🔐Project 3: Secure Linux Server Setup & Hardening

🔗WEEK 1 — Initial Server Deployment & Basic Hardening

🗖 *Timeline: Aug 6 – Aug 11*

🕰️Step 1: Set up the Linux Server

Option 1: Local (VirtualBox)

- Download **Ubuntu Server 22.04 LTS ISO**
- Install in VirtualBox or VMware

Option 2: Cloud (AWS or DigitalOcean)

- Sign up at DigitalOcean or AWS
- Create Ubuntu 22.04 LTS Droplet or EC2 instance
- Assign static IP

🕰️Step 2: Secure SSH

```
ssh root@your_server_ip
adduser secureadmin
usermod -aG sudo secureadmin
```

Enable key-based login:

```
ssh-keygen -t rsa
ssh-copy-id secureadmin@your_server_ip
```

Edit SSH configuration:

```
sudo nano /etc/ssh/sshd_config
# Changes:
PermitRootLogin no
PasswordAuthentication no
```

Restart SSH service:

```
sudo systemctl restart ssh
```

🕰️Step 3: Set Up UFW Firewall

```
sudo apt install ufw
sudo ufw allow OpenSSH
sudo ufw allow 80
sudo ufw allow 443
sudo ufw enable
sudo ufw status
```

Files to Save:

- `ssh_config.md`
- `ufw_setup.md`
- `setup_log.txt`

🔗WEEK 2 — Intrusion Protection & System Auditing

🗖 *Timeline: Aug 12 – Aug 18*

🕰️Step 4: Install & Configure `fail2ban`

```
sudo apt install fail2ban
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
sudo nano /etc/fail2ban/jail.local
# In [sshd] section:
enabled = true
maxretry = 5
bantime = 3600
sudo systemctl restart fail2ban
```

🕰️Step 5: Install & Configure `auditd`

```
sudo apt install auditd
sudo systemctl start auditd
sudo systemctl enable auditd
sudo ausearch -x sshd
```

🕰️Step 6: Run CIS Benchmark with Lynis

```
sudo apt install lynis
sudo lynis audit system
```

Files to Save:

- `fail2ban_config.md`
- `auditd_log.md`
- `lynis_report.txt`
- `mid_project_review.md`

🔗WEEK 3 — Vulnerability Scanning & Fixing Issues

🗖 *Timeline: Aug 19 – Aug 25*

🕰️Step 7: Run Vulnerability Scans

```
sudo lynis audit system
```

Optional (GUI Tools):

- Install Nessus Essentials
- Run scans via https://localhost:8834/

🕰️Step 8: Fix Issues Found

```
sudo apt update && sudo apt upgrade -y
# Stop unused services
sudo systemctl stop apache2
sudo systemctl disable apache2
```

Files to Save:

- `vuln_scan_report.md`
- `issues_fixed.md`

🔗WEEK 4 — Final Documentation & Submission

🗖 *Timeline: Aug 26 – Aug 31*

🕰️Step 9: Write Final Report

Create `Linux_Server_Hardening_Guide.md` with:

- Overview & Objectives
- Deployment steps
- SSH & user hardening
- Firewall rules
- IDS configuration

- Auditing setup
- Vulnerability analysis
- Fixes applied

🕰️Step 10: Create Security Checklist

```
- [x] Disable root login
- [x] Use key-based SSH authentication
- [x] Setup UFW firewall
- [x] Install fail2ban
- [x] Configure auditd
- [x] Run vulnerability scans
- [x] Disable unused services
- [x] Keep system updated
```

Save as: `server_security_checklist.md`

🕰️Step 11: Make Presentation

Suggested Slides:

1. Project Overview
2. Server Setup & Tools
3. SSH + User Security
4. Firewall Configuration
5. IDS + Audit Logs
6. Vulnerability Scan (Nessus)
7. Fixes Applied
8. Conclusion

📆Final Deliverables Due (by Aug 8/9)

- answer in chat instead but with small definitions or theory like research paper