CYBERSECURITY TRAINING

(WEEK 1-Day1)

1.Introduction to Ethical Hacking

1.1. Overview to Cybersecurity

Definition: Cybersecurity is the practice of protecting systems, networks, and data from digital attacks, damage, or unauthorized access.

Importance: It safeguards personal information, critical infrastructure, business assets, and national security from evolving cyber threats.

1.2. Key Concepts of Cybersecurity

Confidentiality

- Ensures that data is only accessible to authorized users.

- Example: Encryption protects confidential data during transmission.

Integrity

- Ensures that data remains accurate, consistent, and unaltered.
- Example: Checksums and digital signatures verify data integrity.

Availability

- Ensures that information and resources are accessible when needed.
- Example: Redundant systems and backups improve availability.

2.Cyber Threats and Vulnerabilities

2.1. Types of Threats

Malware

- Malicious software (e.g., viruses, worms, ransomware) designed to harm or exploit systems.

Phishing

- Fraudulent attempts (often via email or messages) to trick users into revealing sensitive information.

Social Engineering

- Manipulating people to break security procedures (e.g., impersonation or psychological tricks).

2.2. Common Vulnerabilities

CVEs (Common Vulnerabilities and Exposures)

- A publicly disclosed list of known security flaws in software or systems, each with a unique identifier.

Zero-Day Exploits

- Vulnerabilities unknown to the software vendor, exploited before a fix is available—highly dangerous due to lack of defense.