CYBERSECURITY DAILY DAIRY

Day 1: Introduction to Cybersecurity & Ethical Hacking.

Date: June 18, 2025

Topics Covered:

- Introduction to Ethical Hacking
- Importance of Ethical Hacking in Cybersecurity
- Difference between Ethical and Malicious Hacking
- Legal and Ethical Aspects of Hacking
- Hacking Methodologies:
    - Reconnaissance
    - Scanning
    - Exploitation
    - Post-Exploitation
- CIA Triad in Cybersecurity
- Career Options in Cybersecurity
- Cyber Threats and Vulnerabilities

What I Learned:

Today I learned the foundation of cybersecurity and its growing importance in protecting digital infrastructure. Ethical hacking plays a crucial role in detecting vulnerabilities before malicious hackers exploit them.

I understood that ethical hackers follow a structured approach, known as the Hacking Methodology, which includes:

- **Reconnaissance** – Information gathering
- **Scanning** – Target detection and vulnerability identification
- **Exploitation** – Gaining unauthorized access
- **Post-Exploitation** – Maintaining access, covering tracks, or extracting data

CIA Triad: Core Pillars of Cybersecurity

- **Confidentiality** – Ensuring that sensitive data is accessed only by authorized people
- **Integrity** – Making sure the data is accurate and not altered without permission
- **Availability** – Ensuring that systems and data are accessible when needed

The CIA Triad is the foundation of cybersecurity – all strategies and defenses revolve around maintaining these three principles.

Job Preferences in Cybersecurity:

Based on my interest in problem-solving, practical tasks, and protecting digital environments, here are some roles that appeal to me:

- **Penetration Tester (Ethical Hacker)** – Simulate attacks to find vulnerabilities
- **SOC Analyst (Security Operations Center)** – Monitor and respond to threats in real time
- **Cybersecurity Analyst** – Analyze and strengthen security measures
- **Network Security Engineer** – Secure network infrastructure
- **Security Researcher** – Study new attack trends and develop countermeasures

These roles require skills in networking, Linux, scripting, and the use of various security tools — all of which I will be learning in the coming weeks.

Legal & Ethical Guidelines:

- Always work with written permission
- Follow applicable cyber laws (e.g., IT Act 2000 in India)
- Report vulnerabilities responsibly and ethically

Cyber Threats and Vulnerabilities:

Types of Threats:

1. Malware
Malicious software designed to harm or exploit systems.

- **Viruses**
  - Infect other files or systems and spread as they replicate.
  - ***Example:*** The ILOVEYOU virus spread via email attachments and caused widespread damage.
- **Worms**
  - Self-replicating malware that spreads across networks without needing a host file.
  - ***Example:*** The WannaCry ransomware worm exploited a vulnerability to encrypt data and demand ransom.
- **Ransomware**
  - Encrypts files and demands payment for decryption.
  - ***Example:*** Cryptolocker ransomware encrypted files and demanded payment in cryptocurrency.

2. Phishing
Fraudulent attempts to obtain sensitive information by impersonating a trustworthy entity.

- **Email Phishing**
    - Sending fake emails to trick users into providing personal information.
    - ***Example:*** An email posing as a bank, asking users to click a link and enter account details.
- **Spear Phishing**
    - Targeted attacks on specific individuals or organizations.
    - ***Example:*** A fake email sent to a company CFO requesting a fake wire transfer.

3. Social Engineering
Manipulating individuals into revealing confidential information or taking harmful actions.

- **Pretexting**
    - Creating a fake scenario to gain access or information.
    - *Example:* Pretending to be IT support to obtain login credentials.
- **Baiting**
    - Offering something desirable to lure victims into installing malware or revealing information.
    - *Example:* Leaving a USB drive labeled “Employee Salaries” in a public place to entice someone to use it.

Examples of Social Engineering Techniques:

- **Pretexting:** A fake phone call from "IT support" asking for usernames and passwords.
- **Baiting:** A USB labeled “Confidential Data” left in a cafeteria to trick someone into plugging it in.