

WEEK 4: JOURNAL PHASE 4: Initial System Configuration & Security

Task: System configuration and security setup using SSH

Machines Used: Linux Mint (workstation) and Ubuntu (server)

1. SSH Key-Based Authentication

For this part, I used Linux Mint to connect to my Ubuntu server.

I created an SSH key on Linux Mint and copied it to Ubuntu using:

```
ssh-copy-id abdulazeer@192.168.56.101
```

After that, I tested the connection and it logged me in without asking for a password, which shows the key-based authentication is working.

```
abulazeer@VirtualBox:~$ ssh-copy-id abdulazeer@192.168.56.101
/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
abdulazeer@192.168.56.101's password:

Number of key(s) added: 1

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

abulazeer@VirtualBox:~$ ssh abdulazeer@192.168.56.101
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-35-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

6 updates can be applied immediately.
3 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Last login: Sat Nov 1 11:39:14 2025 from 192.168.56.102
abdulazeer@Ubuntu:~$
```

2. Firewall Configuration (Only allow Mint to connect)

On Ubuntu, I enabled the firewall (UFW) and set it so only my Mint machine (192.168.56.102) can connect through SSH.

Commands used:

sudo ufw enable

sudo ufw allow from 192.168.56.102 to any port 22

sudo ufw deny 22

sudo ufw status verbose

```
abdulazeer@Ubuntu:~$ sudo ufw enable
[sudo] password for abdulazeer:
Firewall is active and enabled on system startup
abdulazeer@Ubuntu:~$ sudo ufw allow from 192.168.56.102 to any port 22
Rule added
abdulazeer@Ubuntu:~$ sudo ufw deny 22
Rule added
Rule added (v6)
abdulazeer@Ubuntu:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: allow (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
22/tcp (OpenSSH) ALLOW IN Anywhere
22 ALLOW IN 192.168.56.102
22 DENY IN Anywhere
22/tcp (OpenSSH (v6)) ALLOW IN Anywhere (v6)
22 (v6) DENY IN Anywhere (v6)

abdulazeer@Ubuntu:~$
```

3. sshd_config Before and After Change

I opened the SSH config file using:

sudo nano /etc/ssh/sshd_config

My file didn't have "PasswordAuthentication yes", so I added:

PasswordAuthentication no

Then restarted SSH:

sudo systemctl restart ssh

```
adminuser@Ubuntu: ~  
Get:13 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [206 kB]  
Get:14 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [71.5 kB]  
Get:15 http://security.ubuntu.com/ubuntu noble-security/universe Icons (48x48) [46.6 kB]  
Get:16 http://security.ubuntu.com/ubuntu noble-security/universe Icons (64x64) [72.9 kB]  
Get:17 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [19.5 kB]  
Get:18 http://gb.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1,620 kB]  
Get:19 http://security.ubuntu.com/ubuntu noble-security/multiverse Translation-en [5,956 B]  
Get:20 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]  
Get:21 http://gb.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [303 kB]  
Get:22 http://gb.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [175 kB]  
Get:23 http://gb.archive.ubuntu.com/ubuntu noble-updates/main Icons (48x48) [36.0 kB]  
Get:24 http://gb.archive.ubuntu.com/ubuntu noble-updates/main Icons (64x64) [51.0 kB]  
Get:25 http://gb.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [15.7 kB]  
Get:26 http://gb.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [2,307 kB]  
Get:27 http://gb.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [526 kB]  
Get:28 http://gb.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]  
Get:29 http://gb.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1,500 kB]  
Get:30 http://gb.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [304 kB]  
Get:31 http://gb.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [377 kB]  
Get:32 http://gb.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [31.4 kB]  
Get:33 http://gb.archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [5,808 B]  
Get:34 http://gb.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]  
Get:35 http://gb.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [7,148 B]  
Get:36 http://gb.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]  
Get:37 http://gb.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [11.0 kB]  
Get:38 http://gb.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]  
Fetched 13.3 MB in 2s (5,504 kB/s)  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
104 packages can be upgraded. Run 'apt list --upgradable' to see them.  
adminuser@Ubuntu: $  
  
abdulazeer@Ubuntu:~$ sudo ufw status verbose  
Status: active  
Logging: on (low)  
Default: allow (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  
  
To Action From  
--  
22/tcp (OpenSSH) ALLOW IN Anywhere  
22 ALLOW IN 192.168.56.102  
22 DENY IN Anywhere  
22/tcp (OpenSSH (v6)) ALLOW IN Anywhere (v6)  
22 (v6) DENY IN Anywhere (v6)  
  
abdulazeer@Ubuntu:~$ sudo nano /etc/ssh/sshd_config  
abdulazeer@Ubuntu:~$ sudo systemctl restart ssh  
abdulazeer@Ubuntu:~$ sudo nano /etc/ssh/sshd_config  
abdulazeer@Ubuntu:~$ sudo systemctl restart ssh  
abdulazeer@Ubuntu:~$
```

4. Creating a Non-Root Admin User

I created a new admin user called adminuser:

```
sudo adduser adminuser
```

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

Then switched to the account and tested sudo:

```
su - adminuser
```

```
sudo apt update
```

```
adminuser@Ubuntu:~$ sudo ufw status numbered
Status: active

      To Action      From
      --  -
[ 1] OpenSSH      ALLOW IN    Anywhere
[ 2] 22           ALLOW IN    192.168.56.102
[ 3] 22           DENY IN     Anywhere
[ 4] OpenSSH (v6) ALLOW IN    Anywhere (v6)
[ 5] 22 (v6)      DENY IN     Anywhere (v6)

adminuser@Ubuntu:~$
```

5. Remote Administration Through SSH

All my changes on Ubuntu were done from Linux Mint using SSH.

Commands like:

```
sudo apt update
```

```
uname -a
```

prove the remote management is working.

6. Firewall Rules Documentation (Numbered)

I used:

```
sudo ufw status numbered
```

This shows the exact firewall rule order.

Conclusion

In Week 4, I configured secure access to my server. I set up SSH keys, updated the SSH configuration, created an admin user, and restricted the firewall to only my workstation. Everything was done through SSH with screenshots as evidence.