Auditing Ubuntu with Lynis - What is Server Hardening?

When a server is first installed, it often comes with default settings and unnecessary services that make it vulnerable to attack. Do the following after setting up your VM. You may work alongside a partner or group, but all work should be done on your own VM.

Server hardening is the process of:

- Reducing the attack surface (turning off what you don't need).
- Securing critical services with stronger settings.
- Applying updates to fix known vulnerabilities.
- Setting up monitoring to catch suspicious activity.

One tool that helps with this is **Lynis**, a widely used security auditing tool for Linux and Unix systems. This week, you'll run Lynis to identify weaknesses and review its findings on your VM. In future weeks, you'll apply fixes.

Part 1 – Install Lynis

1. Update your package lists:

```
sudo apt update
```

2. Install Lynis:

```
sudo apt install lynis -y
```

2. Verify installation:

```
lynis show version
```

Part 2 – Run a Security Audit

1. Run a full system audit:

```
sudo lynis audit system
```

2. Let the scan complete.
3. At the end, note down:

- **Hardening index score** (out of 100+).
- **Warnings** (serious issues).
- **Suggestions** (recommended best practices).

Reports are saved here. Check them out:

- `/var/log/lynis.log`
- `/var/log/lynis-report.dat`

Part 3 – Analyze the Results

Answer these questions in your submission:

1. What was your **hardening index score**?
2. List at least **2 warnings** Lynis flagged.
3. List at least **2 suggestions** for improving security.
4. In your own words: *Why is auditing important before putting a server into production?*

Submission

Turn in a short write-up (about a paragraph not including screenshot) that includes:

- Your hardening index.
- Two warnings and two suggestions.
- Your reflection on why auditing matters.
- Screenshot of your output. Be sure that your username is your last name and first initial.