Week 4: Capture The Flag (CTFs)

🔹 **What is CTF?**

- **Capture The Flag (CTF)** is a type of cybersecurity competition where participants solve security-related challenges to earn points and "capture flags."
- Challenges can range from web vulnerabilities, cryptography, reverse engineering, and forensics to binary exploitation.

Types of CTF Challenges:

1. **Jeopardy-style**: Solve different security problems to earn points, with varying difficulty levels.
2. **Attack-Defense**: Teams attack each other's systems while defending their own.

🔹 **How to Solve CTF Challenges?**

- **Reconnaissance:** Gather as much information as possible about the challenge (source code, network traffic, etc.).
- **Exploitation:** Use common attacks like SQL injection, XSS, buffer overflow, or reverse engineering to solve the challenge.
- **Flag Identification:** The "flag" is often a string of text like FLAG{<some_text>} that you find by exploiting the vulnerability.

Common CTF Techniques:

1. **Web Exploitation:**
    - Look for input validation issues (e.g., SQLi, XSS).
    - Check HTTP headers, cookies, and hidden fields for sensitive information.
2. **Reverse Engineering:**
    - Analyze binary files or applications to understand the underlying code.
    - Tools like **Ghidra** or **IDA Pro** can help.
3. **Cryptography:**
    - Work on puzzles involving encryption and decryption.

- Learn to use tools like **CyberChef** to decode and solve challenges.

4. **Forensics:**
    - Extract hidden data from files, network traffic, or logs.
    - Look for **steganography** or hidden messages.

- **How to Approach CTFs?**

1. **Start with Easy Challenges:** Begin with easier challenges to understand the environment and tools used.
2. **Collaborate with Others:** Work with team members or online communities for faster problem-solving.
3. **Use Resources:** Leverage tools, write-ups, and forums when stuck.
4. **Practice Regularly:** Participate in as many CTFs as you can to improve problem-solving skills.