Week 1: Foundations of Cybersecurity & Forensics

Cybersecurity fundamentals includes CIA triad :-

Confidentiality:-

- Ensures that sensitive information is only accessible to authorized people.
- Prevents disclosure and theft of data
- Implement through encryption , access control and authentication mechanism.

Integrity:-

- Maintains the accuracy and trustworthiness by preventing data modification , deletion and access control.
- Implemented using cryptographic has function.

Availability:-

- Keeping systems and data accessible to user whenever needed
- Protect the data from downtime caused by cyberattack

Cybersecurity threats

1. **Hacking:-** Unauthorized access to or control over computer or network.

2. **Phishing:-** Fraudulent attempts to obtain sensitive information by pretending to be a trustworthy entity.

3. **Identity Theft:-** Stealing someone's personal information to commit fraud or gain unauthorized access

4. **Cyberstalking:-** Using the internet to harass, threaten, or intimidate someone

5. **Online Fraud & Scams:-** Deceptive activities conducted over the internet to defraud individuals or businesses.

6. **Ransomware Attacks:-** Malicious software that locks users out of their systems until a ransom is paid.

7. **Cyberterrorism:-** Using digital means to disrupt or damage government systems, causing fear or harm. ○ Example: Hackers attack a country's power grid, leading to widespread blackouts.

8. **Child Exploitation & Cyberbullying:-** Abusing, harassing, or exploiting children online.

9. **Denial of Service (DoS) & Distributed Denial of Service (DDoS) Attacks**:- Overloading a network or website with traffic to make it unavailable.

Types of Cyber Attacks:

- **Man-in-the-Middle (MITM) Attack** – Intercepting communication between two parties to steal or manipulate data.
- **SQL Injection** – Exploiting vulnerabilities in databases to gain unauthorized access.
- **Brute Force Attack** – Attempting to crack passwords by systematically trying different combinations.
- **Social Engineering** – Manipulating individuals into revealing confidential information.

CyberForensic:-

A forensic investigation follows a structured process to ensure the integrity and accuracy of digital evidence. This is overview of the key phases:

1. Identification

- Recognizing potential sources of digital evidence (computers, mobile devices, cloud storage).
- Securing and isolating affected systems to prevent tampering.

2. Collection & Preservation

- Acquiring data using forensic tools while maintaining its integrity.
- Creating forensic images (bit-by-bit copies) to analyze without altering original data.
- Documenting chain of custody to ensure evidence is admissible in court.

3. Analysis

- Examining collected data for signs of unauthorized access, malware, or suspicious activity.
- Using forensic software to recover deleted files, analyze logs, and detect anomalies.
- Correlating findings with known attack patterns.

4. Documentation & Reporting

- Recording findings in a structured report, including timelines, evidence details, and conclusions.
- Presenting results in a clear and legally defensible manner.

5. Presentation & Legal Proceedings

- Providing expert testimony if required.

- Ensuring evidence meets legal standards for admissibility in court.

Lab setup :-