Week 4 – Initial System Configuration & Security Implementation

Introduction

In Week 4, core security controls were implemented on the Ubuntu server. All administration was performed remotely from the Fedora workstation using SSH. The aim of this phase was to secure remote access, restrict network traffic, and apply proper user privilege management.

SSH Key-Based Authentication

SSH key-based authentication was configured to replace password-based login. This improves security by preventing brute-force password attacks.

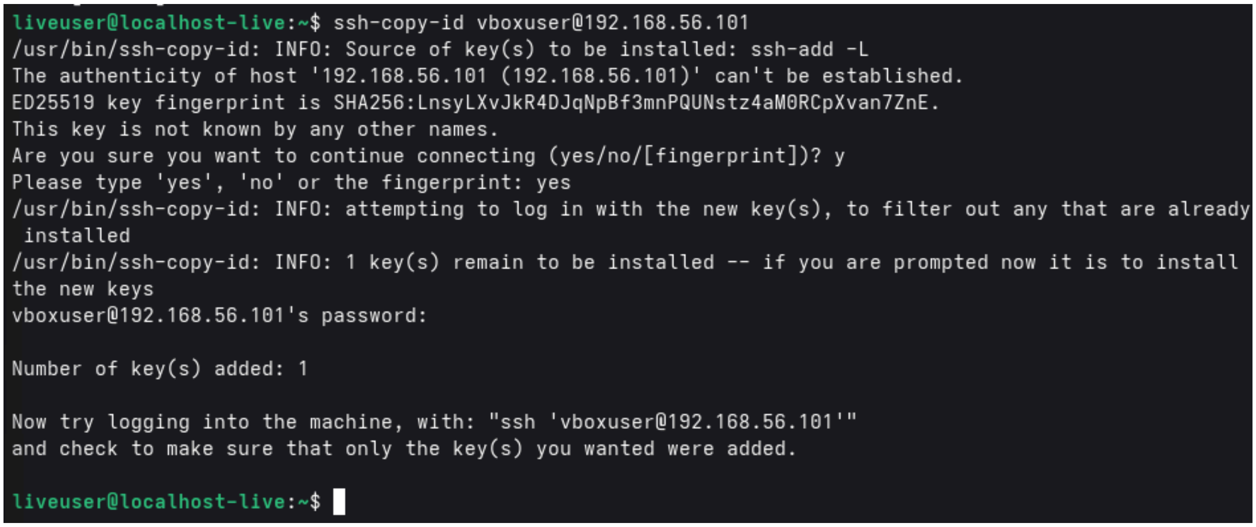
Key Generation (Workstation)

```
ssh-keygen -t ed25519
```

What this does:
Generates a secure public–private key pair used for passwordless SSH authentication.

Copy Public Key to Server

```
ssh-copy-id user@192.168.56.101
```



```
liveuser@localhost-live:~$ ssh-copy-id vboxuser@192.168.56.101
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ssh-add -L
The authenticity of host '192.168.56.101 (192.168.56.101)' can't be established.
ED25519 key fingerprint is SHA256:LnsyLXvJkR4DJqNpBf3mnPQUNstz4aM0RCpXvan7ZnE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already
 installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install
the new keys
vboxuser@192.168.56.101's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'vboxuser@192.168.56.101'"
and check to make sure that only the key(s) you wanted were added.

liveuser@localhost-live:~$ 
```

What this does:

Allowing secure login without a password.

SSH Configuration Hardening (Server)

```
sudo nano /etc/ssh/sshd_config
```

What this does:
Opens the SSH configuration file to disable insecure options and enforce stronger authentication.

```
PasswordAuthentication no
PermitRootLogin no
```

Restart SSH Service

```
sudo systemctl restart ssh
```

What this does:
Applies the updated SSH configuration by restarting the SSH service.

Firewall Configuration (UFW)

A firewall was configured to allow SSH access **only from the Fedora workstation**.

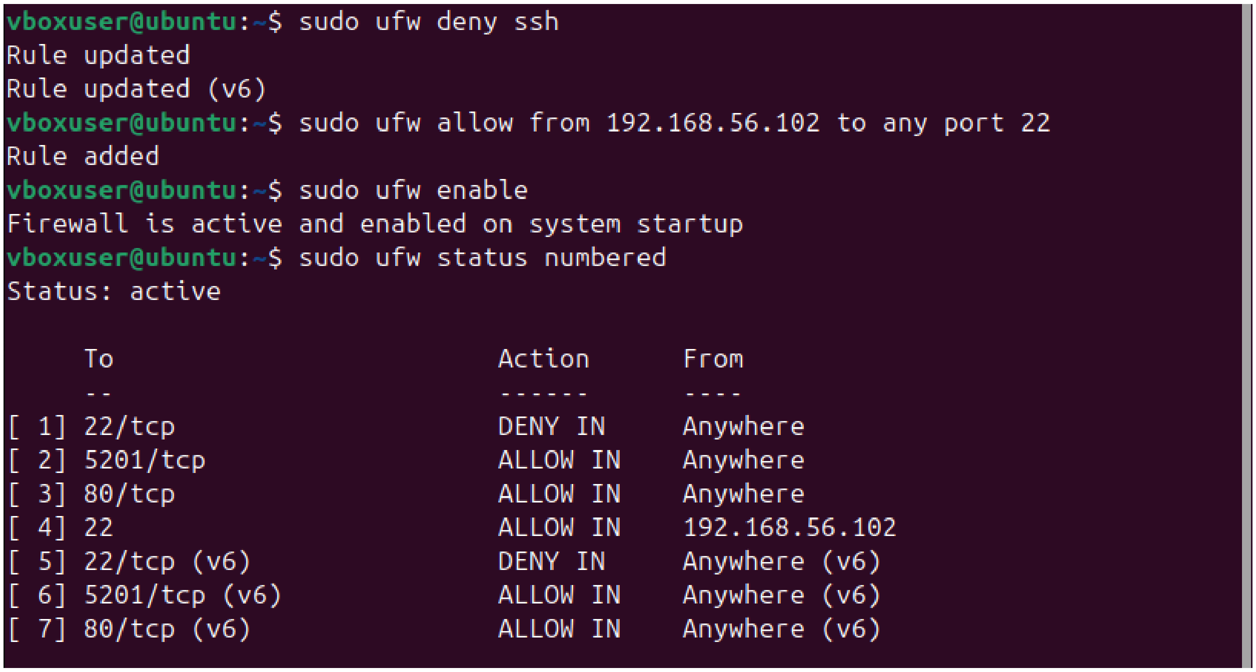
Enable Firewall

```
sudo ufw enable
```

What this does:
Activates the Uncomplicated Firewall to block all traffic by default unless explicitly allowed.

Allow SSH from Workstation Only

```
sudo ufw allow from 192.168.56.102 to any port 22
```



```
vboxuser@ubuntu:~$ sudo ufw deny ssh
Rule updated
Rule updated (v6)
vboxuser@ubuntu:~$ sudo ufw allow from 192.168.56.102 to any port 22
Rule added
vboxuser@ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
vboxuser@ubuntu:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     DENY IN     Anywhere
[ 2] 5201/tcp                   ALLOW IN    Anywhere
[ 3] 80/tcp                     ALLOW IN    Anywhere
[ 4] 22                         ALLOW IN    192.168.56.102
[ 5] 22/tcp (v6)                DENY IN     Anywhere (v6)
[ 6] 5201/tcp (v6)              ALLOW IN    Anywhere (v6)
[ 7] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
```

What this does:
Allows SSH connections only from the Fedora workstation IP, blocking all other sources.

Check Firewall Rules

```
sudo ufw status verbose
```

What this does:
Displays all active firewall rules and confirms that SSH access is restricted correctly.

User and Privilege Management

A non-root administrative user was created to follow the principle of least privilege.

Create New User

```
sudo adduser adminuser
```

What this does:
Creates a new user account for administrative tasks instead of using the root account.

Grant Sudo Privileges

```
sudo usermod -aG sudo adminuser
```

What this does:
Adds the user to the sudo group, allowing administrative commands when required.

Verify Sudo Access

```
sudo whoami
```

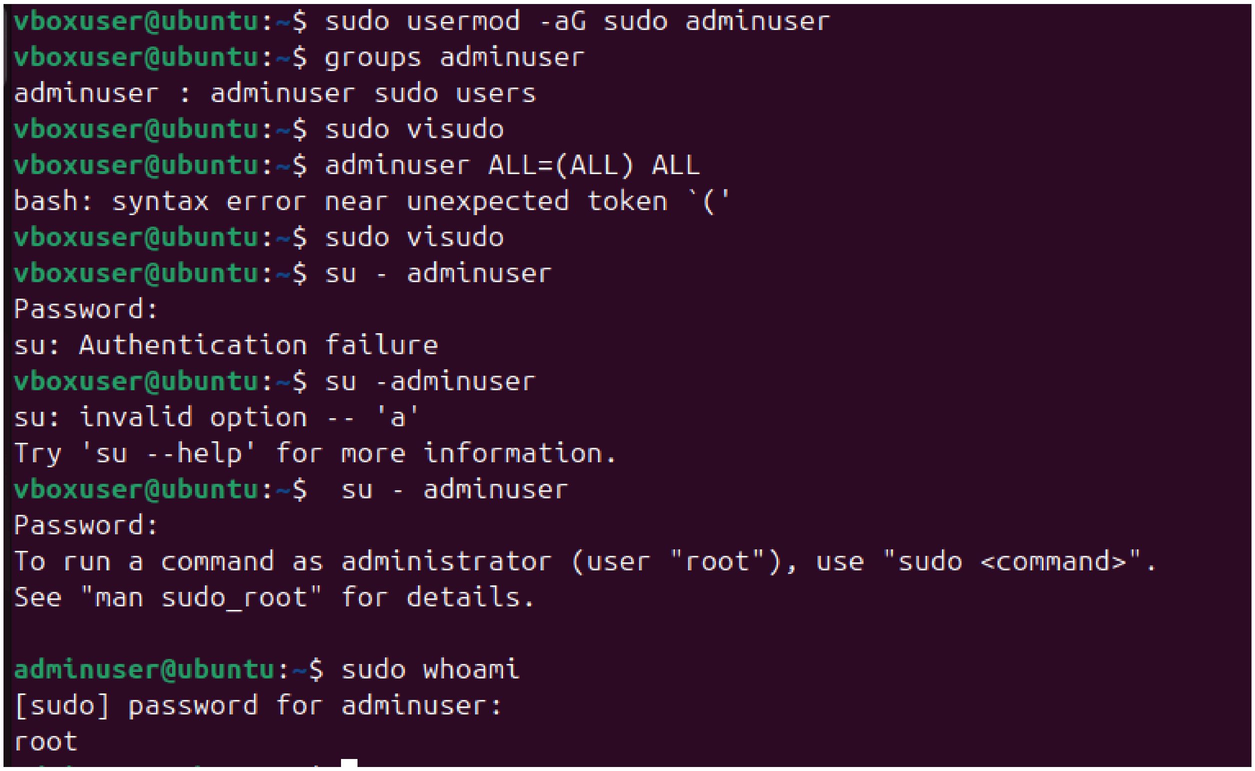
What this does:
Confirms that the user can execute commands with administrative privileges.

Remote Administration Evidence

All configuration tasks were executed remotely from the Fedora workstation using SSH.

```
ssh adminuser@192.168.56.101
```

What this does:
Establishes a secure remote session to the Ubuntu server for command-line administration.



```
vboxuser@ubuntu:~$ sudo usermod -aG sudo adminuser
vboxuser@ubuntu:~$ groups adminuser
adminuser : adminuser sudo users
vboxuser@ubuntu:~$ sudo visudo
vboxuser@ubuntu:~$ adminuser ALL=(ALL) ALL
bash: syntax error near unexpected token `('
vboxuser@ubuntu:~$ sudo visudo
vboxuser@ubuntu:~$ su - adminuser
Password:
su: Authentication failure
vboxuser@ubuntu:~$ su -adminuser
su: invalid option -- 'a'
Try 'su --help' for more information.
vboxuser@ubuntu:~$  su - adminuser
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

adminuser@ubuntu:~$ sudo whoami
[sudo] password for adminuser:
root
```