Task 14: Linux Server Hardening & Secure Configuration

Tools:
- Primary: Ubuntu / Kali Linux
- Alternatives: Lynis, CIS Benchmarks

Hints / Mini Guide:

1. Review default Linux system settings to understand users, services, and open ports.
2. Remove unused user accounts and restrict sudo access based on least privilege.
3. Disable root login and configure SSH using key-based authentication.
4. Update system packages and enable automatic security updates.
5. Configure a firewall to allow only required network traffic.
6. Stop and disable unnecessary services running on the server.
7. Secure file permissions for sensitive system and configuration files.
8. Review system logs to monitor authentication and system activity.

Deliverables:

- Linux Hardening Checklist
- Security configuration summary

Final Outcome:
- Ability to secure Linux systems against common attacks

Interview Questions Related To Above Task:

- What is server hardening?
- Why disable root login?
- What is least privilege?
- Purpose of firewall?
- Risks of unused services?

📌 **Task Submission Guidelines**

- ⏰ **Time Window:**

Youcan complete the task anytime between 10:00 AM to 10:00 PM on the given day. Submission link closes at 10:00 PM

- 🔍 **Self-Research Allowed:**

Youare free to explore, Google, or refer to tutorials to understand concepts and complete the task effectively.

- 🛠️ **Debug Yourself:**

Tryto resolve all errors by yourself. This helps you learn problem-solving and ensures you don't face the same issues in future tasks.

- 💸 **No Paid Tools:**

Ifthe task involves any paid software/tools, do not purchase anything. Just learn the process or find free alternatives.

- 📁 **GitHub Submission:**

Create a new GitHub repository for each task.
Add everything you used for the task — code, datasets, screenshots (if any), and a short README.md explaining what you did.

📤 **Submit Here:**

After completing the task, paste your GitHub repo link and submit it using the link below:

- 👉 [Submission Link]