Task 3: Networking Basics for Cyber Security

Tools:

- Primary: Wireshark
- Alternatives: tcpdump, Microsoft Network Monitor

Hints / Mini Guide:

1. Learn basic networking concepts (IP, MAC, DNS, TCP/UDP).
2. Install Wireshark and capture live network traffic.
3. Filter packets by protocol (HTTP, DNS, TCP).
4. Observe three-way TCP handshake.
5. Identify plain-text traffic vs encrypted traffic.
6. Capture DNS queries and analyze them.
7. Save packet captures for analysis.
8. Write observations in simple language.

Deliverables:

- Packet capture file + analysis report

Final Outcome:

- Ability to analyze network traffic

Interview Questions Related To Above Task:

- What is TCP handshake?
- Difference between TCP and UDP?
- What is DNS?
- What is packet sniffing?
- Why is HTTPS more secure than HTTP?

📌 **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]