**Module 1 CS- Introduction**

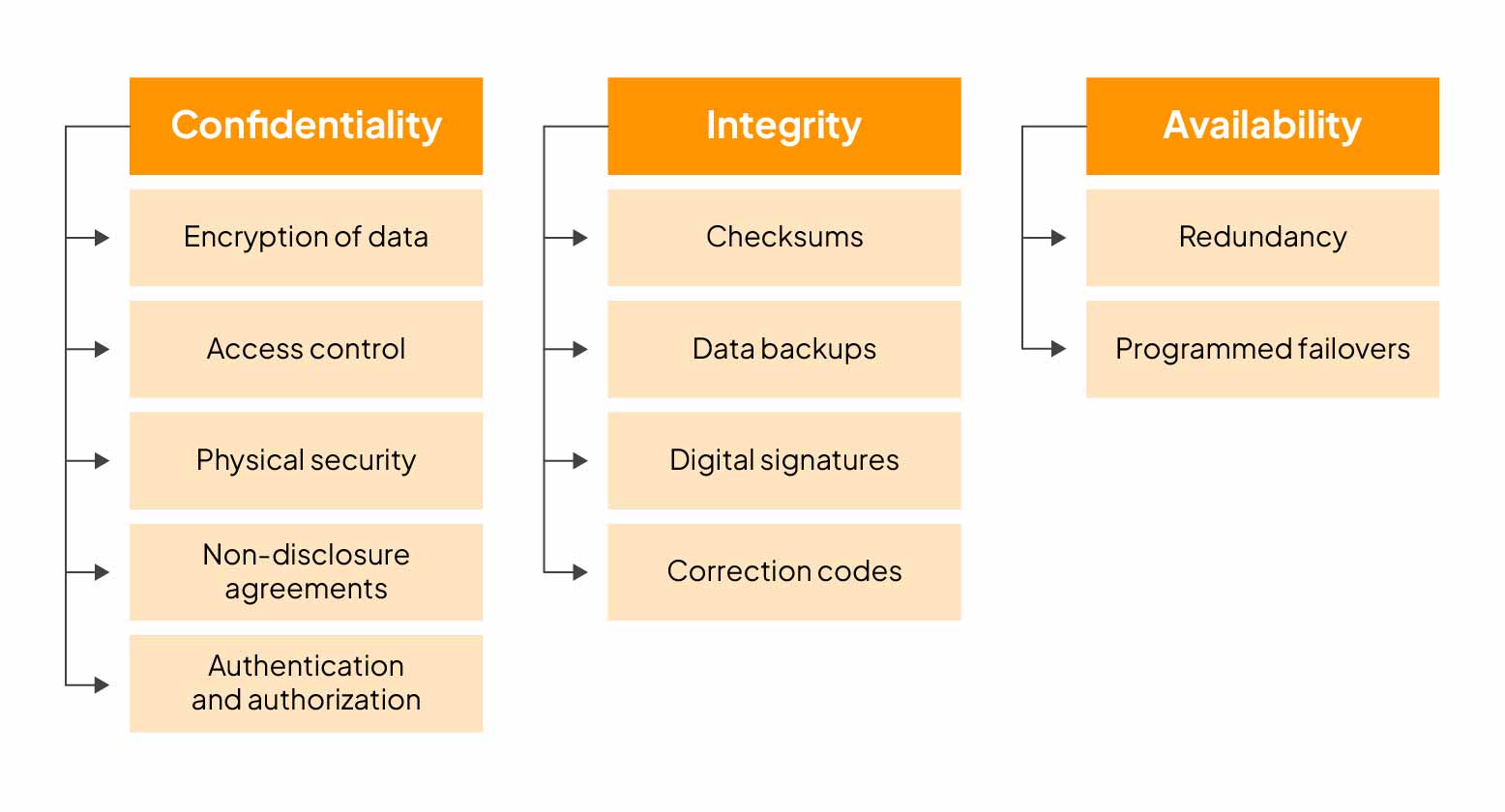
**1. What is the meaning of Cybersecurity?**

Cybersecurity refers to the practice of protecting computer systems, networks, and data from unauthorized access, attacks, or damage.  
**Example:** Using antivirus software like Norton or McAfee to safeguard your computer against malware.

**2. What are the main objectives of Cybersecurity?**

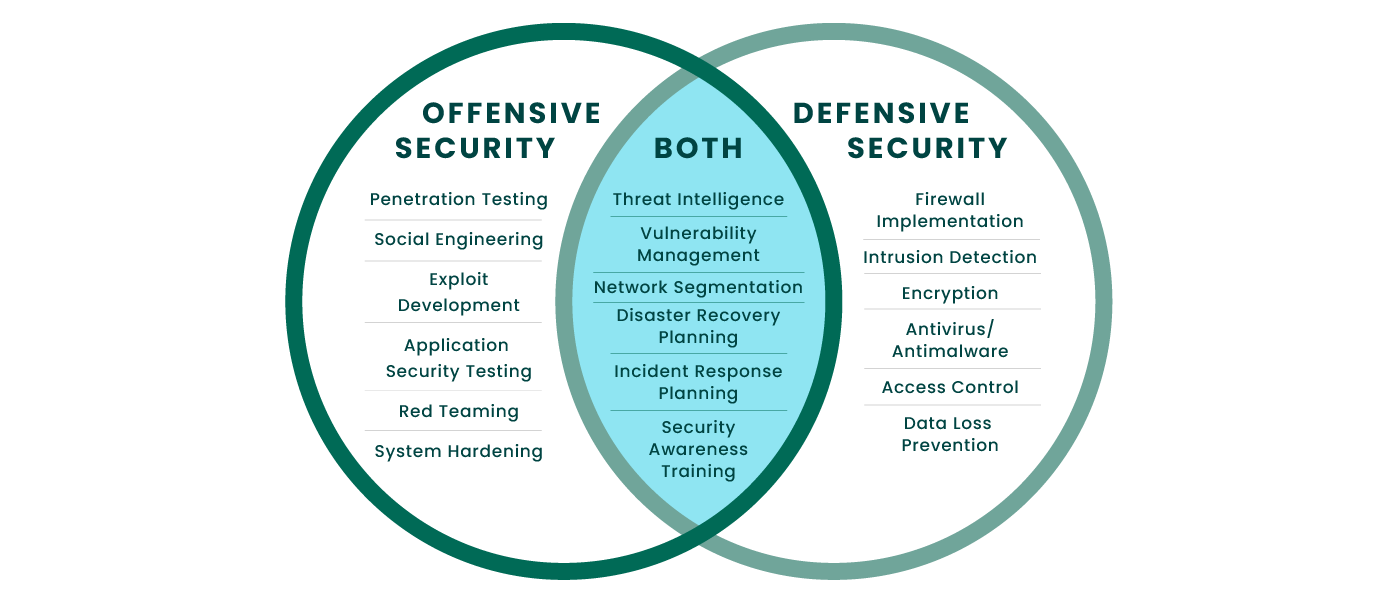
The main objectives are:

1. **Confidentiality:** Ensuring data is accessible only to authorized individuals.  
   *Example:* Encrypting sensitive data during online transactions.
2. **Integrity:** Ensuring data is accurate and not tampered with.  
   *Example:* Using checksums to verify file integrity.
3. **Availability:** Ensuring systems and data are accessible when needed.  
   *Example:* Maintaining server uptime for e-commerce websites like Amazon.



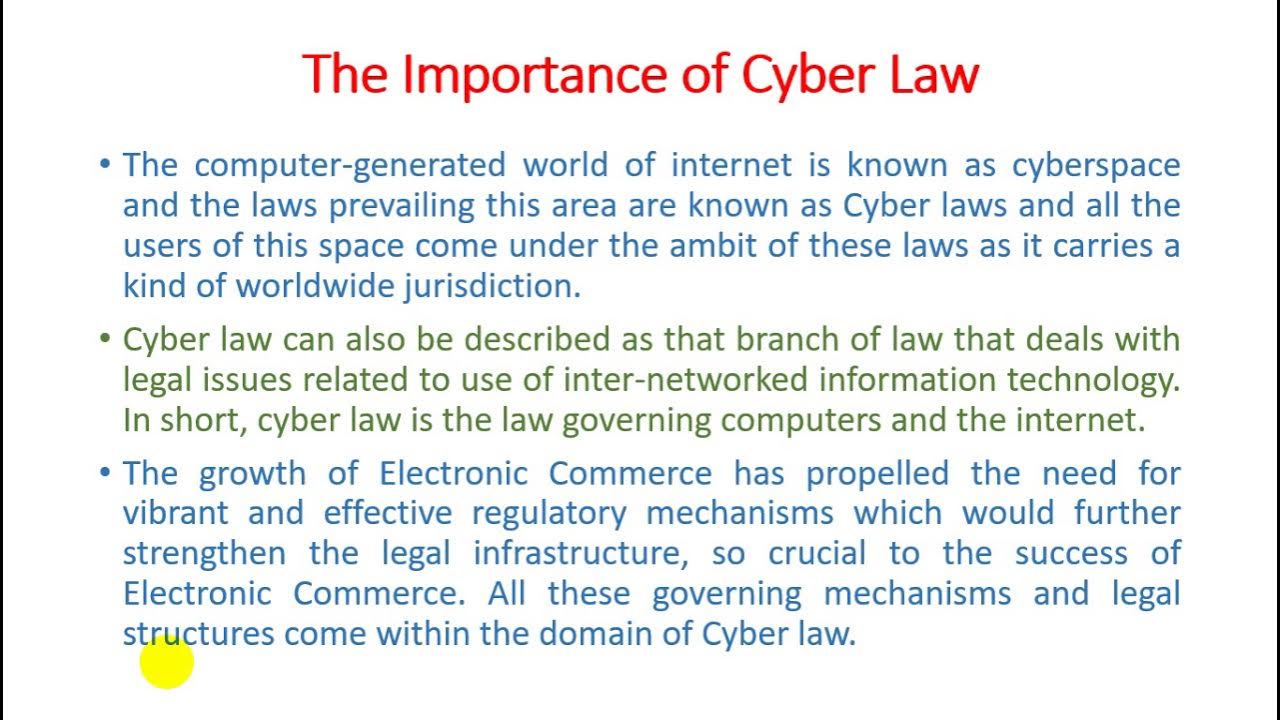
**3. What is offensive and defensive in Cybersecurity?**

* **Offensive Cybersecurity:** Actively identifying and attacking vulnerabilities in systems to strengthen defenses.  
  *Example:* Ethical hacking to test a bank's security system.
* **Defensive Cybersecurity:** Protecting systems from attacks by implementing security measures.  
  *Example:* Using firewalls and intrusion detection systems (IDS).

 **What is offensive and defensive in Cybersecurity?**

**4. What is Cyberspace and Cyber Law?**

* **Cyberspace:** The virtual environment created by interconnected computers, networks, and the internet.  
  *Example:* Social media platforms like Facebook or Twitter are part of cyberspace.
* **Cyber Law:** Legal frameworks governing online activities, protecting against crimes like hacking and identity theft.  
  *Example:* GDPR laws protect users' personal data in the European Union.



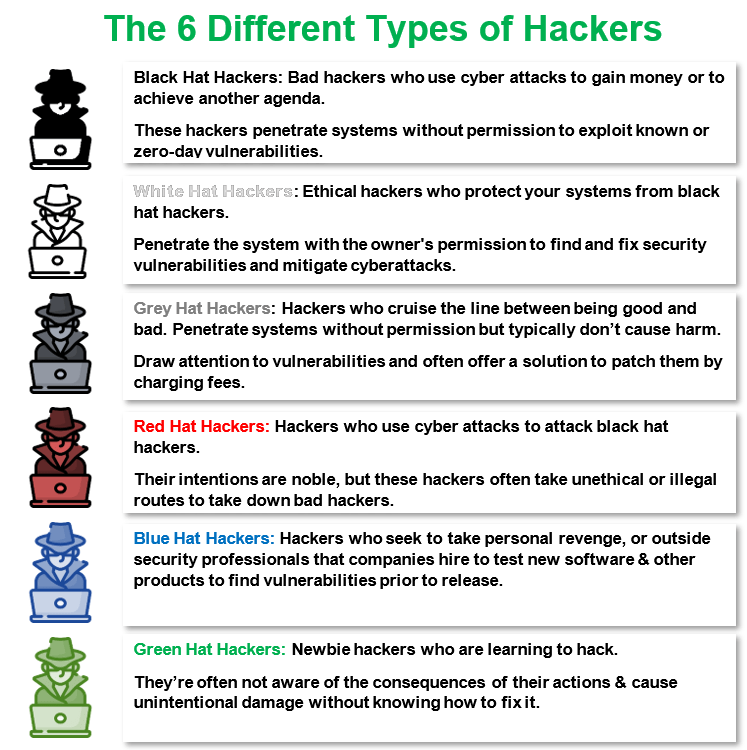
**5. What is Cyber Warfare?**

Cyber warfare involves using cyberattacks by nations or groups to disrupt or damage other nations’ systems or networks.  
**Example:** Stuxnet, a cyberattack on Iran’s nuclear facilities in 2010, caused physical damage to equipment.



**6. Explain the Types of Hackers.**

1. **White Hat Hackers:** Ethical hackers who test security systems legally.  
   *Example:* Security professionals at companies like Google.
2. **Black Hat Hackers:** Malicious hackers who exploit vulnerabilities for illegal purposes.  
   *Example:* Ransomware creators.
3. **Grey Hat Hackers:** Hackers who operate in the gray area, testing systems without permission but not with malicious intent.  
   *Example:* Finding vulnerabilities in a system and notifying the company without exploiting it.



**7. What is the full form of SOC in Cybersecurity?**

SOC stands for **Security Operations Center**.  
It is a centralized unit that monitors, detects, and responds to cybersecurity incidents.  
**Example:** A SOC team analyzes suspicious network traffic to identify potential breaches.

**8. What are the Challenges of Cybersecurity?**

1. **Evolving Threats:** New and sophisticated cyberattacks like ransomware.  
   *Example:* Attackers using AI for phishing scams.
2. **Lack of Awareness:** Employees falling victim to phishing emails.  
   *Example:* A user clicking on a malicious email link causing a data breach.
3. **Shortage of Skilled Professionals:** Insufficient experts in cybersecurity roles.  
   *Example:* Difficulty in hiring ethical hackers or forensic analysts.
4. **Third-Party Risks:** Vulnerabilities in external vendors’ systems.  
   *Example:* The Target data breach was caused by a third-party vendor's compromised credentials.

**Module 2 CS- Fundamental of Operating Systems & Networks**

**1. Difference between Hardware and Software**

**Hardware** refers to the physical components of a computer system (e.g., CPU, RAM, motherboard, etc.). **Software**, on the other hand, refers to the programs and operating systems that run on the hardware (e.g., Windows, Microsoft Office, etc.). You can touch and see hardware, but software is intangible.

**2. Define IP Address Range and Private Address Range**

**IP Address Range**: These are addresses assigned to devices on a network using the Internet Protocol. It consists of a range of addresses available for public or private network assignment.

**Private Address Range**: These are reserved IP addresses within specific ranges for use in private networks. Examples of these ranges include:

* **Class A:** 10.0.0.0 to 10.255.255.255
* **Class B:** 172.16.0.0 to 172.31.255.255
* **Class C:** 192.168.0.0 to 192.168.255.255

**3. Network Protocol and Port Number**

**Network Protocol**: Rules and conventions for communication between network devices. Examples include TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

**Port Number**: A numerical identifier in a device's network stack used to specify a specific process or service. For example, port 80 is used for HTTP traffic, while port 443 is used for HTTPS traffic.

**4. Types of Network Devices**

Examples include:

* **Router**: Forwards data packets between computer networks.
* **Switch**: Connects devices within a network and uses MAC addresses to forward data to the correct device.
* **Hub**: Connects multiple Ethernet devices, making them act as a single network segment.
* **Modem**: Converts data between analog and digital forms.

**5. Tools for Data Backup and Recovery**

Common tools include:

* **Acronis True Image**: Comprehensive backup solution with cloud storage.
* **EaseUS Todo Backup**: Easy-to-use interface for backups and cloning.
* **Carbonite**: Provides automatic cloud backup for all files.

**6. HTTP and HTTPS Protocols**

**HTTP (HyperText Transfer Protocol)**: Foundation of data communication for the World Wide Web, transmitting data in plain text.

**HTTPS (HyperText Transfer Protocol Secure)**: HTTP with encryption, providing secure communication over a computer network by using SSL/TLS protocols.

**7. SSL and TLS Security**

**SSL (Secure Sockets Layer)**: Protocol for encrypting data transmitted over networks. It is the predecessor to TLS.

**TLS (Transport Layer Security)**: Successor to SSL, providing enhanced security and encryption for data transmission over networks.

**8. MAC Address**

**MAC (Media Access Control) Address**: Unique identifier assigned to network interfaces for communication within a network segment. An example would be: 00:14:22:01:23:45.

**Information gathering**

**1. What is information gathering in cybersecurity?**

**Answer:** Information gathering, also known as reconnaissance, is the first step in the cybersecurity process. It involves collecting data about a target to identify potential vulnerabilities and entry points for a cyberattack.

**Example:** An attacker may gather information about a company’s IP address range, employee details, and publicly available information to plan a cyberattack.

**2. What are the different methods of information gathering?**

**Answer:** Methods include passive and active information gathering. Passive methods involve collecting information without direct interaction with the target, while active methods involve direct interaction.

**Example:**

* **Passive:** Searching for a company’s domain registration details (WHOIS lookup).
* **Active:** Conducting a port scan on the company’s network to identify open ports.

**3. What tools are commonly used for information gathering?**

**Answer:** Common tools include Nmap, Wireshark, Maltego, and Shodan.

**Example:** Nmap can be used to scan a network for open ports and services running on those ports, helping identify potential vulnerabilities.

**4. How does social engineering play a role in information gathering?**

**Answer:** Social engineering involves manipulating individuals into divulging confidential information. It is a crucial part of information gathering as it can provide sensitive data that technical methods cannot.

**Example:** An attacker might call an employee pretending to be from the IT department to obtain login credentials.

**5. What are the ethical considerations in information gathering?**

**Answer:** Ethical considerations include obtaining proper authorization before conducting information gathering activities and respecting privacy and legal boundaries.

**Example:** Ethical hackers, also known as white-hat hackers, obtain permission from organizations to conduct penetration testing and information gathering to improve security.

**6. How can organizations protect themselves against malicious information gathering?**

**Answer:** Organizations can implement security measures such as network firewalls, intrusion detection systems, regular security audits, employee training on social engineering, and using VPNs.

**Example:** Regularly updating software and security patches can close vulnerabilities that attackers might exploit during information gathering.