**CEH ASSIGNMENT**

Module 1 CS- Introduction

1. Cyber seurity refers to the practice of protecting systems, networks, and data from digital attacks, theft, and damage. It encompasses a range of technologies, processes, and practices designed to safeguard devices, data, and infrastructure from cyber threats.

2. The main objectives of cybersecurity can be summarized by the **CIA Triad**, which stands for:

**Confidentiality**: Ensuring that sensitive information is accessible only to those authorized to access it. This involves protecting data from unauthorized access and breaches.

**Integrity**: Maintaining the accuracy and reliability of data. This means ensuring that information is not altered or destroyed by unauthorized individuals and that any changes are made by authorized users.

**Availability**: Ensuring that information and systems are accessible to authorized users when needed. This involves protecting against disruptions, such as denial-of-service attacks or natural disasters.

3. -Offensive cybersecurity involves proactive measures designed to identify and exploit vulnerabilities in systems and networks.

-Defensive cybersecurity focuses on protecting systems, networks, and data from cyber threats.

4. Cyberspace refers to the virtual environment created by interconnected computer networks and systems. It encompasses the internet and all digital communications, including websites, social media, emails, and online services.

**Cyber law** (or internet law) refers to the legal frameworks and regulations governing activities in cyberspace.

5. Cyber welfare refers to the initiatives and practices aimed at promoting well-being and safety in the digital environment.

6.White Hat Hackers

Intent: Ethical hacking for security purposes

Black Hat Hackers

Intent: Malicious activities for personal gain.

Gray Hat Hackers

Intent: A mix of ethical and unethical behavior.

7. **Security Operations Center**

**8.** **Evolving Threat Landscape**

**Insider Threats**

**Data Privacy Regulations**

**Inadequate Security Policies**

**Incident Response Challenges**

**Public Awareness and Perception**