

Week 4 — Initial System Configuration & Core Security Implementation

Overview

Week 4 focuses on the **deployment of the Linux server and implementation of foundational security controls**. This phase transitions from planning to practical execution and establishes a secure baseline configuration for the operating system. All administrative tasks were performed **remotely via SSH** from the workstation, enforcing command-line proficiency and reflecting real-world server management practices.

The core objective of this week is to secure remote access, restrict network exposure, and enforce least-privilege user management while maintaining system usability and performance.

Objectives

- Configure secure SSH access using key-based authentication
 - Disable insecure authentication mechanisms
 - Implement host-based firewall rules
 - Enforce least-privilege user and privilege management
 - Document configuration changes with before-and-after evidence
-

Deliverables

- SSH key-based authentication configuration
 - Firewall configuration with restricted access
 - Non-root administrative user configuration
 - Remote administration evidence via SSH
 - Configuration file comparisons
-

1. Secure Shell (SSH) Configuration

1.1 SSH Key-Based Authentication

To improve authentication security, SSH key-based authentication was configured to replace password-based login. This mitigates brute-force attacks and aligns with industry best practices.

Key Generation (Workstation):

`ssh-keygen`

Public Key Deployment (Server):

`ssh-copy-id adminuser@192.168.56.103`

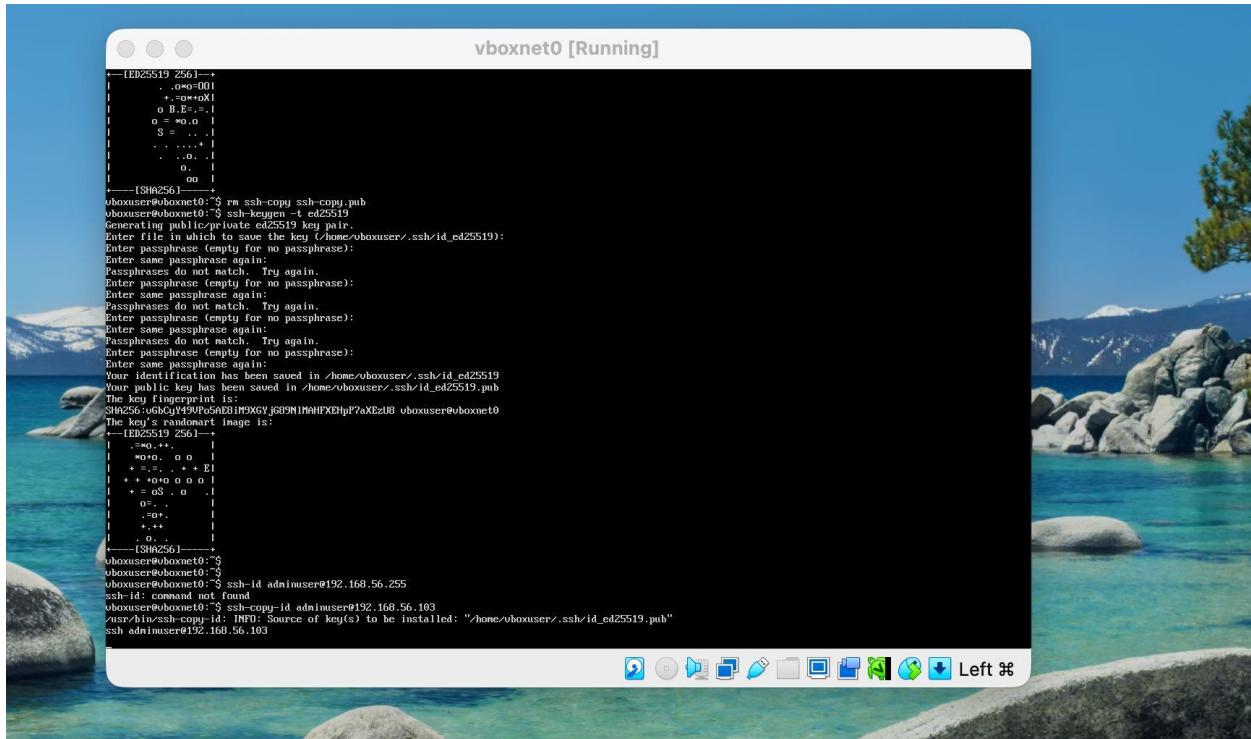


Figure W4-1: SSH key-based authentication configured successfully.

1.2 SSH Hardening

The SSH daemon configuration file was modified to disable insecure options.

Configuration File: `/etc/ssh/sshd_config`

Before Configuration:

```
#PasswordAuthentication yes  
#PermitRootLogin yes
```

After Configuration:

```
PasswordAuthentication no  
PermitRootLogin no
```

The SSH service was restarted to apply the changes:

```
sudo systemctl restart ssh
```

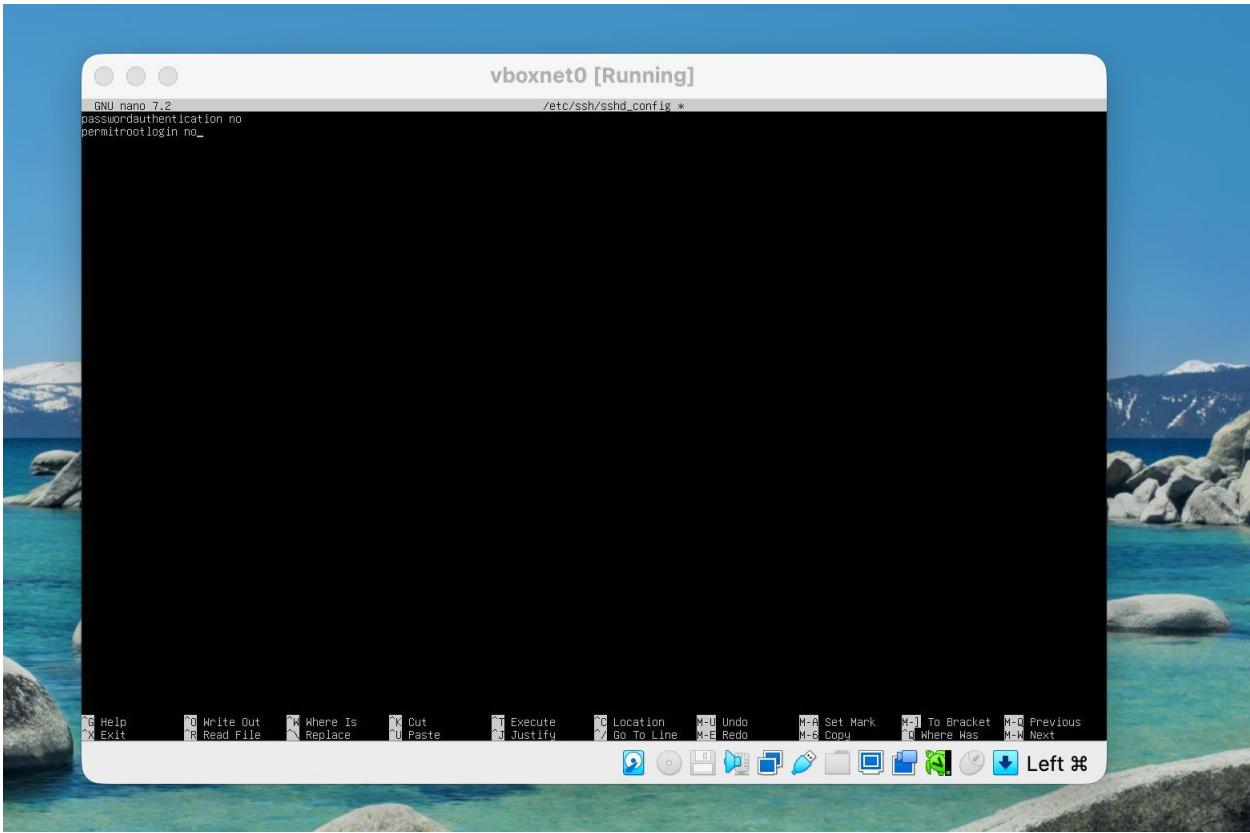


Figure W4-2: SSH configuration before and after hardening.

2. User and Privilege Management

2.1 Non-Root Administrative User

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

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

Root login was disabled for routine administration, reducing the impact of potential credential compromise.

```

vboxnet0 [Running]

Usage of /:
Memory usage: 4x
Swap usage: 0x
Processes: 99
Users logged in: 0
IPv4 address for enp0s8: 10.0.2.15
IPv6 address for enp0s8: fd17:625c:f037:2:a00:27ff:fe15:10ff

Expanded Security Maintenance for Applications is not enabled.
34 updates can be applied immediately.
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

Failed to connect to https://changelogs.ubuntu.com/meta-release-its. Check your Internet connection or proxy settings

vboxuser@vboxnet0:~$ sudo adduser adminuser
[sudo] password for vboxuser:
info: Adding user `adminuser' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `adminuser' (1001) ...
info: Adding new user `adminuser' (1001) with group `adminuser (1001)' ...
info: Creating home directory `/home/adminuser' ...
info: Copying files from `/etc/skel' ...

password:
Retype new password:
password updated successfully
Changing the user information for adminuser
Enter the new value, or press ENTER for the default
  Full Name []: suagat thanu
  Room Number []: 10
  Work Phone []: 11
  Home Phone []: 12
  Other []: 13
Is the information correct? [Y/n] yes
info: Adding new user `adminuser' to supplemental / extra groups `users' ...
info: Adding user `adminuser' to group `users' ...
vboxuser@vboxnet0:~$ sudo usermod -aG sudo adminuser
vboxuser@vboxnet0:~$ getent
getent: wrong number of arguments
Try 'getent --help' or 'getent --usage' for more information.
vboxuser@vboxnet0:~$ getent group sudo
sudo:x:27:vboxuser,adminuser
vboxuser@vboxnet0:~$ sudo:x:27:adminuser
sudo:x:27:adminuser: command not found
vboxuser@vboxnet0:~$
```

Figure W4-3: Non-root administrative user configuration.

3. Firewall Configuration (UFW)

3.1 Firewall Policy

A host-based firewall was configured using **UFW (Uncomplicated Firewall)** to restrict network access.

Firewall Rules Implemented: - Default deny incoming traffic - Allow SSH access only from the trusted workstation IP

```

sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow from 192.168.56.1 to any port 22
sudo ufw enable
sudo ufw status verbose
```

This configuration significantly reduces the server's attack surface while maintaining required remote access.

vboxnet0 [Running]

```
uboxnet0 Login: uboxuser
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-90-generic aarch64)

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

System information as of Thu Dec 18 08:16:39 AM UTC 2025

System load: 0.0
Usage of /: 8.6% of 33.21GB
Memory usage: 4%
Swap usage: 0%
Processes: 96
Users logged in: 0
IPv4 address for emp0s8: 10.0.2.15
IPv6 address for emp0s8: fd17:625c:f037:2:a00:27ff:fe15:18f6

Expanded Security Maintenance for Applications is not enabled.

34 updates can be applied immediately.
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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

uboxuser@vboxnet0:~$ sudo ufw default deny incoming
[sudo] password for uboxuser:
Default incoming policy changed to 'deny'
(see sure to update your rules accordingly)
uboxuser@vboxnet0:~$ sudo ufw allow from 192.168.56.1 to any port 22
Rules updated
uboxuser@vboxnet0:~$ sudo ufw enable
Firewall is active and enabled on system startup
uboxuser@vboxnet0:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To           Action      From
22           ALLOW IN   192.168.56.1

uboxuser@vboxnet0:~$
```

Figure W4-4: UFW firewall rules showing restricted SSH access.

4. Remote Administration Evidence

All system configuration tasks were executed remotely from the workstation using SSH, demonstrating adherence to the coursework's administrative constraints.

Example remote command execution:

```
ssh adminuser@192.168.56.103
hostname
whoami
uptime
```

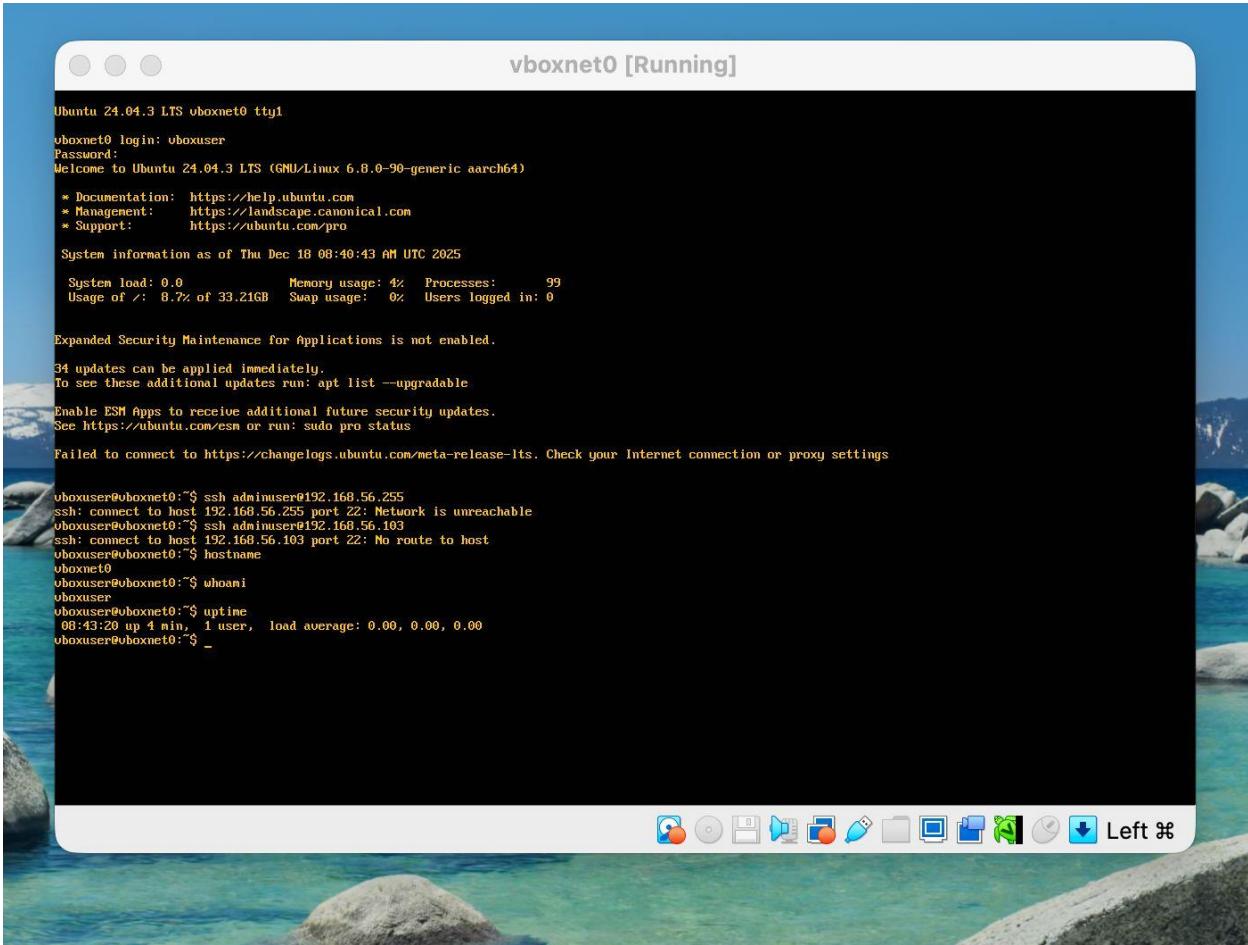


Figure W4-5: Evidence of remote administration via SSH.

5. Configuration Validation

The following checks were performed to validate the security configuration:

- SSH password authentication disabled
- Root login blocked
- Firewall enabled and active
- SSH access restricted to trusted IP

```
sudo sshd -T | grep -E 'passwordauthentication|permitrootlogin'  
sudo ufw status
```

These validation steps confirm that the foundational security controls are functioning as intended.

6. Reflection

Key Security Improvements

- Eliminated password-based SSH authentication
- Reduced risk of brute-force and credential-based attacks
- Enforced least-privilege access model
- Limited network exposure through strict firewall rules

Challenges Encountered

- Risk of locking out SSH access during configuration
- Ensuring firewall rules were applied correctly before enabling UFW

Learning Outcomes Achieved

- ✓Implementing secure remote access mechanisms
- ✓Applying user privilege management principles
- ✓Configuring host-based firewalls
- ✓Performing secure system administration via SSH

This week directly supports **Learning Outcome 3** by implementing operating system security mechanisms and **Learning Outcome 4** by demonstrating practical command-line administration skills.

References

- OpenSSH Hardening Guide. Available:
<https://www.ssh.com/academy/ssh/security> (Accessed: 2025)
- Ubuntu UFW Documentation. Available:
<https://help.ubuntu.com/community/UFW> (Accessed: 2025)