Task 4 :Linux Server Hardening

Objective: **Capture and analyze live network traffic to identify credentials or suspicious activity.**
Tools : **Ubuntu, UFW, fail2ban, SSH**

Deliverables: **Before/after state summary, applied commands list, screenshots**

Hints/Mini Guide:

Disable root login via SSH, enforce key-based login, block unused ports.

Outcome:Gain practical knowledge on securing Linux systems.

Interview Questions:

1.What is server hardening?
2.What is UFW and how does it work?
3.Why disable root login in SSH?
4.What is fail2ban used for?
5.How do you check for open ports on Linux?
6.What is key-based authentication?
7.What are system services and how to manage them?
8.How do you secure SSH?
9.Why is patch management important?
10.How can you audit server security?

Key Concepts: **System Hardening, Firewall Configuration, SSH Security, Access Control**

🌟 Task Submission Guidelines

🕙 Time Window:

You've got a 12-hour window—from 10:00 AM to 10:00 PM—to give your best. It's your time to shine. But remember, once the clock hits 10:00 PM, submissions close.

🔍 Self-Research Allowed:

You're not alone—but we believe in your ability to explore and grow. Feel free to use Google, YouTube, or any learning resource. Learning how to learn is your biggest strength.

🛠️ Debug Yourself:

Mistakes? Perfect. That's how real learning happens. Try solving issues on your own—it'll build your confidence and sharpen your problem-solving skills for the future.

💸 No Paid Tools:

We value learning over luxury. If any task points to a paid tool, skip it. Don't spend a single rupee. Just search for free, open-source options—we promise, it's part of the real-world hustle.

📁 GitHub Submission:

For each task, start fresh. Create a new GitHub repo.

Upload everything you used—your code, dataset, screenshots (if any), and a short README.md. That README is your story—tell us what you built, why, and how.

📩 Submission:

When you're done and proud of what you've built, drop your GitHub repo link through the submission form. Let your work speak for you.