Fundamentals of Information Security

Prepared By : Jayshree Dasa

Unit - 1

Introduction to Cyber security & Ethical Hacking

Prepared By : Jayshree Dasa

Need for Cyber Security

- Imagine you have a house filled with valuable items. To keep your house safe from burglars, you lock your doors and windows, install security cameras, and maybe even get a guard dog. These measures help protect your home from intruders who might want to steal your belongings.
- Similarly, in the digital world, our computers, smartphones, and networks contain valuable information such as personal data, financial details, and sensitive documents. To protect this information from cybercriminals who might want to steal, damage, or misuse it, we need cyber security.

Cyber Security

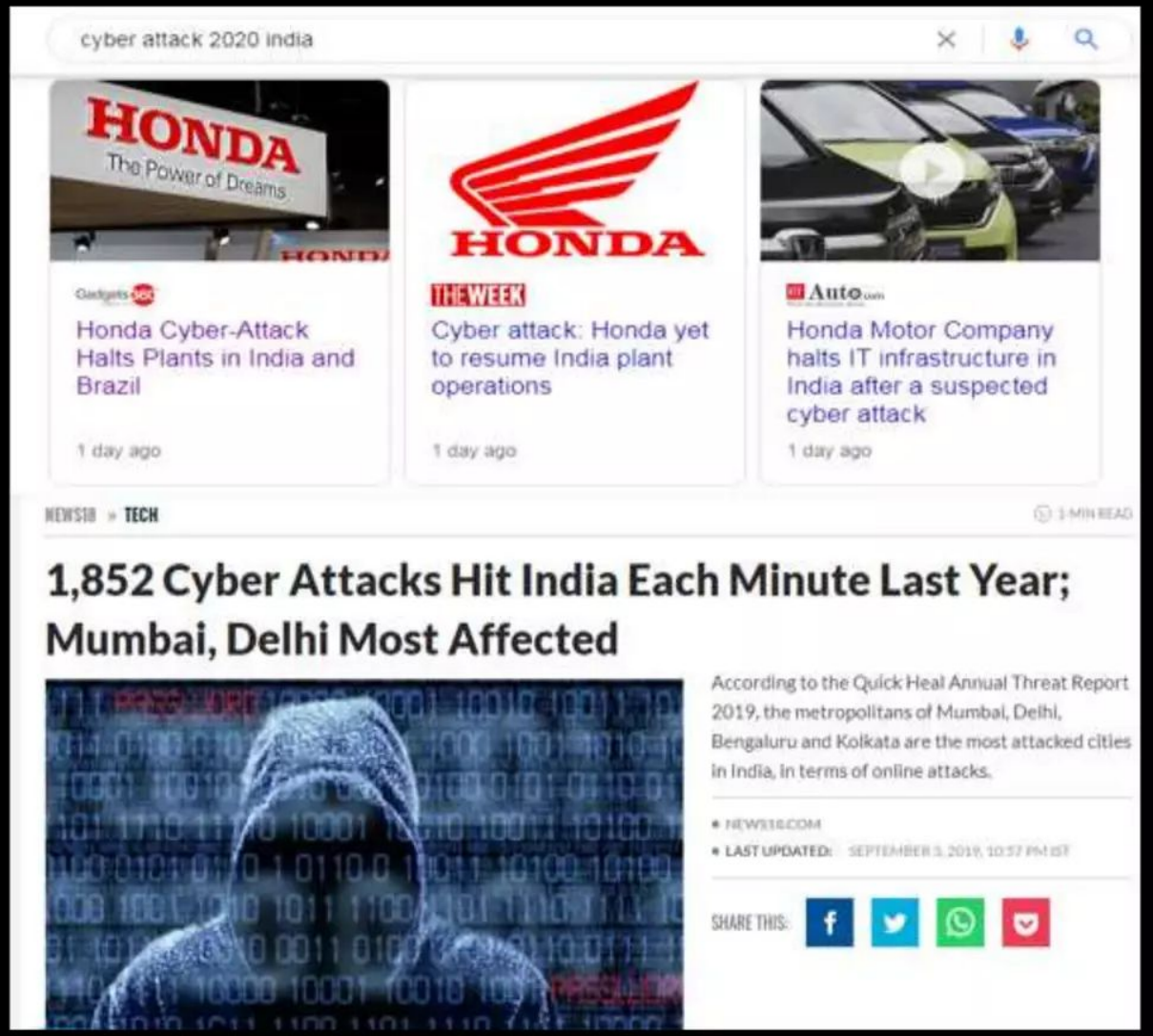
- Cyber security involves using various technologies, processes, and practices to protect our digital information and systems from cyber threats. These threats include viruses, hackers, and phishing attacks. Cyber security helps keep our digital world safe, just like locks and security systems keep our homes secure.
- **Example:** Imagine you have an email account. You use a strong password, enable two-factor authentication (where you need a code sent to your phone in addition to your password), and avoid clicking on suspicious links. These actions are part of cyber security practices to protect your email account from being hacked.

What is Cyber Attack?

- A cyber attack is any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices. Usually, the attacker seeks some type of benefit from disrupting the victim's network.

- An attacker is a person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent.

- Malware, Phishing, Man-in-the-middle attack, Denial-of-service attack, SQL injection etc. are the common types of cyber attack.



What is Cyber Security?

- Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
- It's also known as information technology security or electronic information security.
- The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories. Such as Network security, Application security, Information security & Operational security.

Why Cyber Security?

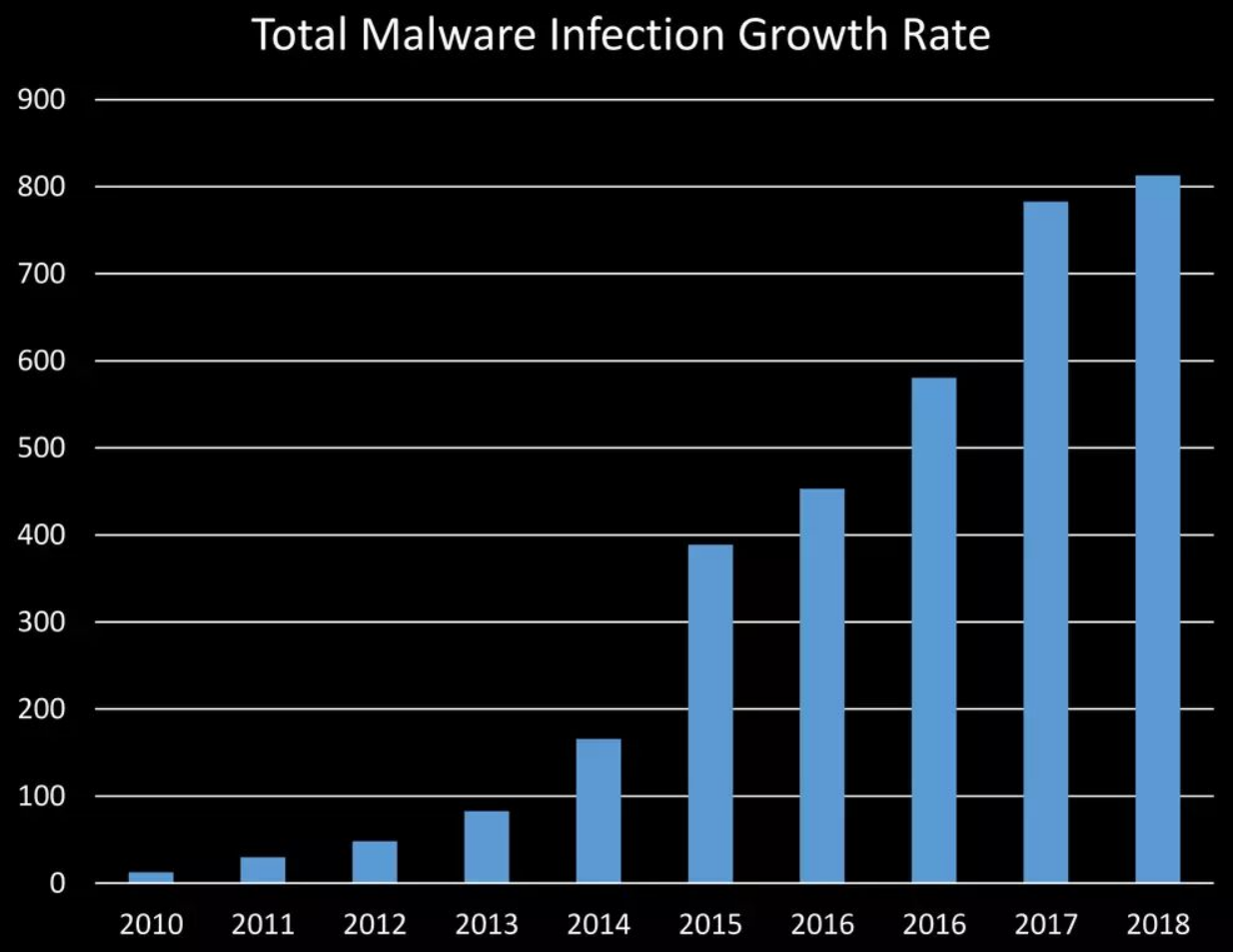
To build a computer system that prevents hackers' access and safeguard system and information from malicious attack.

To manage adequate preventive measures in order to avoid security breaches.

To safeguard user or customer information available in business transactions and visits.

To test networks at regular intervals.

To create security awareness at all levels in a business.



CIA Triad

- Confidentiality
- Integrity
- Availability

What is CIA?

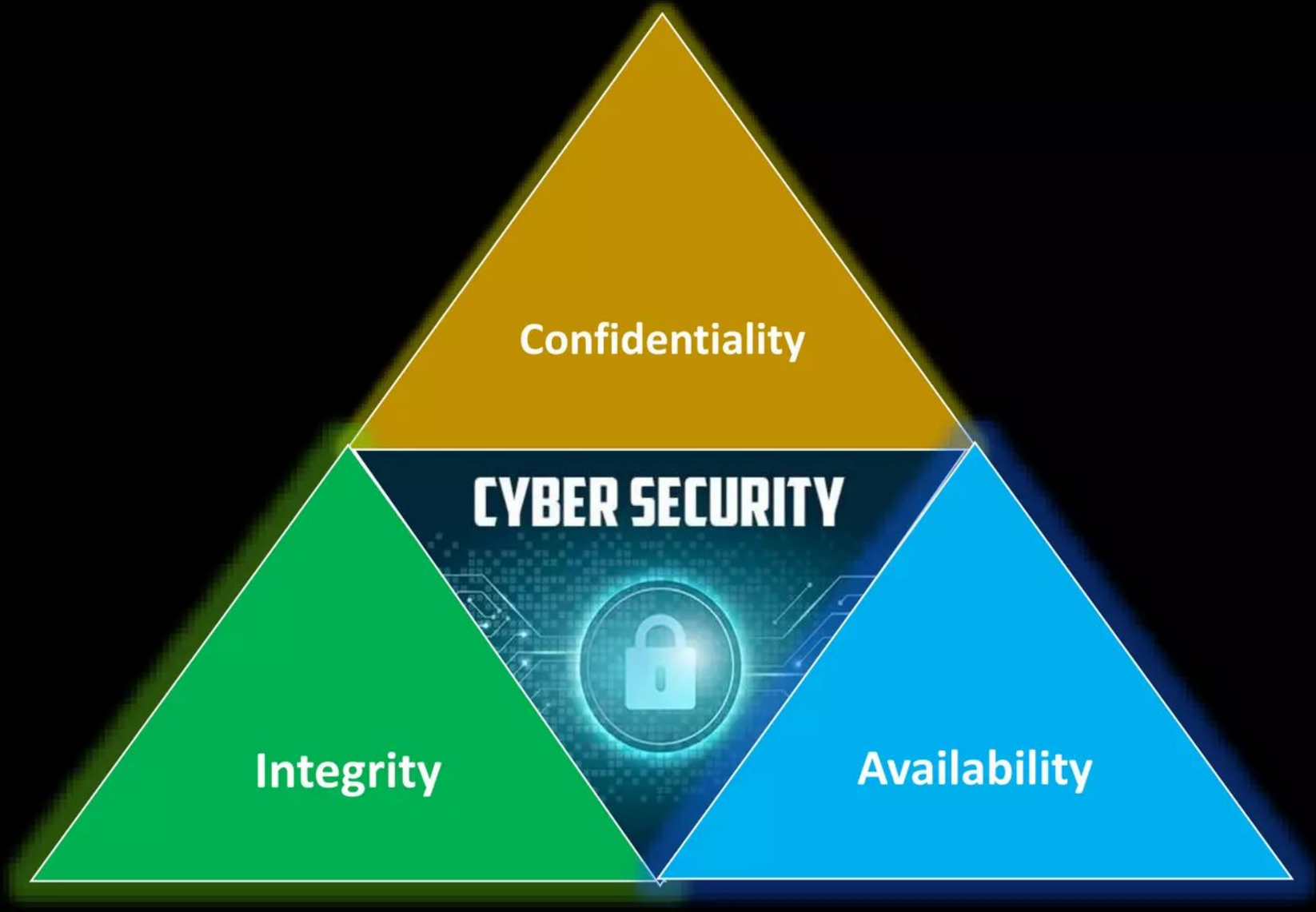
The CIA triad is a guide for measures in information security.

The CIA triad serves as a tool or guide for securing information systems and networks and related technological assets.

What is CIA Triad?

The CIA triad is a model that shows the three main goals needed to achieve information security.

Fundamental Goals of Cyber Security



Confidentiality

- **Definition:** Confidentiality means keeping information secret and accessible only to those who are authorized to see it.
- **Example:** Imagine you have a diary where you write your personal thoughts. You keep it locked in a drawer, and only you have the key. This ensures that no one else can read your diary entries, keeping your thoughts confidential.
- **In Cyber Security:** Encryption is often used to keep data confidential. For example, when you send a message over a secure messaging app, the app encrypts the message so that only the intended recipient can read it.

Integrity

- **Definition:** Integrity means ensuring that information is accurate, consistent, and not altered by unauthorized individuals.
- **Example:** Think of a bank statement you receive every month. You trust that the statement accurately reflects your transactions and account balance. If someone were to change the figures, the integrity of your bank statement would be compromised.
- **In Cyber Security:** Checksums and digital signatures are used to verify the integrity of data. For instance, when you download software, the developer might provide a checksum value that you can use to verify that the file hasn't been tampered with.

Availability

- **Definition:** Availability means ensuring that information and resources are accessible to authorized users when they need them.
- **Example:** Imagine you run an online store. You want your website to be available to customers 24/7 so they can make purchases at any time. If the website goes down, your customers can't buy anything, affecting your business.
- **In Cyber Security:** Redundant systems, regular backups, and protection against attacks like Distributed Denial of Service (DDoS) help maintain the availability of services and data. For example, an online banking service must be available to customers at all times, so banks implement measures to ensure their systems are up and running continuously.

The CIA Triad

What Is the CIA?		
Confidentiality	**Integrity**	**Availability**
The information is safe from accidental or intentional disclosure.	The information is safe from accidental or intentional modification or alteration.	The information is available to authorized users when needed.
Example		
I send you a message, and no one else knows what that message is.	I send you a message, and you receive exactly what I sent you (without any modification)	I send you a message, and you are able to receive it.
What's The Purpose of the CIA?		
Data is not disclosed	Data is not tampered	Data is available
How Can You Achieve the CIA?		
e.g., Encryption	e.g., Hashing, Digital signatures	e.g., Backups, redundant systems

Introduction

- Hacking:

  It is the **non-conventional** way of interacting with the system.

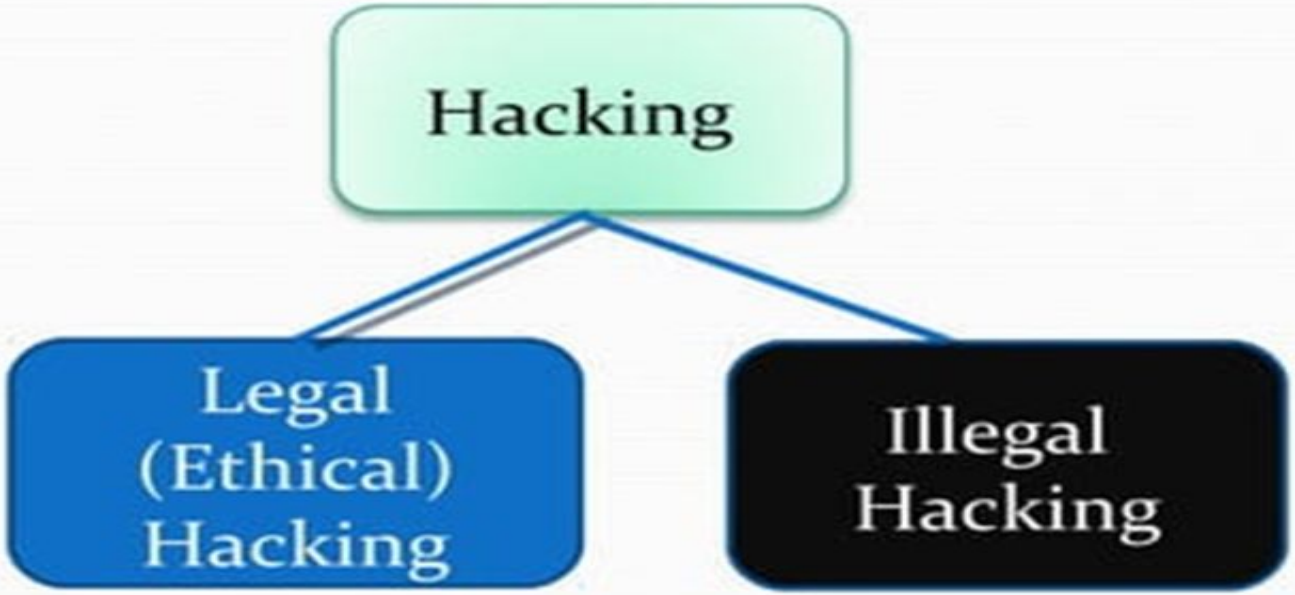
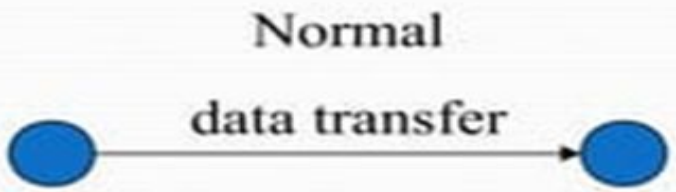
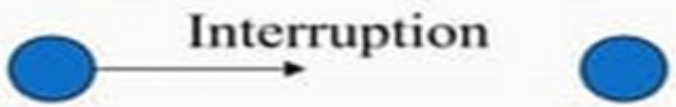
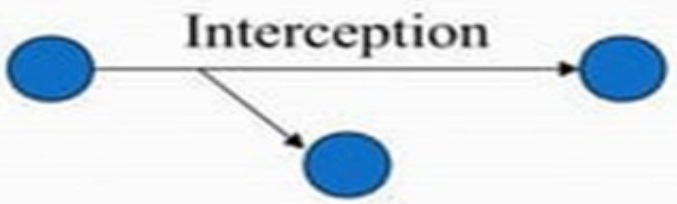


Figure: ways of hacking

Cont..


Normal
data transfer


Interruption


Interception


Modification


Fabrication

Cont..

- Interruption: An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on the availability.
- Interception: Information disclosure/information leakage. An unauthorized party gains access to an asset. This is an attack on confidentiality.
- Fabrication: An unauthorized party inserts counterfeit objects into the system. This is an attack on the authenticity.
- Modification: modifying the content of a message being transmitted in a network which leads integrity violation.

Hackers:

- A hacker is an individual who uses computer, networking or other skills to overcome a technical problem.(Good guys)
- A person who uses his or her abilities to gain unauthorized access to systems or networks in order to commit crimes.(Bad guys)

Types of Hackers

I. Black Hat Hacker
II. White Hat Hacker
III. Grey Hat Hacker

Cont..

I. **Black Hat Hacker**

- A black hat hackers or crackers are individuals with extraordinary computing skills, They use their knowledge and skill for their own personal gains probably by hurting others.

II. **White Hat Hacker**

- White hat hackers are those individuals professing hacker skills and using them for defensive purposes.
- use their knowledge and skill for the good of others and for the common good.

Cont..

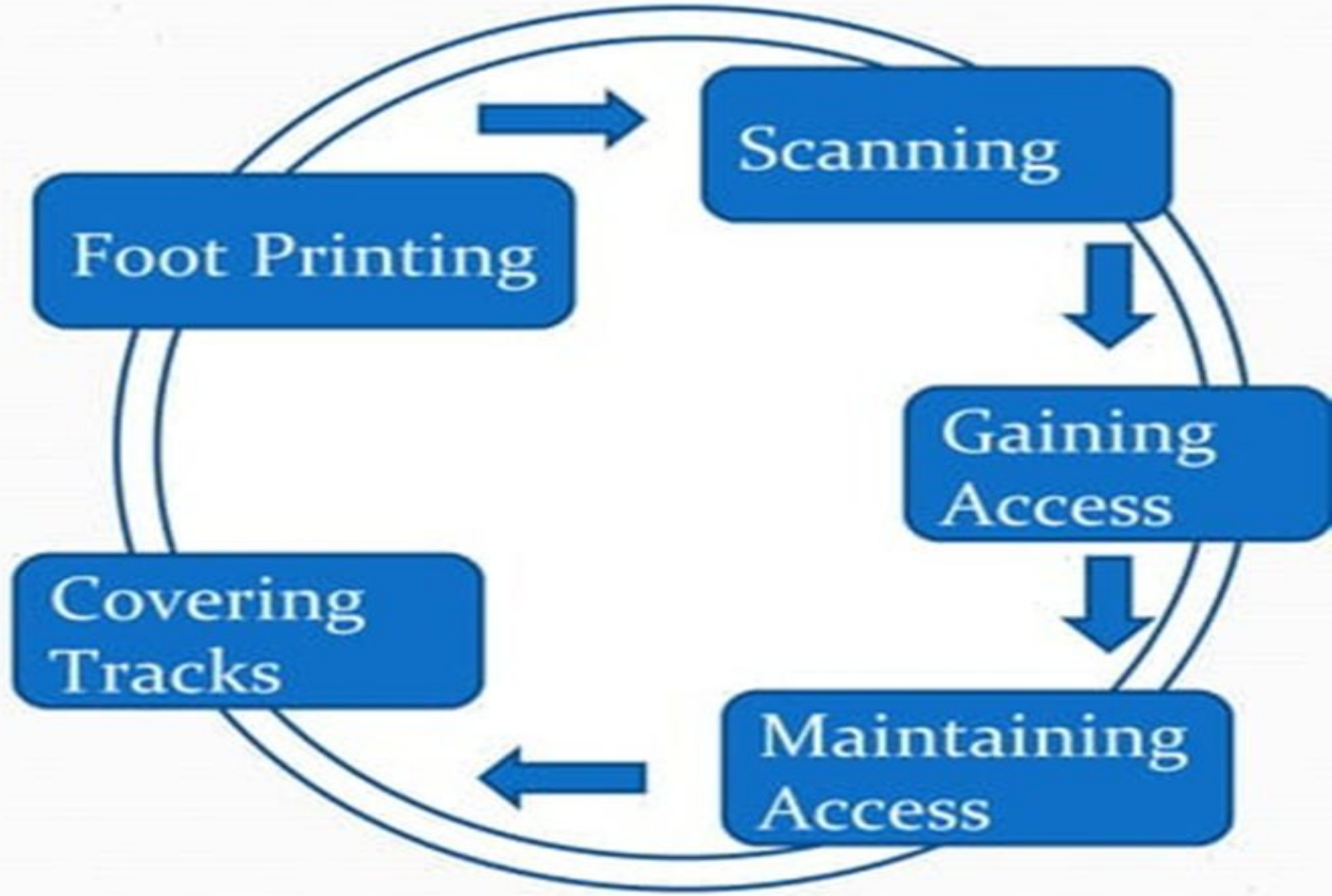
III. Grey Hat Hacker

- These are individuals who work both offensively and defensively at various times.
- We cannot predict their behavior.

Phases of Ethical Hacking

Hacking Process

i. Foot Printing
ii. Scanning
iii. Gaining Access
iv. Maintaining Access
v. Covering Tracks



Cont..

i. **Foot Printing:**

Collecting as much information about target such as DNS servers, Administrative contact and problem revealed by administrative.

ii. **Scanning:**

Collecting information by Port Scanning, Network Scanning, Finger Printing, etc. Example: SNMP Scanner.

iii. **Gaining Access**:

Enough data has been gathered at this point for attempt to access the target. Techniques are password eavesdropping, buffer overflow, etc.

Cont..

iv. **Maintaining Access:**

- Once a hacker has gained access, they want to keep that access for future exploitation and attacks.
- Once the hacker owns the system, they can use it as a base to launch additional attacks(eg. Trojans)

v. **Covering Tracks:**

- Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action.

Need Ethical Hacking

- Protection from possible External Attacks

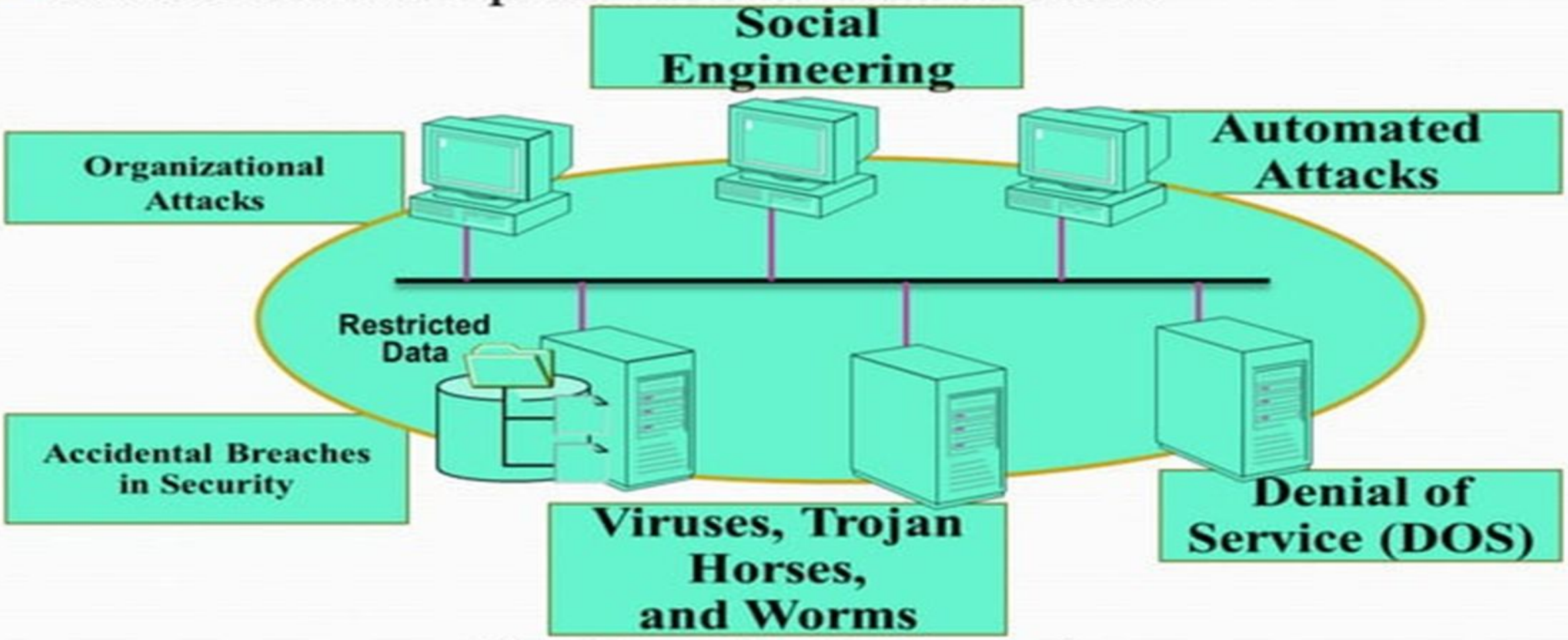


Fig: Protection from attacks

Advantage:

- To catch a thief -you have to think like a thief.
- Helps in closing the open holes in the system network
- Prevents website defacements
- Provides high security to banking and financial establishments.

Disadvantage:

- All depends upon the trustworthiness of the ethical hacker.
- Hiring professionals is expensive.

Security Architecture in Cyber Security

- Security architecture refers to the design and structure of systems that ensure the security of an organization's data and IT infrastructure. It involves implementing measures and protocols to protect against threats and vulnerabilities.

Cont.....

Key Components of Security Architecture

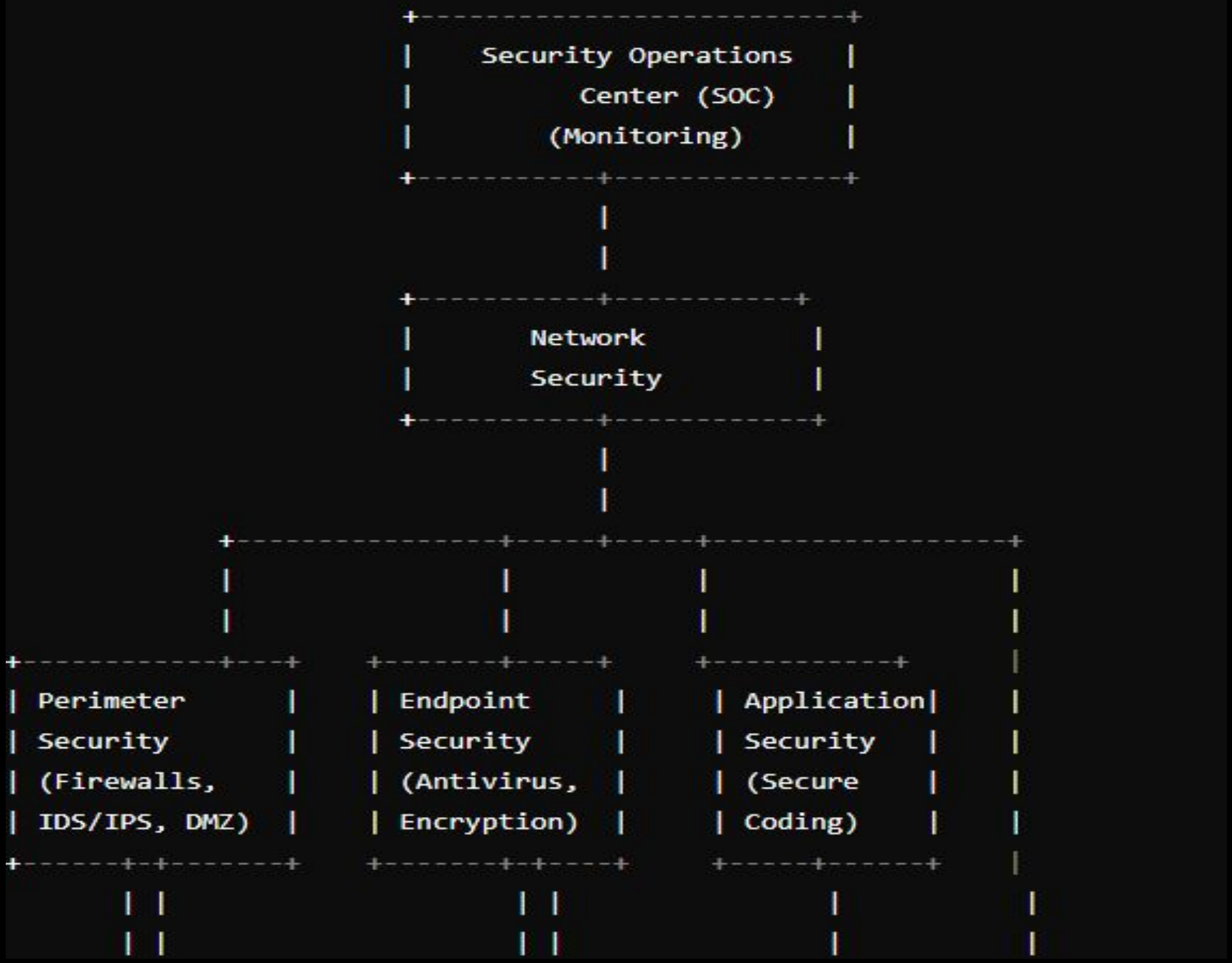
1. **Perimeter Security**: Protects the boundary of the network using firewalls, intrusion detection/prevention systems (IDS/IPS), and demilitarized zones (DMZ).
2. **Network Security**: Ensures the security of the internal network through segmentation, secure communication channels, and network access controls.
3. **Endpoint Security**: Protects individual devices like computers, smartphones, and servers using antivirus software, encryption, and endpoint detection and response (EDR).
4. **Application Security**: Secures software applications from threats by implementing secure coding practices, conducting regular security assessments, and using application firewalls.

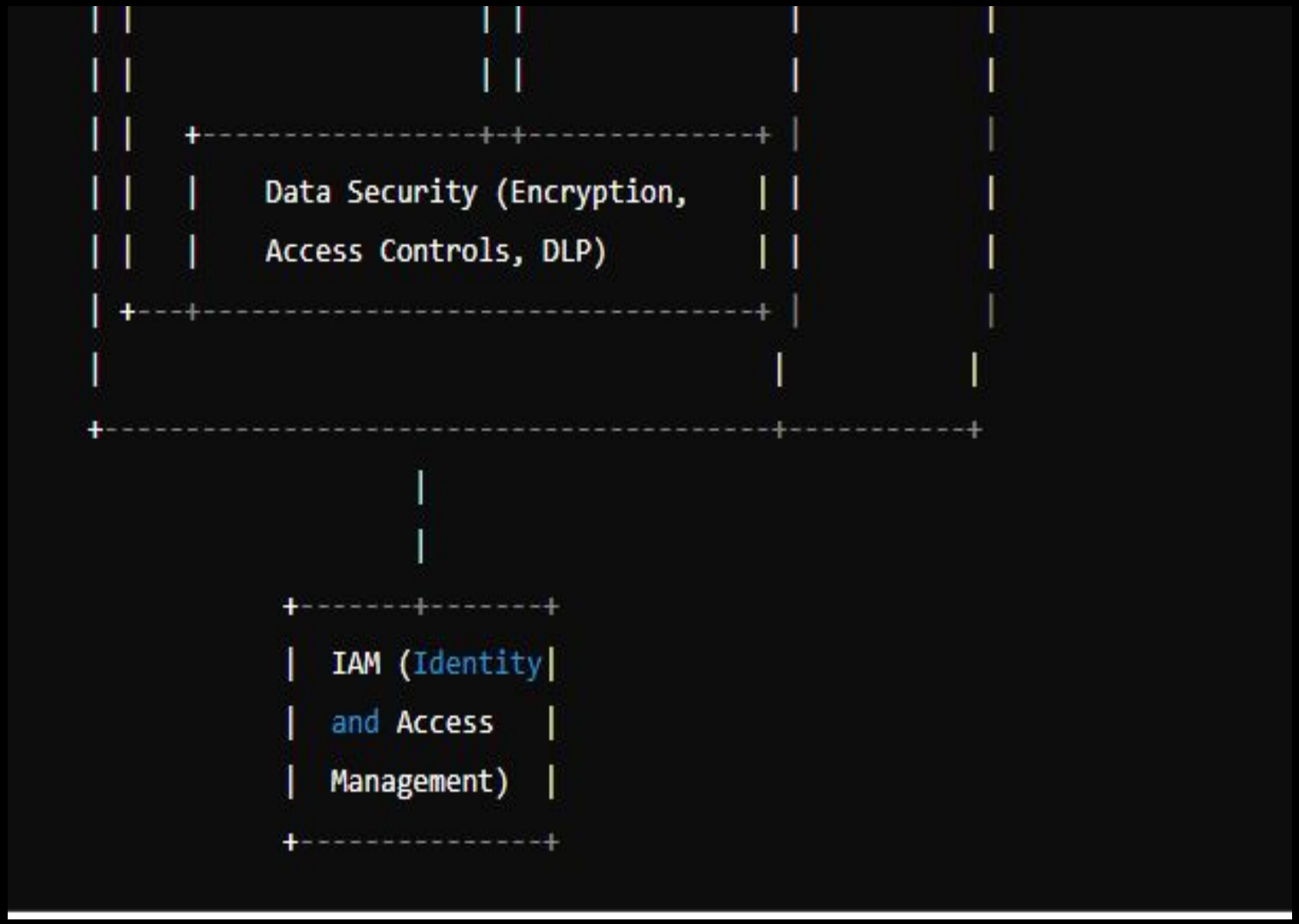
Cont.….

4. Data Security: Ensures the confidentiality, integrity, and availability of data through encryption, access controls, and data loss prevention (DLP) solutions.

5. Identity and Access Management (IAM): Manages user identities and controls access to resources through authentication (passwords, biometrics) and authorization (role-based access control).

6. Security Operations Center (SOC): A centralized unit that monitors, detects, and responds to security incidents using security information and event management (SIEM) systems.


Security Operations Center (SOC) (Monitoring)
Network Security
Perimeter Security (Firewalls, IDS/IPS, DMZ)
Endpoint Security (Antivirus, Encryption)
Application Security (Secure Coding)


Data Security (Encryption,
Access Controls, DLP)
IAM (Identity
and Access
Management)

Explanation of the Diagram

- **Perimeter Security:** Forms the outermost layer of defense, preventing unauthorized access to the network.
- **Network Security:** Manages the internal network's security by controlling traffic and segmenting networks.
- **Endpoint Security:** Focuses on protecting individual devices from threats.
- **Application Security:** Ensures that applications are secure from vulnerabilities.
- **Data Security:** Protects data through encryption and access controls.
- **Identity and Access Management (IAM):** Controls who can access what within the organization.
- **Security Operations Center (SOC):** Monitors the entire security architecture, detecting and responding to threats.

What is a Penetration Testing?

What is penetration Testing

Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit, Penetration testing can be automated with software applications or performed manually Either way.

The process of pen testing involves gathering information about the target before the test, identifying possible entry points, attempting to break in and reporting back the findings.

The main objective of penetration testing is to identify security weaknesses. Penetration testing can also be used to test an organization's security policy, its adherence to compliance requirements, its employees' security awareness and the organization's ability to identify and respond to security incidents.

Types of Vulnerabilities Assessment

1. Active Assessment
2. Passive Assessment
3. Network Assessment
4. Wireless Network Assessment
5. Application Assessment

Black Box Testing	White Box Testing
It is also called Specification Based Technique.	It is also called Structural Testing Technique.
Internal structure and coding knowledge is not required.	Internal structure and coding knowledge is required.
Main concentrate on functionality of system.	Main concentrate on code structure ,branches , loops, conditions etc.
Implementation knowledge is not required.	Implementation knowledge is required.

Fig 3: Comparison of Black Box and White Box Testing

Phases of Penetration Testing

1. Pre-Attack Phase
2. Attack Phase
3. Post-Attack Phase

Vulnerability Assessment VS Penetration Testing

Vulnerability Assessment	Penetration Testing
1. Automated Scanning	1. Automated and Manual
2. Less Time Consuming	2. More Time Consuming
3. Passive Scanning	3. Aggresive Scanning
4. Wide Scope	4. Focussed Scope
5. No Exploitation	5. Exploitation after discovery

Regulations & Frameworks

Regulatory Compliance And Restrictions

Cybersecurity Frameworks

Cybersecurity frameworks provide structured guidelines and best practices for managing cybersecurity risks. Key examples include:

NIST Cybersecurity Framework (National Institute of Standards and Technology):

- **Region:** United States
- **Focus:** Helps organizations manage and reduce cybersecurity risk.
- **Key Points:** Based on five functions – Identify, Protect, Detect, Respond, and Recover.

Cont….

ISO/IEC 27001:

ISO(International Organization for Standardization)

IEC(International Electrotechnical Commission)

- **Region:** International
- **Focus:** Provides requirements for an information security management system (ISMS).
- **Key Points:** Emphasizes risk management and continuous improvement.

Cont….

ISO/IEC 27001: Small level IT’s companies which are running on information technology for ex - Hosting companies, SAAS companies, IT Service provider companies.

Benefits : Increase client trust + prevent from hacking or cyber threat + secure in data breach + increase your business.

Cont….

ISO/IEC 27001

- Physical security control - biometric box at entrance | CCTV | digital entry register for employee register.
- Networking - secured networking and cyber security persecution etc.
- Operation software - You can’t install any kind of the software without permission.

Cybersecurity Regulations

Cybersecurity regulations are laws and rules designed to protect data and systems from cyber threats. Key examples include:

GDPR (General Data Protection Regulation):

- **Region:** European Union
- **Focus:** Protects personal data and privacy of EU citizens.
- **Key Points:** Requires data protection measures and mandates reporting data breaches within 72 hours.

GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) law taking effect on May 25, 2018. The goal of GDPR is to give EU citizens control over their personal data and regulate the data collection and processing approach of companies around the globe.

Businesses that are not in compliance with GDPR's requirement can face large fines up to 4% of a company's annual global revenue OR €20 million (whichever is greater).

How it effects?

There are six main ways in which this will affect website owners:

- How you collect user's data via forms (contact forms, newsletter signups etc.)
- How you collect analytics data
- What you do with the data
- Where the data is stored
- How you communicate with your customers and contacts
- The plugins and themes you use

Does GDPR apply to my WordPress site?

YES. It applies to every business, large and small, around the world (not just in the European Union).
If your website has visitors from European Union countries, then this law applies to you.

Requirements of GDPR

1- Protect user's personally identifying information (PII)
eg: name, emails, physical address, IP address, health information, income, etc.

2- Set higher standards for companies for collecting, storing, and using the data.

Cont….

HIPAA (Health Insurance Portability and Accountability Act):

- **Region:** United States
- **Focus:** Protects sensitive patient health information.
- **Key Points:** Sets standards for protecting electronic health records and requires safeguards to ensure data privacy and security.

Thank you!