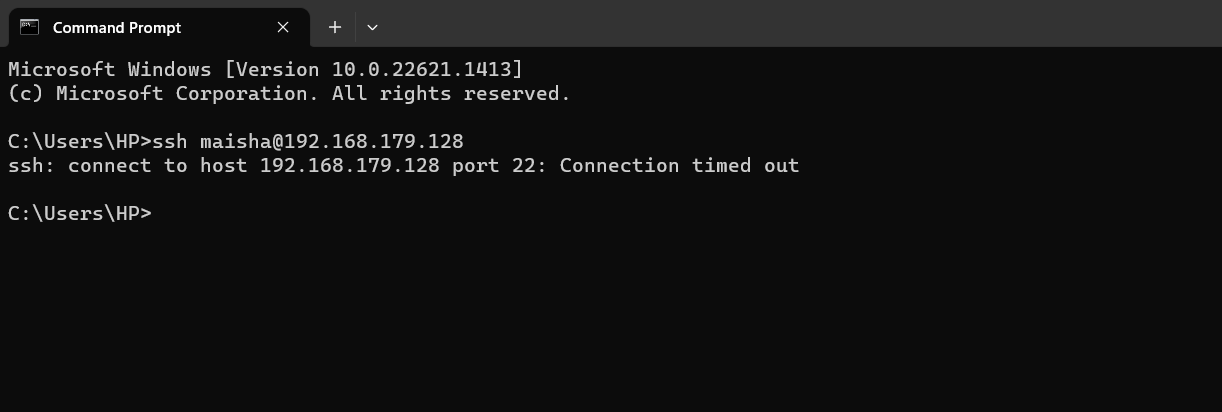


# Part 2: Enable Firewall and Configuration of Firewall Logging

1. Enable ufw
   1. *sudo ufw enable*
2. Enable rate limiting for port 22
   1. *sudo ufw limit 22*
   2. confirm the rule is enabled using *sudo ufw status.* Take a screenshot and paste it here.

s

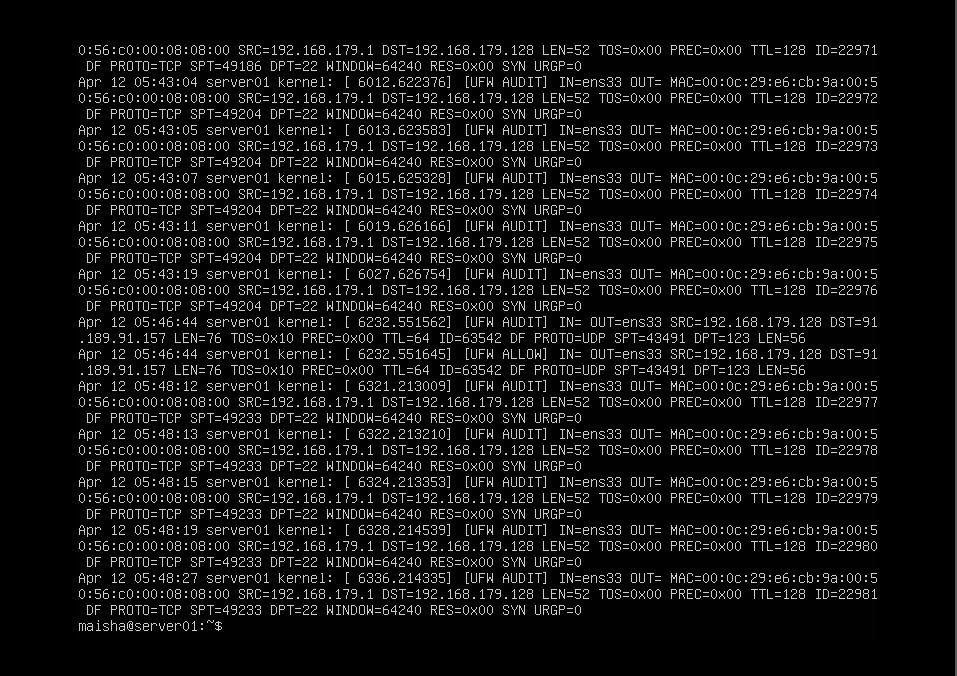
1. Adjust the firewall rule to limit only from your source IP allow to login. What is the syntax you have to apply?
   1. Open another ssh session to verify if you can login to the server. Can you able to login? Take a screenshot and paste it here.



Adjust the firewall’s logging from low to medium

* 1. *ufw logging medium*

1. Log out of your second SSH session and log back in
2. Read the firewall’s log messages
   1. *Sudo cat /var/log/ufw.log*
   2. Take a screenshot of the log messages and paste it here. Highlighted your ssh session.

cle

# Part 3: Install antivirus Software in Linux server

1. Install the ClamAV antivirus
   1. Update the package lists:

Sudo apt-get update

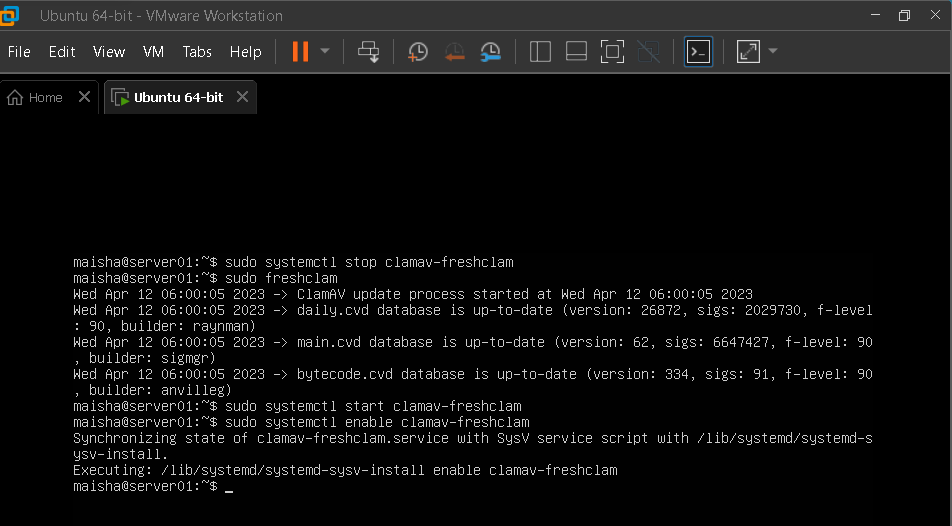
* 1. Install ClamAV

*apt-get install clamav clamav-daemon –y*

* 1. Take a screenshot of the results and paste it here

sudo

1. Update your ClamAV database
   1. *sudo systemctl stop clamav-freshclam*
   2. *sudo freshclam*
   3. *systemctl start clamav-freshclam*
   4. *systemctl enable clamav-freshclam*
   5. Take a screenshot of the results and paste it here

cle

1. Perform an infected scan on your own user’s home directory
   1. *clamscan infected /home/username*
   2. Take a screenshot of the results and paste it here

