# GNU+Linux with Shell Scripting – Day-3 Assignments

## Lab-1: Compromised Private Key

The private key that you used to login to your instance is compromised. Your goal is to change the key to a new one as soon as possible. Encrypt the key with a passphrase during its generation for an added layer of security. Change the SSH port on the remote machine from the default port 22 to 27243. Add SSH Configuration on your Mac to use this new port by default when to connect to the instance.

Ans :

Changing to new key for the VM instance

VM :

ssh-keygen -t rsa -b 4096 -m PEM -f ~/.ssh/hayagreevan-key.pem -C "Hayagreevan V"

cd ~/.ssh

mv authorized\_keys authorized\_keys\_old

cat hayagreevan-key.pem.pub >> authorized\_keys

Local Machine :

scp -i Hayagreevan\_Vijayakumar.pem ubuntu@3.215.73.224:/home/ubuntu/.ssh/hayagreevan-key.pem ~/Documents

ssh -i hayagreevan-key.pem ubuntu@3.215.73.224

Changing ssh port from 22 to 27243 :

VM:

sudo ufw allow 27243/tcp

nano /etc/ssh/sshd\_config (Add “Port 27243”)

sudo systemctl daemon-reload

sudo systemctl restart ssh

LM:

ssh -i Hayagreevan-key.pem [ubuntu@3.215.73.224](mailto:ubuntu@3.215.73.224) -p 27243

Setting ssh config in mac :

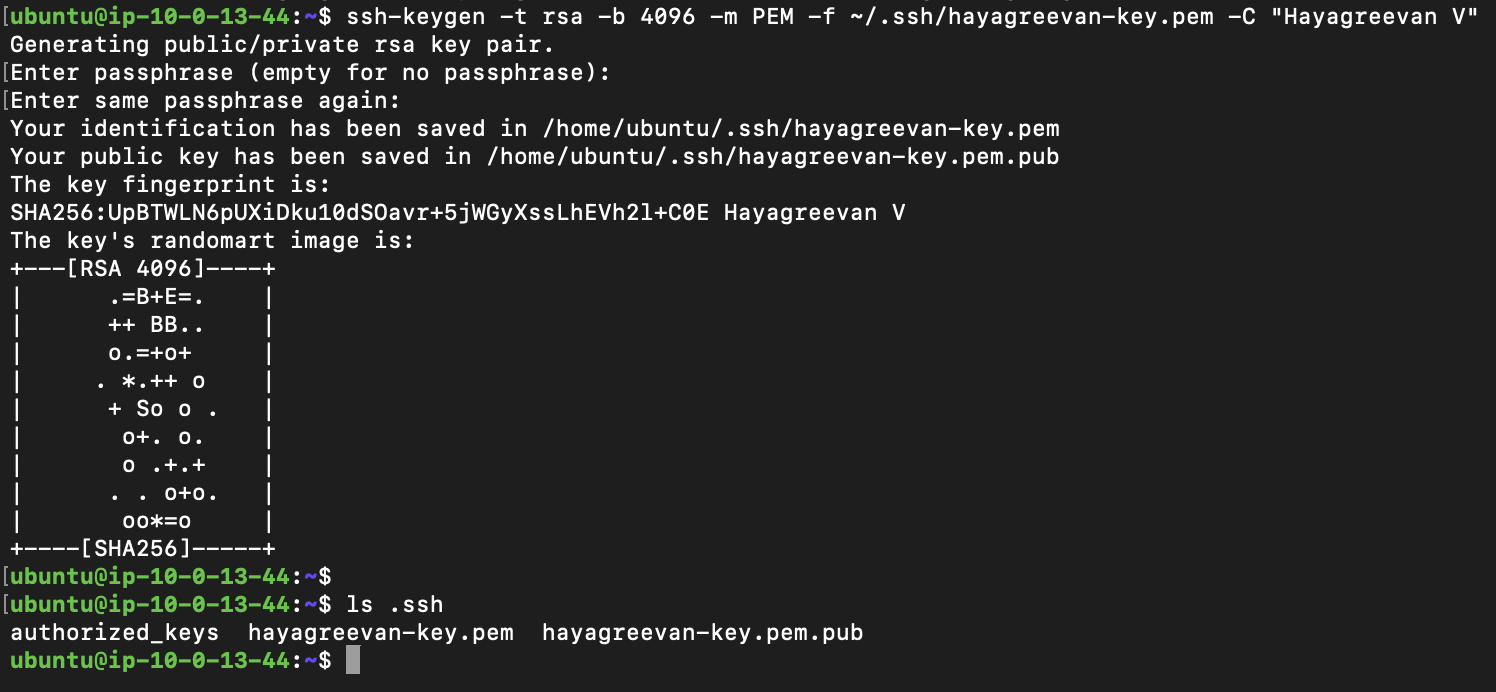
Host vm

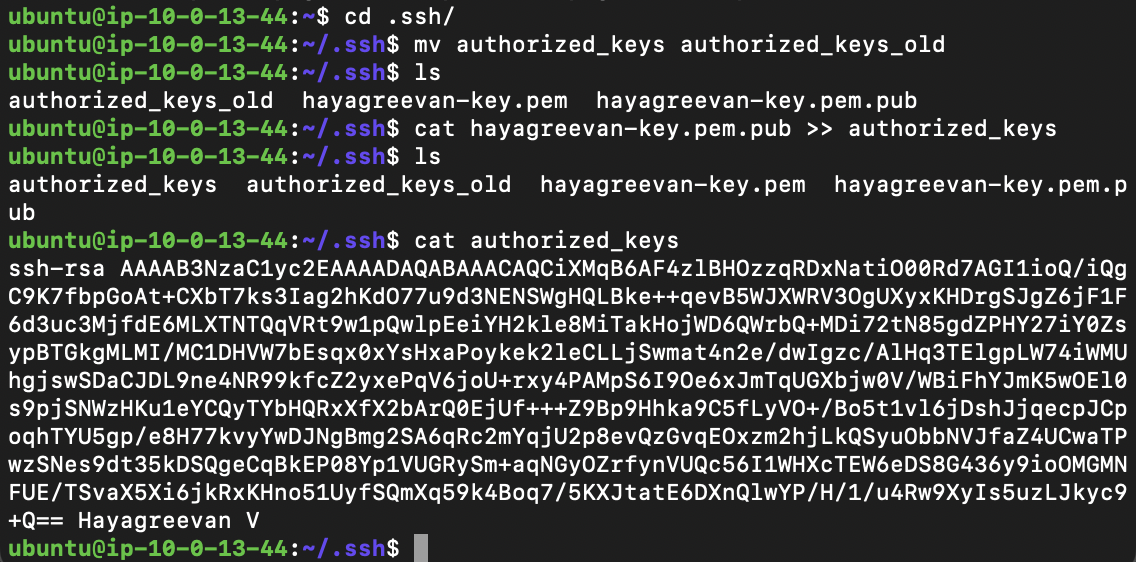
HostName 3.215.73.224

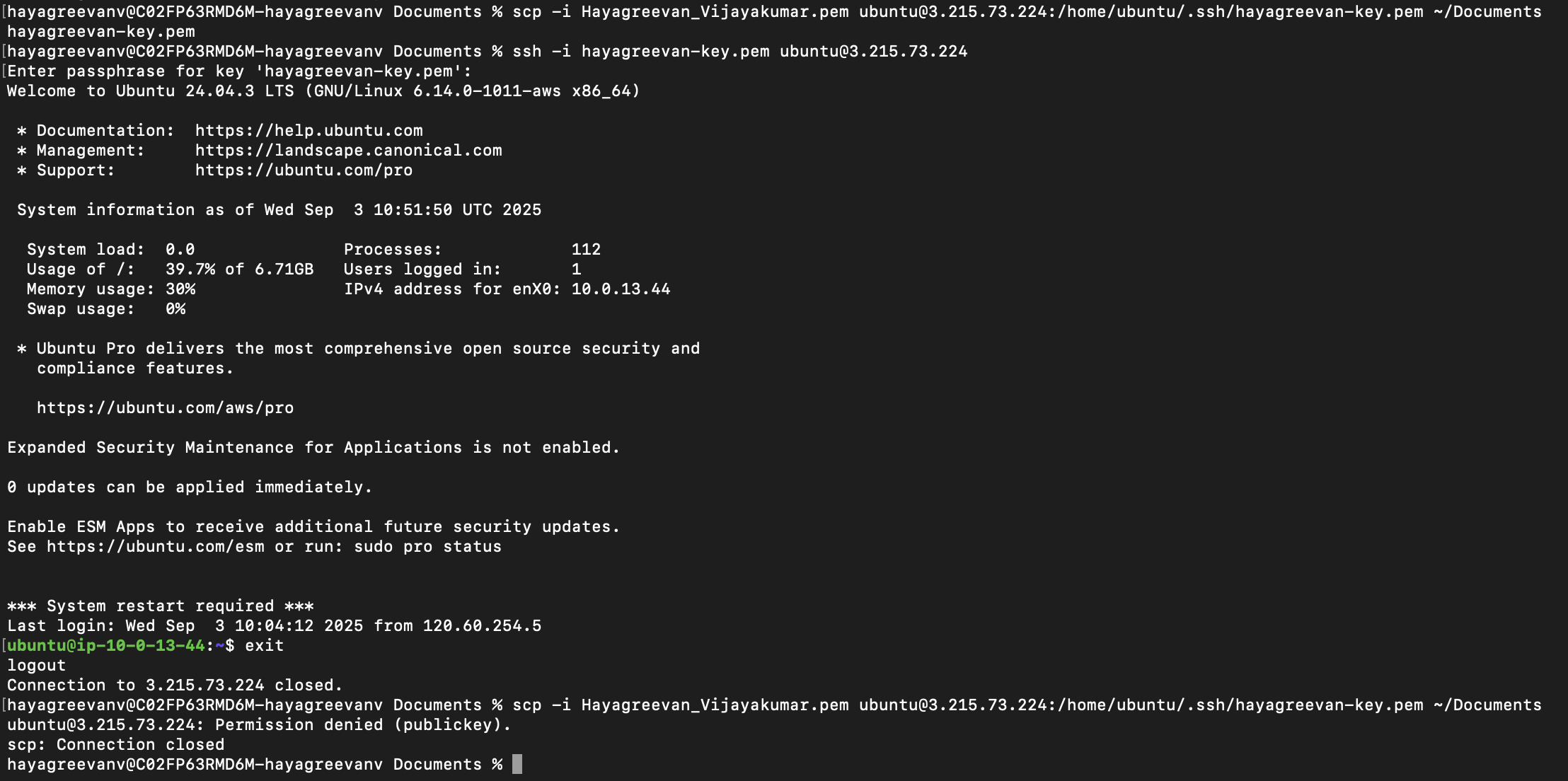
User ubuntu

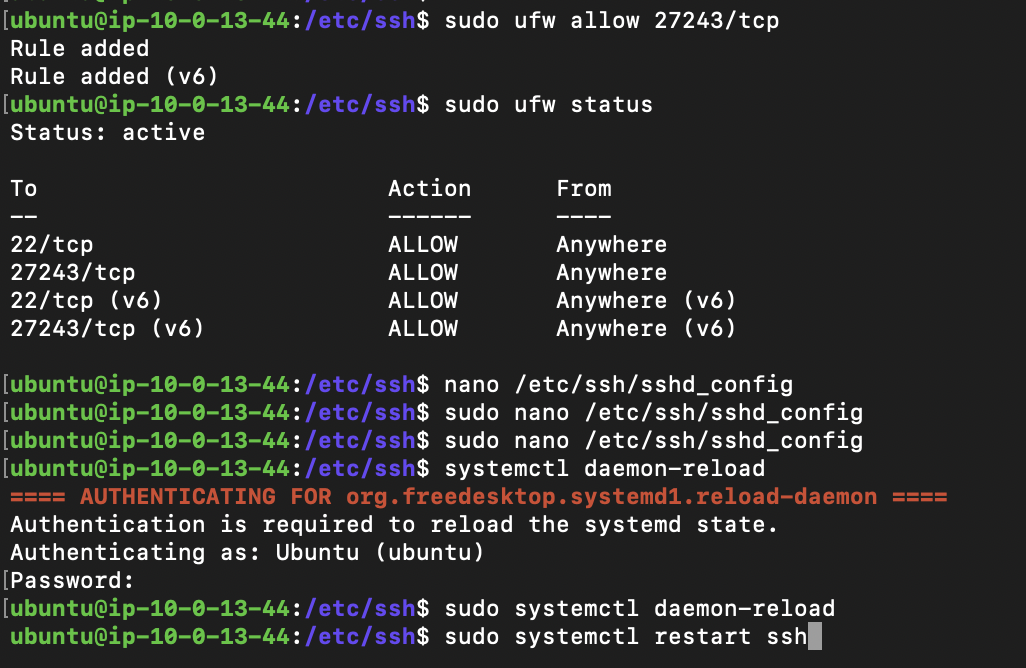
Port 27243

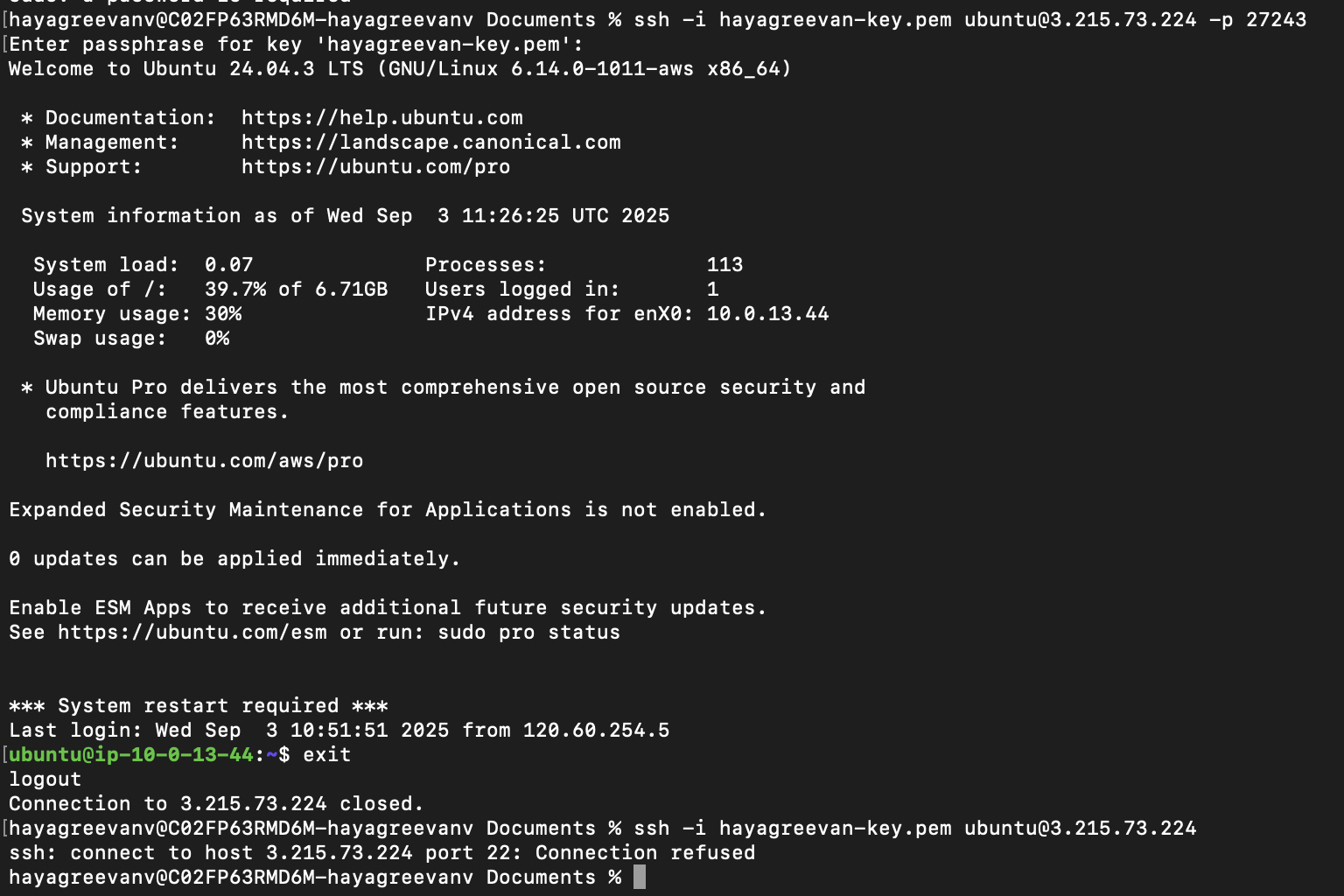
IdentityFile ~/.ssh/hayagreevan-vm-key.pem







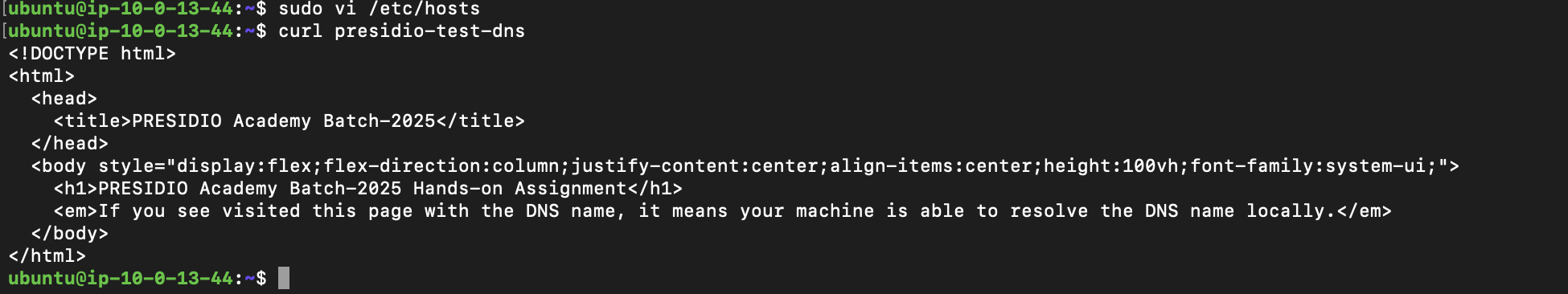


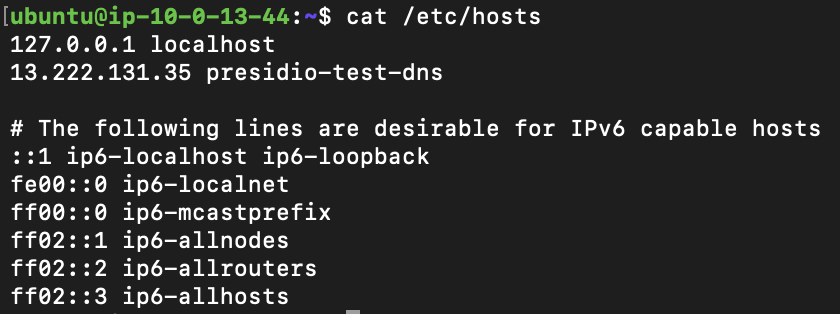


## Lab-2: Custom DNS Entry

There is a website running at 13.222.131.35 over port 80. The application (imaginary) in your system connects to it with a DNS name, not its IP address. Configure your compute instance to successfully resolve the DNS name (choose a DNS name of your own). Before that, check whether the server exists by pinging it. Check whether your compute instance is able to resolve the DNS name.

Ans : Add “13.222.131.35 <dns-name>” in /etc/hosts





## Lab-3: Zipping Files

Your audit team requires you to provide the log files in your system. Compress the folder /var/log/ as a tar ball and store it to /var/. Copy it to anyone of your friends' machine with scp and share the screenshot of it in your assignment.

Ans:

VM:

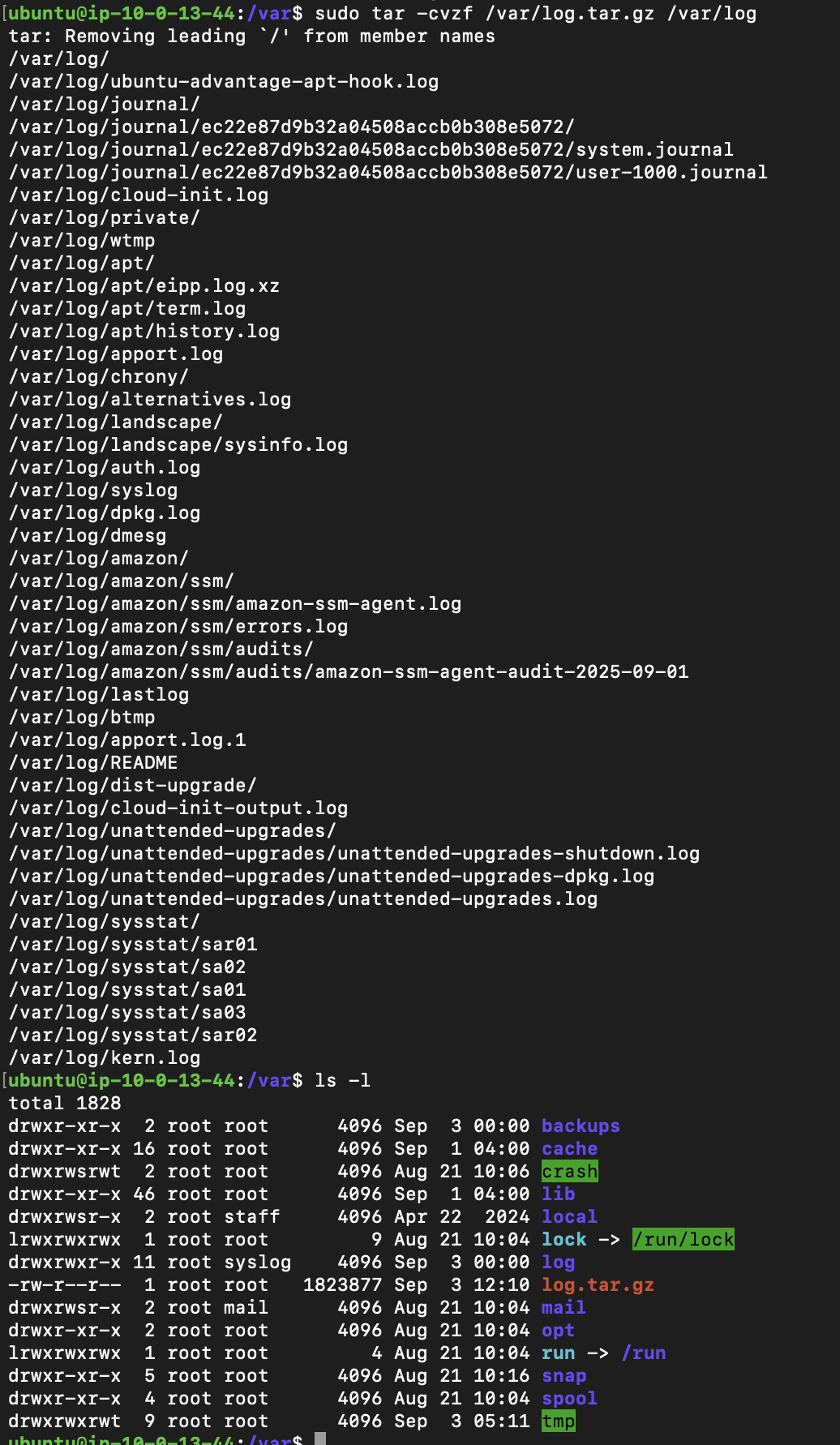
tar -cvzf /var/log.tar.gz /var/log

sudo mv /var/log.tar.gz ~

sudo chown ubuntu:ubuntu ~/log.tar.gz

Local Machine :

scp vm:/home/ubuntu/log.tar.gz ~/Downloads



File transfer between VMs using nc :

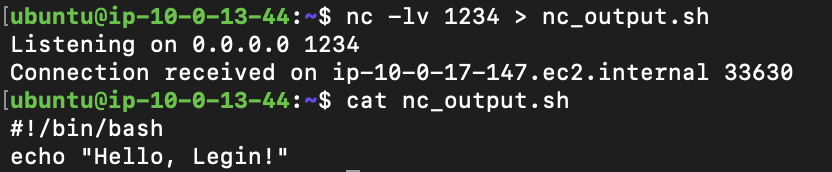
sudo ufw allow 1234/tcp

Reciever : nc -lv<port> > outputfile

nc -lv 1234 > output.tar.gz

Sender : nc <receiver-host-ip> <port> < inputfile

nc 10.0.17.147 1234 < log.tar.gz



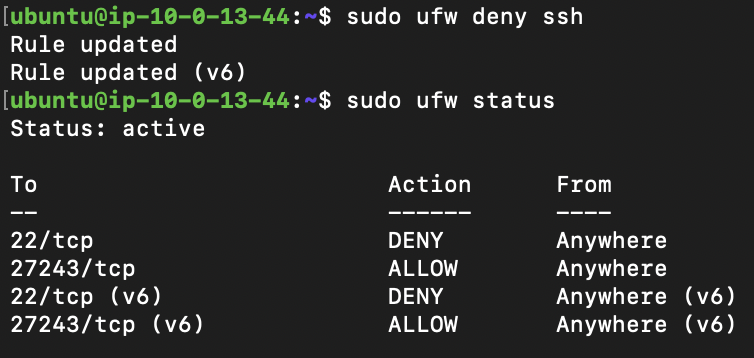
## Lab-4: Firewall Management

You have previously configured SSH to allow connections only in port 27243. Use your system’s firewall to block any incoming connections on port 22 and allow incoming connection on port 27243 only from your computer.

Ans : sudo ufw allow 27243

sudo ufw deny 22

sudo ufw status



## Lab-5: Package Management

Update and upgrade your system with the default package manager in your system. Install “cmatrix”, but before installing, get the description of the package. Finally, find the easter egg in your package manager.

Ans:

sudo apt update

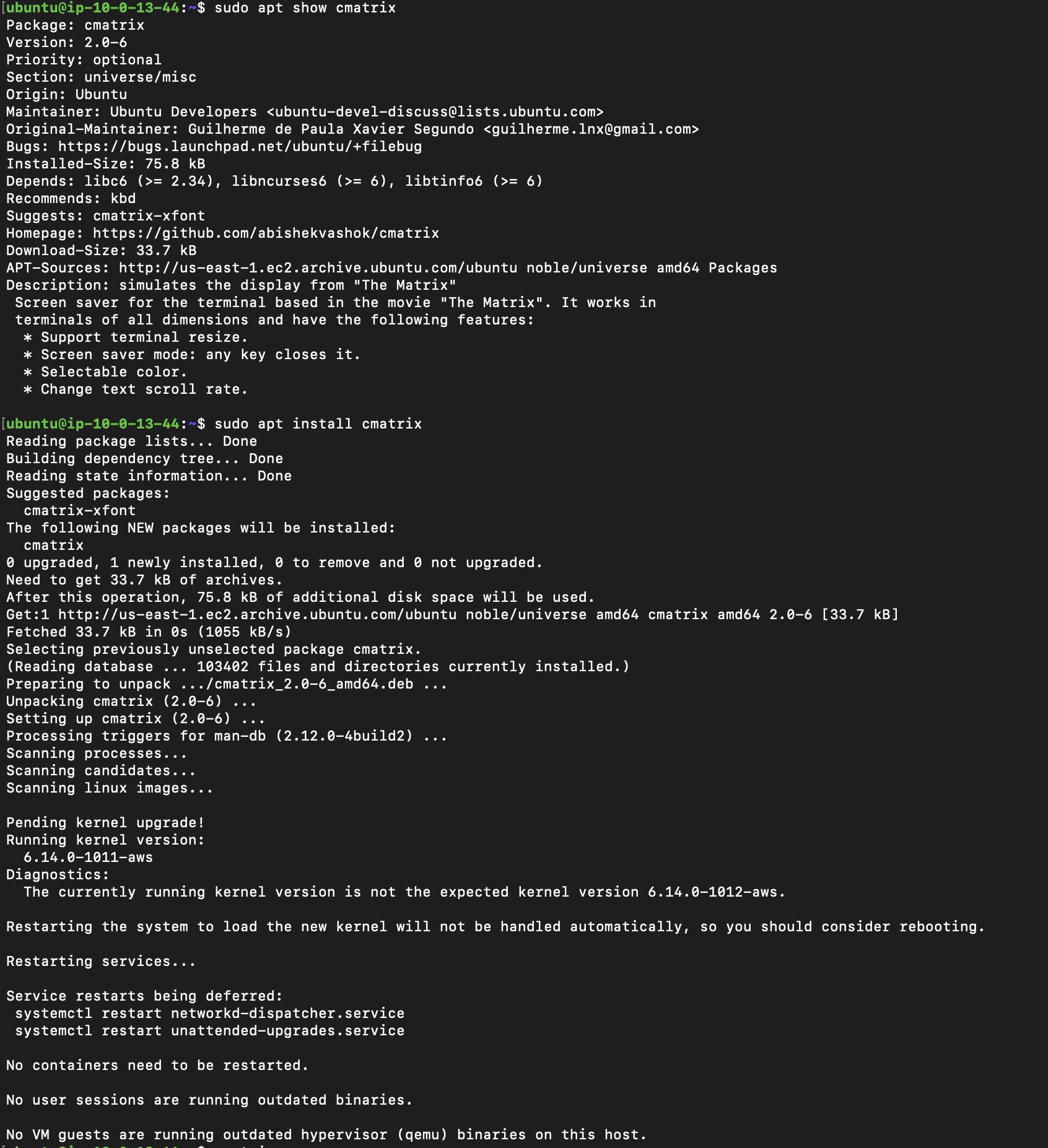
sudo apt upgrade

sudo apt list

sudo apt search cmatrix

sudo apt show cmatrix

sudo apt install cmatrix



Man: nc, telnet, ufw, tar, apt, scp, ssh

<https://www.cyberciti.biz/faq/ufw-allow-incoming-ssh-connections-from-a-specific-ip-address-subnet-on-ubuntu-debian/>

<https://www.cyberciti.biz/faq/howto-change-ssh-port-on-linux-or-unix-server/>

<https://linuxize.com/post/using-the-ssh-config-file/>

<https://www.freecodecamp.org/news/how-to-compress-files-in-linux-with-tar-command/>

<https://chatgpt.com/share/68b85fd9-e7d0-800a-946c-7e71eb8b371b>