CRAC SESSION -2

Objectives: The primary objective of the session was to provide students with practical exposure and foundational knowledge in the domain of cybersecurity through an industry-oriented learning approach. Organized in collaboration with CRAC Learning Foundation, the session aimed to introduce students to real-world cybersecurity concepts such as web security, OSINT (Open-Source Intelligence), and system vulnerabilities. The session was conducted on 10th April 2026, starting from 11:00 AM onwards at Lab 108, Excellence Center, Block A, DPGITM, Gurugram. The session was attended by 28 students from the BCA and Computer Science and Engineering departments having keen interest in cyber security.

Key contents covered in the session were:

a) **Introduction to Cybersecurity Concepts**
   - The session began with an overview of cybersecurity and its significance in today's digital world.
   - Students were introduced to fundamental concepts including web security and OSINT.
   - The importance of identifying vulnerabilities and securing systems was emphasized.

b) **Web Security and Protocol Understanding**
   - Detailed explanation of HTTP and HTTPS protocols and their role in secure communication.
   - Discussion on common vulnerabilities such as broken access control and how attackers exploit such weaknesses.
   - Real-world examples were used to enhance conceptual understanding.

c) **Hands-on Learning using Wireshark**
   - Live demonstration of capturing network packets using Wireshark.
   - Practical exposure helped students connect theoretical knowledge with real-world application.

d) **Capture The Flag (CTF) Competition**
   - A competitive CTF challenge was conducted on the Defhawk platform.
   - Students applied their knowledge to solve cybersecurity problems and challenges.
   - The activity encouraged teamwork, critical thinking, and problem-solving skills in a real-time environment.

Resource Persons:

Mr. Krishna : Currently working as a Security Researcher at Defhawk. Experience in web and API security testing. Disclosed multiple security vulnerabilities including CVE-2025-1473,CVE-2025-1474 .

Some of the glimpses of the event are attached.