🔐 Cybersecurity Internship – Phase 1 (Hands-on Task 2)

✅ TASK 2: Perform a Basic Network Scan Using Nmap

🎯 Task Objective

Get hands-on with **network scanning** to identify open ports and services using nmap. This task builds your foundational skills in ethical hacking and reconnaissance.

🛠️ Tools Used

- **Nmap** (Install from https://nmap.org/download.html)
- **Kali Linux or any Linux OS** (optional)
- **Command line / Terminal**
- A **target IP** like scanme.nmap.org (safe public test server)

📘 Mini Guide: How to Do This Task

1. Install nmap on your system (use terminal or download for Windows).
2. Scan a public server using:
   bash
   nmap scanme.nmap.org
3. Try more flags like:
   - nmap -sV scanme.nmap.org (service detection)
   - nmap -O scanme.nmap.org (OS detection)
   - nmap -p- scanme.nmap.org (all ports)
4. Document each command you run and interpret the results.
5. Save the output as screenshots or copy into a .txt file.
6. Summarize what you found in a short report.

📤 Expected Output / Learning Outcome

- You'll understand what a **port scan** looks like
- You'll learn how attackers gather information (legally, here)
- You'll become familiar with nmap commands and results

💡 Key Concepts to Observe

- Open vs Closed vs Filtered ports
- Service detection
- Common ports and protocols
- Ethical use of scanning tools

❓ 10 Interview Questions (Based on This Task)

1. What is the purpose of `nmap` in cybersecurity?
2. What's the difference between TCP and UDP scanning?
3. Explain what the `-sV` and `-O` flags do.
4. Why should you never run `nmap` scans without permission?
5. What are filtered ports?
6. How does OS fingerprinting work in `nmap`?
7. What is banner grabbing?
8. Why is port scanning important in penetration testing?
9. List 3 common ports and their services.
10. What does a "closed" port indicate?

📁 GitHub Submission Instructions

1. In the same repo Cybersecurity-Internship-UJAR, create a folder Task-02-Nmap-Scan
2. Upload:
    - Report as Nmap_Scan_Report.pdf
    - All command outputs/screenshots in a folder
    - README.md with basic scan summary and key findings
3. Push the updates to GitHub

⏳ Deadline & Submission Guide

- **Deadline**: Complete within 2 days from Task 1
- Use only **legal, publicly allowed targets** like scanme.nmap.org
- Avoid any real IP unless you have permission
- No paid tools — use CLI and basic research
- Document errors and fixes — learning from troubleshooting is critical
- Submit GitHub link on your dashboard or form