CYBERSECURITY DAILY DAIRY

Day 1: Introduction to Cybersecurity & Ethical Hacking (June 18, 2025)

Topics Covered:

- Ethical Hacking: Intro, importance, difference from malicious hacking, legal/ethical aspects.
- Hacking Methodologies: Reconnaissance, Scanning, Exploitation, Post-Exploitation.
- CIA Triad: Confidentiality, Integrity, Availability.
- Cybersecurity Career Options.
- Cyber Threats and Vulnerabilities.

What I Learned:

I learned the basics of cybersecurity and how ethical hacking helps find vulnerabilities. Ethical hackers follow a method: gathering info (Reconnaissance), finding weaknesses (Scanning), gaining access (Exploitation), and keeping access or getting data (Post-Exploitation). The CIA Triad (Confidentiality, Integrity, Availability) is key to cybersecurity.

Job Preferences in Cybersecurity:

- Penetration Tester (Ethical Hacker)
- SOC Analyst
- Cybersecurity Analyst
- Network Security Engineer
- Security Researcher
  These roles need skills in networking, Linux, scripting, and security tools.

Legal & Ethical Guidelines:

Always get written permission, follow cyber laws (like India's IT Act 2000), and report vulnerabilities responsibly.

Cyber Threats and Vulnerabilities:

Types of Threats:

1. **Malware:** Harmful software.
   - **Viruses:** Infect files and spread (e.g., ILOVEYOU).
   - **Worms:** Self-replicating, spread across networks (e.g., WannaCry).
   - **Ransomware:** Encrypts files, demands payment (e.g., Cryptolocker).
2. **Phishing:** Tricking people for sensitive info.
   - **Email Phishing:** Fake emails for personal data (e.g., fake bank emails).
   - **Spear Phishing:** Targeted attacks (e.g., fake CFO email for wire transfer).
3. **Social Engineering:** Manipulating people.