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
```

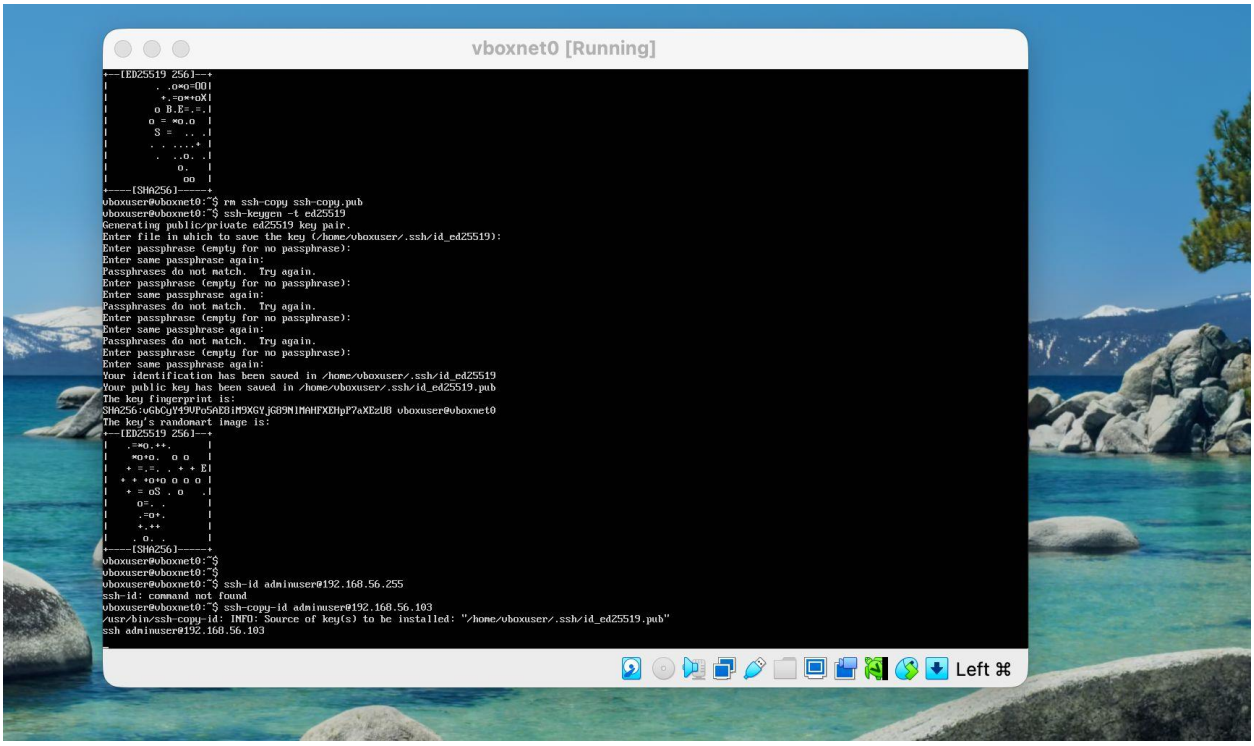

Figure W4-1: SSH key-based authentication configured successfully.

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
```

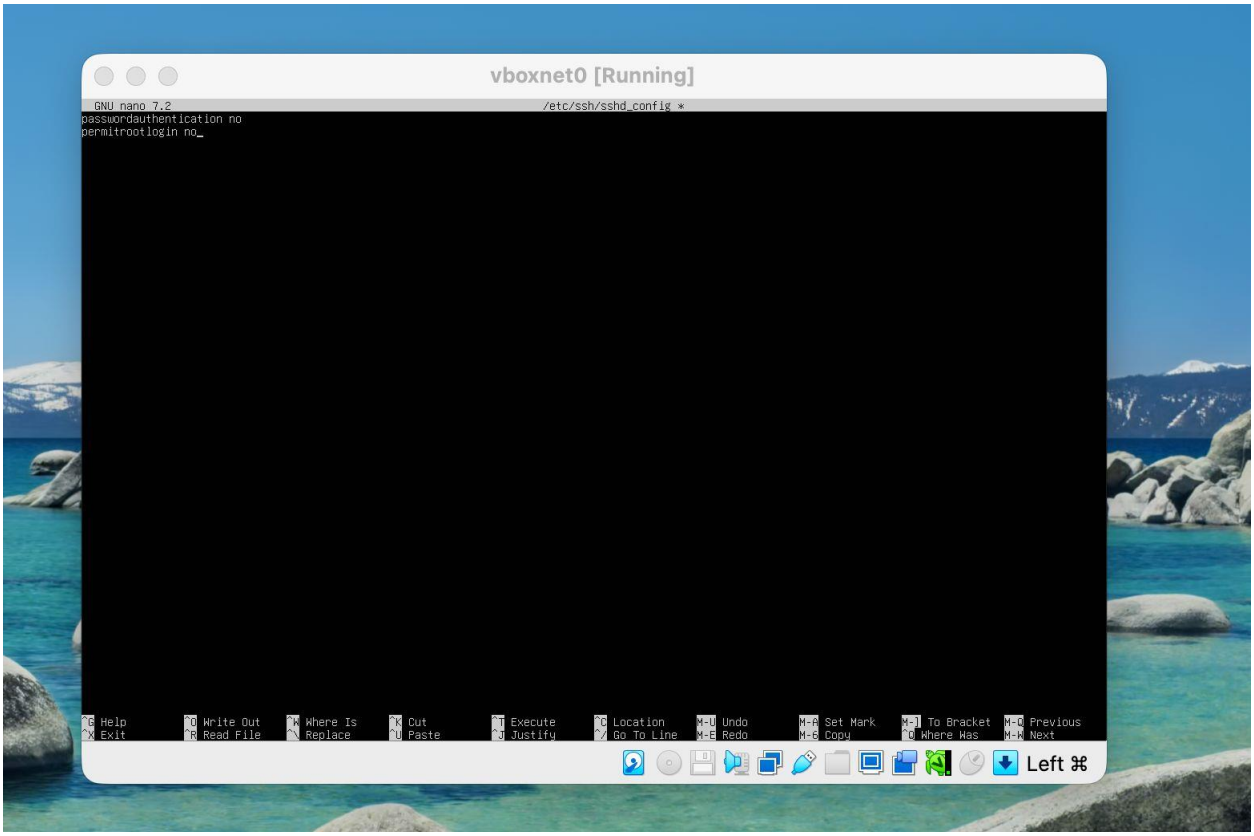

Figure W4-2: SSH configuration before and after hardening.

---

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.

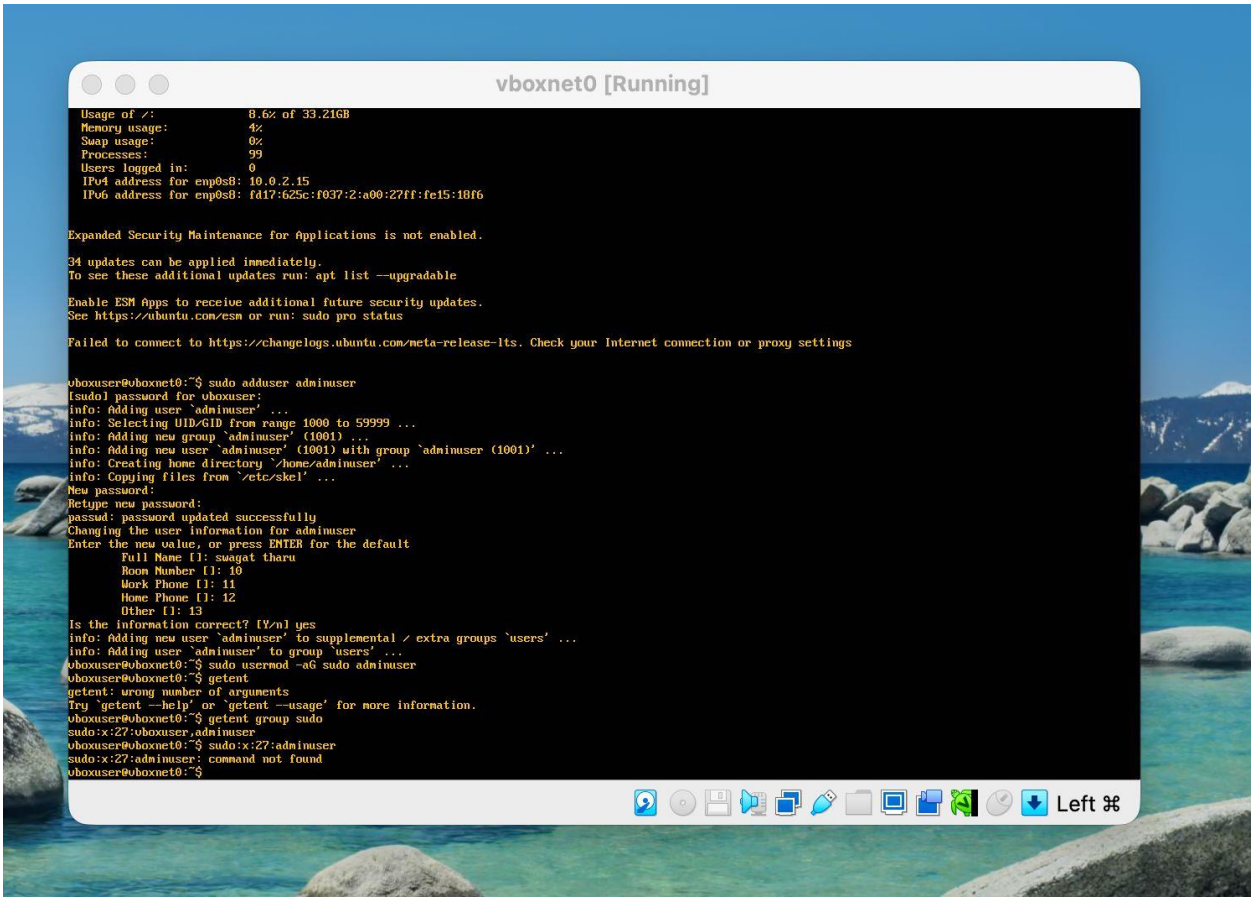

Figure W4-3: Non-root administrative user configuration.

---

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.

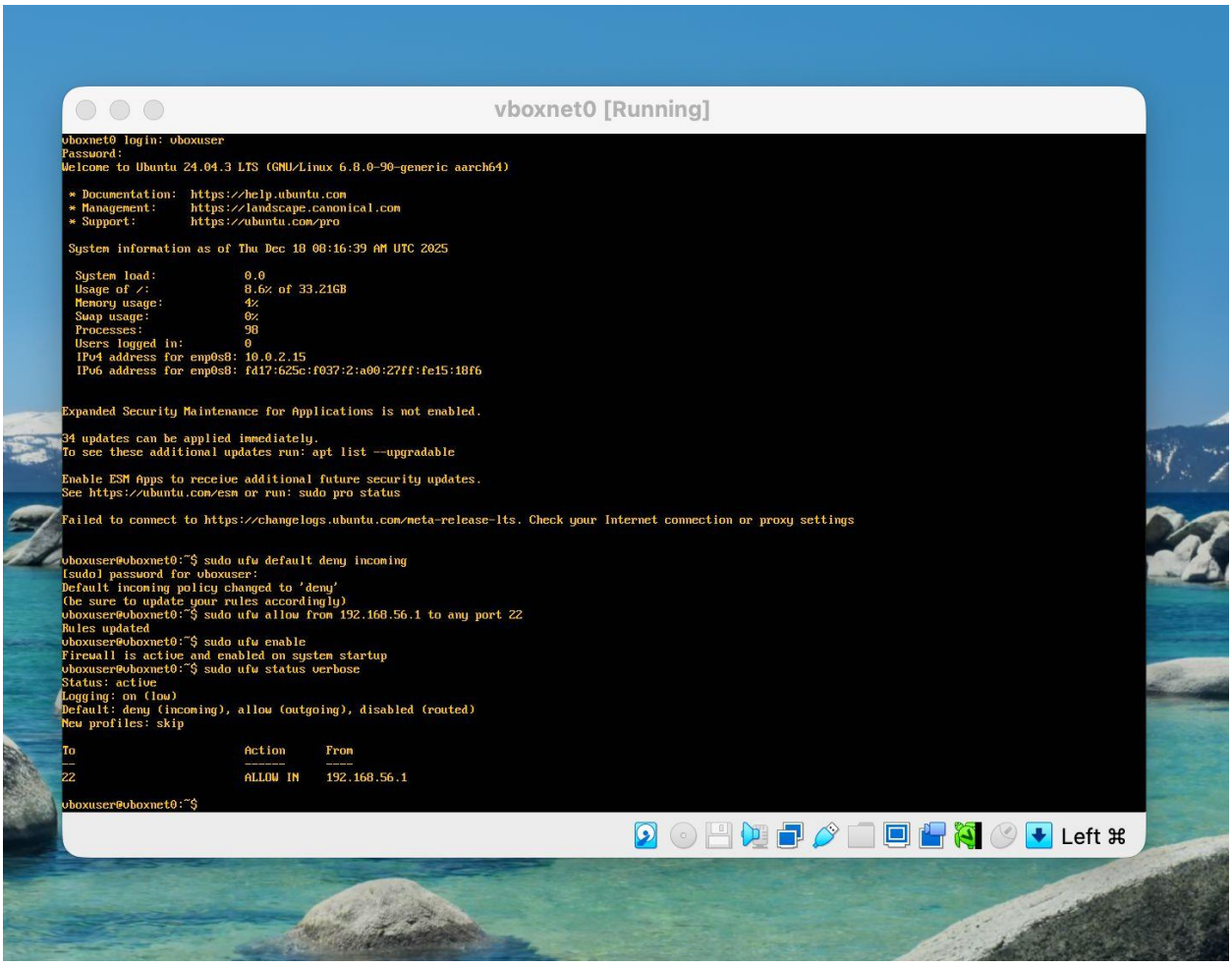

Figure W4-4: UFW firewall rules showing restricted SSH access.

---

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
```

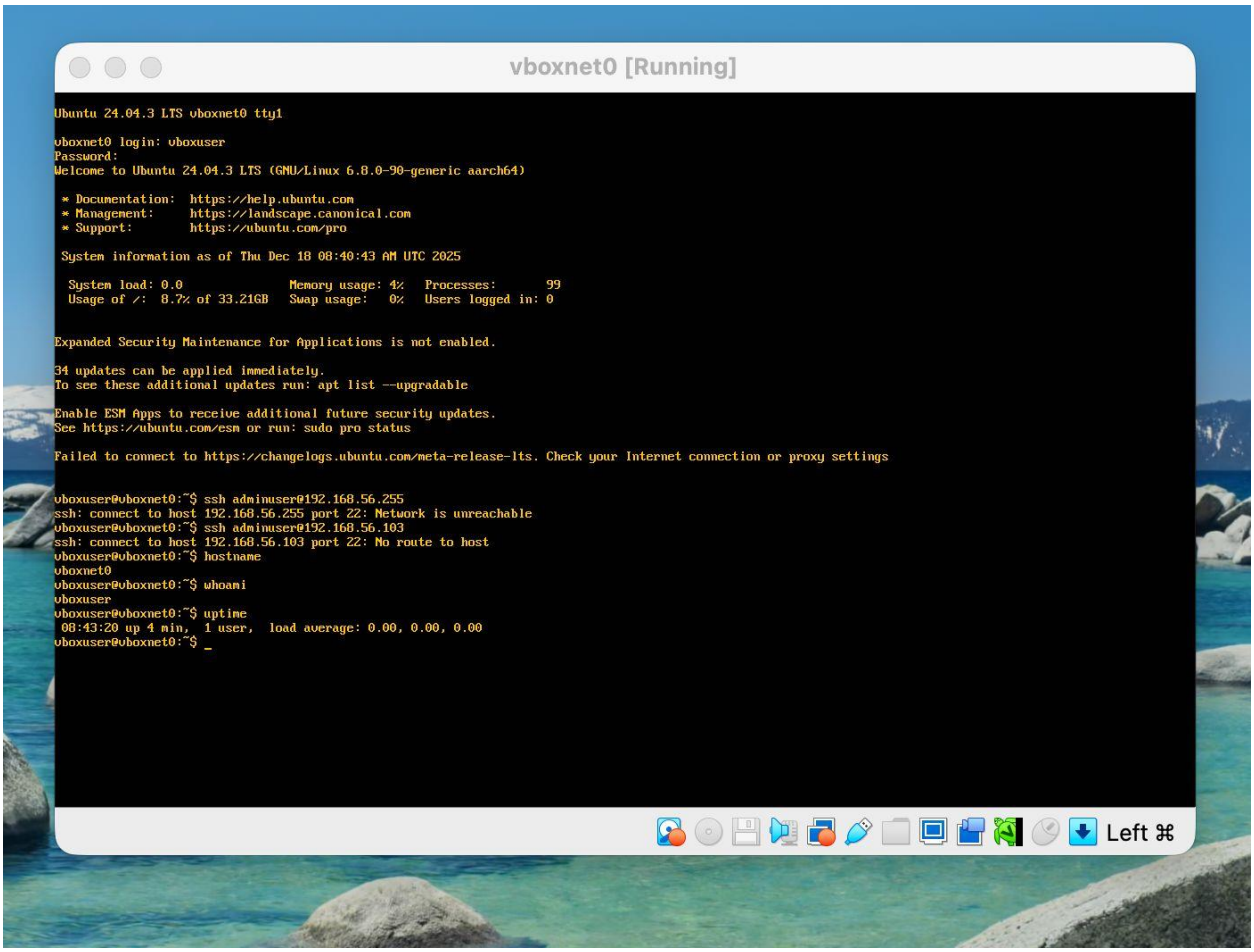

Figure W4-5: Evidence of remote administration via SSH.

---

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)