Task 3 :Network Packet Sniffing and Analysis

Objective: Capture and analyze live network traffic to identify credentials or suspicious activity.
Tools : Wireshark, TCPDump
Deliverables:PCAP files, analysis report with identified security issues

Hints/Mini Guide:

Apply filters like http.request or ip.addr ==<target>. Look for credentials in POST data.

Outcome:Understand network-level risks and how sniffing tools are used.

Interview Questions:

1. What is packet sniffing?
2. How does Wireshark capture network traffic?
3. What is the difference between TCP and UDP?
4. What kind of information can be seen in HTTP packets?
5. How can passwords be exposed in plaintext over a network?
6. What are some signs of suspicious network activity?
7. What is ARP poisoning?
8. What is a man-in-the-middle attack?
9. How can HTTPS help prevent packet sniffing?
10. What are PCAP files used for?

Key Concepts: **Network Protocols, Packet Analysis, HTTP, TCP/IP, Data Interception**

🌟 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.