Task 12: Log Monitoring & Analysis

Tools:
- Linux logs, Windows Event Viewer
- Alternatives: Splunk Free

Hints / Mini Guide:

1. Understand log types.
2. Analyze authentication logs.
3. Identify failed logins.
4. Detect anomalies.
5. Correlate events.
6. Learn SIEM basics.
7. Write alerts.
8. Document findings.

Deliverables:

- Log analysis report

Final Outcome:
- Incident detection skills

Interview Questions Related To Above Task:

- What is log?
- What is SIEM?
- Why logs are important?
- What is anomaly detection?
- Examples of security logs?

📌 **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]