**What is cyber security**?

Cyber security is the protection of internet-connected systems such as hardware, software and data from cyber threats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems

Computer security, cyber security, or information technology security is the protection of computer systems and networks from information disclosure, theft of, or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide

• The term cyber security refers to techniques and practices designed to protect digital data.

• The data that is stored, transmitted or used on an information system.

• Whereas security related to the protection which includes systems security, network security and application and information security.

**Why is cyber security important?**

Cyber security is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems.

•Cyber attacks can be extremely expensive for businesses to endure

• In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.

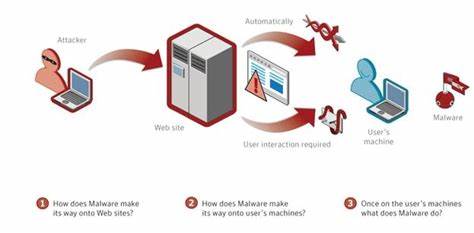
**Types of Cyber Attacks**

Cyber-attacks can be classified into the following categories

1) Web-based attacks

2) System-based attacks

**Web-based attacks**



These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows

1. **Injection attacks**

Injection attacks. Attack type. Attack description. Blind SQL Injection. Allows an attacker to use an error page returned by the database server to ask a series of True and False questions using SQL statements in order to gain total control of the database or execute commands on the system.

Example- SQL Injection, code Injection, log Injection, XML Injection etc

**2. DNS Spoofing**

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attackers computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

**3. Session Hijacking**

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data

**. 4. Phishing**

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

**5. Brute force**

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security

**6. Denial of Service**

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following

**Volume-based attacks**-

Volume-based attacks are characterized by an excessive amount of traffic (sometimes in excess of 100 Gbps). They do not mandate large amounts of traffic to be generated by one location or one source.

**Application layer attacks**- Its goal is to crash the web server and is measured in request per second.

**7. Dictionary attacks**

In cryptanalysis and computer security, a dictionary attack is an attack using a restricted subset of a keyspace to defeat a cipher or authentication mechanism by trying to determine its decryption key

**8. URL Interpretation**

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

**9. File Inclusion attacks**

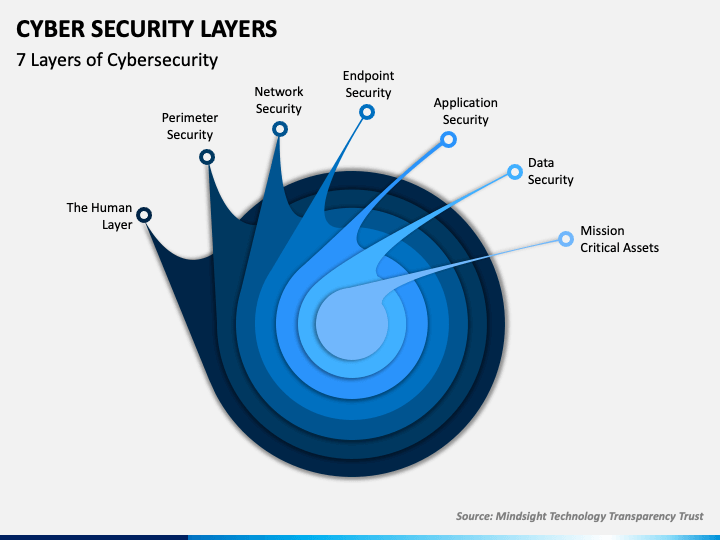
It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

**9. File Inclusion attacks**

It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

**10. Man in the middle attacks**

acts as It is a type of attack that allows an attacker to intercepts the connection between client and server and a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.



**The Seven Layers Of Cyber security**

1: Mission Critical Assets – This is the data you need to protect

2: Data Security – Data security controls protect the storage and transfer of data.

3: Application Security – Applications security controls protect access to an application, an application’s access to your mission critical assets, and the internal security of the application.

4: Endpoint Security – Endpoint security controls protect the connection between devices and the network.

5: Network Security – Network security controls protect an organization’s network and prevent unauthorized access of the network.

6: Perimeter Security – Perimeter security controls include both the physical and digital security methodologies that protect the business overall.

7: The Human Layer – Humans are the weakest link in any cyber security posture.

**SECURITY VULNERABILITIES, THREATS AND ATTACKS**

**Categories of vulnerabilities**

• Corrupted (Loss of integrity)

• Leaky (Loss of confidentiality)

• Passive – Make use of information from the system without affecting system resources

• Active – Alter system resources or affect operation

• Insider – Initiated by an entity inside the organization

• Outsider – Initiated from outside the perimeter

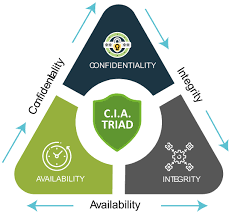
**Computer criminals**

A cybercrime is a crime that involves a computer or a computer network. The computer may have been used in committing the crime, or it may be the target Cybercrime may harm someone's security or finances.

or moderation is to understand who commits these crimes and why. Many studies have attempted to determine the characteristics of computer criminals. By studying those who have already used computers to commit crimes, we may be able in the future to spot likely criminals and prevent the crimes from occurring.

**CIA Triad**

The CIA Triad is actually a security model that has been developed to help people think about various parts of IT security.



**CIA triad broken down:** Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization.

**Confidentiality**

Confidentiality measures are designed to prevent sensitive information from unauthorized access. Integrity is the ongoing maintenance of consistency, accuracy and reliability of data throughout its lifecycle. And availability ensures information should be consistently and readily accessible for authorized parties.

**Integrity**

Data integrity is what the "I" in CIA Triad stands for.

This is an essential component of the CIA Triad and designed to protect data from deletion or modification from any unauthorized party, and it ensures that when an authorized person makes a change that should not have been made the damage can be reversed.

**Availability**

Availability is protecting the functionality of support systems and ensuring data is fully available at the point in time (or period requirements) when it is needed by its users. The objective of availability is to ensure that data is available to be used when it is needed to make decisions.

It's important to understand what the CIA Triad is, how it is used to plan and also to implement a quality security policy while understanding the various principles behind it. It's also important to understand the limitations it presents. When you are informed, you can utilize the CIA Triad for what it has to offer and avoid the consequences that may come along by not understanding it.

**Assets and Threat**

What is an Asset: An asset is any data, device or other component of an organization’s systems that is valuable – often because it contains sensitive data or can be used to access such information.

For example: An employee’s desktop computer, laptop or company phone would be considered an asset, as would applications on those devices. Likewise, critical infrastructure, such as servers and support systems, are assets. An organization’s most common assets are information assets.

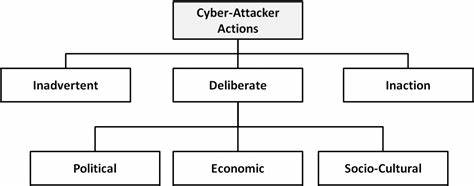
Threats can be categorized as circumstances that compromise the confidentiality, integrity or availability of an asset, and can either be intentional or accidental. Intentional threats include things such as criminal hacking or a malicious insider stealing information, whereas accidental threats generally involve employee error, a technical malfunction or an event that causes physical damage, such as a fire or natural disaster.

Motive of Attackers the categories of cyber-attackers enable us to better understand the attackers' motivations and the actions they take. As shown in Figure, operational cyber security risks arise from three types of actions: i) inadvertent actions (generally by insiders) that are taken without malicious or harmful intent; ii) deliberate actions (by insiders or outsiders) that are taken intentionally and are meant to do harm; and iii) inaction (generally by insiders), such as a failure to act in a given situation, either because of a lack of appropriate skills, knowledge, guidance, or availability of the correct person to take action Of primary concern here are deliberate actions, of which there are three categories of motivation.

1. Political motivations: examples include destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatory actions.

2. Economic motivations: examples include theft of intellectual property or other economically valuable assets (e.g., funds, credit card information); fraud; industrial espionage and sabotage; and blackmail.

3. Socio-cultural motivations: examples include attacks with philosophical, theological, political, and even humanitarian goals. Socio-cultural motivations also include fun, curiosity, and a desire for publicity or ego gratification.



Types of cyber-attacker actions and their motivations when deliberate

**Active attacks**: An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.

**Types of Active attacks**

****

Masquerade: in this attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.

**Session replay**: In this type of attack, a hacker steals an authorized user’s log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.

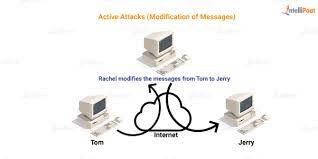
**Message modification**: In this attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.

In a **denial of service (DoS)** attack, users are deprived of access to a network or web resource. This is generally accomplished by overwhelming the target with more traffic than it can handle.

In a **distributed denial-of-service (DDoS)** exploit, large numbers of compromised systems (sometimes called a botnet or zombie army) attack a single target.

**Passive Attacks:** Passive attacks are relatively scarce from a classification perspective, but can be carried out with relative ease, particularly if the traffic is not encrypted.

**Types of Passive attacks:**

****

**Eavesdropping (tapping)**: the attacker simply listens to messages exchanged by two entities. For the attack to be useful, the traffic must not be encrypted. Any unencrypted information, such as a password sent in response to an HTTP request, may be retrieved by the attacker.

**Traffic analysis**: the attacker looks at the metadata transmitted in traffic in order to deduce information relating to the exchange and the participating entities, e.g. the form of the exchanged traffic (rate, duration, etc.). In the cases where encrypted data are used, traffic analysis can also lead to attacks by cryptanalysis, whereby the attacker may obtain information or succeed in unencrypting the traffic.

**Software Attacks:** Malicious code (sometimes called malware) is a type of software designed to take over or damage a computer user's operating system, without the user's knowledge or approval. It can be very difficult to remove and very damaging. Common malware examples are listed in the following table

**Virus** A virus is a program that attempts to damage a computer system and replicate itself to other computer systems. A virus

• Requires a host to replicate and usually attaches itself to a host file or a hard drive sector.

• Replicates each time the host is used.

• Often focuses on destruction or corruption of data.

• Usually attaches to files with execution capabilities such as .doc, .exe, and .bat extensions.

• Often distributes via e-mail. Many viruses can e-mail themselves to everyone in your address book.

• Examples: Stoned, Michelangelo, Melissa, I Love You

**Worm** A worm is a self-replicating program that can be designed to do any number of things, such as delete files or send documents via e-mail. A worm can negatively impact network traffic just in the process of replicating itself.

• Can install a backdoor in the infected computer.

• Is usually introduced into the system through a vulnerability.

• Infects one system and spreads to other systems on the network.

• Example: Code Red.

**Trojan horse** A Trojan horse is a malicious program that is disguised as legitimate software. Discretionary environments are often more vulnerable and susceptible to Trojan horse attacks because security is user focused and user directed. Thus the compromise of a user account could lead to the compromise of the entire environment. A Trojan horse

• Cannot replicate itself.

• Often contains spying functions (such as a packet sniffer) or backdoor functions that allow a computer to be remotely controlled from the network.

• Often is hidden in useful software such as screen savers or games.

• Example: Back Orifice, Net Bus, Whack-a-Mole

**Logic Bomb** A Logic Bomb is malware that lies dormant until triggered. A logic bomb is a specific example of an asynchronous attack.

• A trigger activity may be a specific date and time, the launching of a specific program, or the processing of a specific type of activity.

• Logic bombs do not self-replicate

**Hardware Attacks**

**Common hardware attacks include:**

• Manufacturing backdoors, for malware or other penetrative purposes; backdoors aren’t limited to software and hardware, but they also affect embedded radiofrequency identification (RFID) chips and memory

• Eavesdropping by gaining access to protected memory without opening other hardware

• Inducing faults, causing the interruption of normal behaviour

• Hardware modification tampering with invasive operations

• Backdoor creation; the presence of hidden methods for bypassing normal computer authentication systems

• Counterfeiting product assets that can produce extraordinary operations and those made to gain malicious access to systems

Cyber Threats-Cyber Warfare:Cyber warfare refers to the use of digital attacks -- like computer viruses and hacking -- by one country to disrupt the vital computer systems of another, with the aim of creating damage, death and destruction. Future wars will see hackers using computer code to attack an enemy's infrastructure, fighting alongside troops using conventional weapons like guns and missiles.

**Cyber Crime:**

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations.

**Cyber Terrorism:**

Cyber terrorism is often defined as any premeditated, politically motivated attack against information systems, programs and data that threatens violence or results in violence. The definition is sometimes expanded to include any cyber attack that intimidates or generates fear in the target population

Examples are hacking into computer systems, introducing viruses to vulnerable networks, web site defacing, Denial-of-service attacks, or terroristic threats made via electronic communication

**Cyber Espionage:**

Cyber spying, or cyber espionage, is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information from CYBER SECURITY Page 17 individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet

****

**Security Policies**

A cyber security policy defines and documents an organization's statement of intent, principles and approaches to ensure effective management of cyber security risks in pursuit of its strategic objectives. Use this eBook to bring cyber awareness to your organization for better management of risk

Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information.

A security policy also considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

We use security policies to manage our network security. Most types of security policies are automatically created during the installation. We can also customize policies to suit our specific environment.

**Need of Security policies**

1) It increases efficiency.

2) It upholds discipline and accountability

3) It can make or break a business deal

4) It helps to educate employees on security literacy.

**THE END**