CHAPTER 1 TO 2

CIA traid:

The CIA triad (Confidentiality, Integrity, and Availability) is a model used in information security, but it can also be loosely applied to crime-fighting:

- **Confidentiality:** Protect sensitive information related to the investigation.
- **Integrity:** Ensure the accuracy and reliability of the evidence and data collected.
- **Availability:** Ensure that the necessary resources and information are accessible to those who need them to address the crime.

Attacks on CIA:

- **Confidentiality Attacks:** Stealing secrets.
- **Integrity Attacks:** Changing or faking information.
- **Availability Attacks:** Shutting things down.

Steps to fix a crime:

1. Identify

- **Objective:** Recognize and define the crime or threat.
- **Actions:** Gather initial information, identify the nature of the crime, and determine the key players involved (victims, suspects, witnesses).
- **Tools:** Intelligence reports, surveillance, witness statements, and forensic evidence.

2. Analyze and Evaluate

- **Objective:** Understand the crime in depth and assess its impact.
- **Actions:** Analyze the data collected, evaluate the motives, methods, and opportunities involved in the crime. Assess the potential risks and consequences.
- **Tools:** Data analysis, criminal profiling, threat assessment, and risk analysis.

3. Treat

- **Objective:** Take action to mitigate the threat and prevent future occurrences.
- **Actions:** Develop and implement strategies to address the crime, such as apprehending suspects, securing evidence, and preventing further incidents. This may also involve legal actions, policy changes, or security enhancements.
- **Tools:** Law enforcement operations, legal proceedings, security measures, and community outreach.

Vulnerability

- **What it is**:
  A weakness or flaw in a system, process, or design that could be exploited by an attacker.
- **Example**:
  - A software bug that allows unauthorized access.
  - Weak passwords or outdated software.

Threat

- **What it is**:
  A potential danger that could exploit a vulnerability and cause harm.
- **Example**:
  - A hacker trying to exploit a software bug.
  - A natural disaster like a flood damaging servers.

---

3. Risk

- **What it is**:
  The likelihood of a threat exploiting a vulnerability and the impact it would have.
- **Example**:
  - The risk of a data breach if a hacker exploits a software bug (high likelihood, high impact).
  - The risk of a flood damaging servers in a flood-prone area (low likelihood, high impact).

Cyber attacks:

1. Malware

- **What it is**:
  Malicious software designed to harm, exploit, or steal data from a system.
- **Examples**:
  - Viruses, worms, ransomware, spyware.
- **How it works**:
  - Infects devices via downloads, email attachments, or malicious links.

---

2. Phishing

- **What it is**:
  Tricking users into revealing sensitive information (e.g., passwords, credit card numbers) by pretending to be a trusted entity.
- **How it works**:
  - Fake emails, websites, or messages that look legitimate.
- **Example**:
  - An email pretending to be from your bank asking you to "verify" your account.

---

3. Password Attacks

- **What it is**:
  Attempts to steal or guess passwords to gain unauthorized access.
- **Types**:
  - **Brute Force**: Trying every possible combination.
  - **Dictionary Attack**: Using common words or phrases.
  - **Credential Stuffing**: Using stolen passwords from other sites.

---

4. Man-in-the-Middle (MITM)

- **What it is**:
  An attacker secretly intercepts and alters communication between two parties.
- **How it works**:
  - Eavesdropping on unsecured Wi-Fi or injecting malicious code.
- **Example**:
  - Stealing login credentials during an online banking session.

---

5. Advertising

- **What it is**:
  Using online ads to spread malware.
- **How it works**:
  - Malicious code is hidden in legitimate-looking ads.
- **Example**:
  - Clicking on an ad that secretly downloads malware.

---

6. Rogue Software

- **What it is**:
  Fake or malicious software that pretends to be legitimate.
- **How it works**:
  - Tricks users into downloading and installing it.
- **Example**:
  - Fake antivirus programs that demand payment to "remove" non-existent threats.

---

7. Drive-by Downloads

- **What it is**:
  Automatically downloading malware when visiting a compromised website.
- **How it works**:
  - Exploits vulnerabilities in browsers or plugins.
- **Example**:
  - Visiting a hacked website that silently installs malware.

---

8. DDoS (Distributed Denial of Service)

- **What it is**:
  Overwhelming a system, server, or network with traffic to make it unavailable.
- **How it works**:
  - Uses multiple compromised devices (a botnet) to flood the target.
- **Example**:
  - A website crashing due to a flood of fake traffic.

Summary

- **Malware**: Harmful software.
- **Phishing**: Tricking users into giving up sensitive info.
- **Password Attacks**: Stealing or guessing passwords.
- **MITM**: Intercepting communication.
- **Malvertising**: Spreading malware through ads.
- **Rogue Software**: Fake or malicious programs.
- **Drive-by Downloads**: Auto-downloading malware from websites.
- **DDoS**: Overloading a system to crash it.

Type	**Spreads Via**	**User Action Needed?**	**Main Purpose**
Trojan	Disguised as legitimate software	Yes	Steal data, backdoor access
Worm	Networks, no user interaction	No	Spread rapidly, consume resources
Virus	Attaches to files/programs	Yes	Corrupt files, spread to other systems
Ransomware	Email, downloads, exploits	Sometimes	Encrypt files, demand ransom

---

1. **Impersonation**:
   - The attacker pretends to be a trusted entity (e.g., your bank, IT department, or a popular website).
2. **Harvesting**:

    - The attacker tricks you into entering your login credentials on a fake website or form.
3. **Exploitation**:
    - The attacker uses your stolen credentials to access your accounts, steal data, or commit fraud.

Password attack:

- **Brute Force:** Guessing every possible password.
- **Dictionary Attack:** Guessing common passwords.
- **Keylogger:** Recording what you type to steal passwords.

Prevention:

Update password

Use Alpha-numeric

No dictionary

DoS Prevention:

- **Traffic Analysis & Control:** Monitor and manage data flow.
- **Recovery Management:** Have a backup plan.

MITM Prevention:

- **Encrypted WAP:** Secure your Wi-Fi.
- **HTTPS:** Always check for a padlock.
- **VPN:** Encrypt your internet traffic.

Adware Prevention:

- **Block Ads:** Use ad blockers.
- **Software Updates:** Keep everything up to date.
- **Common Sense:** Stay cautious online.

Propagation refers to the process of spreading, transmitting, or distributing something, depending on the context.

❖ **Common Uses of Propagation:**

1. **Network & Malware Propagation** – The way viruses, worms, and malware spread across systems. *(e.g., Email Worms, USB Infections)*

Prevention Rogue software:

Updated firewalls:

Use efficient antivirus:

General distrust:

Web Attacks:

- The attacker attempts to breach a web application. Common attacks of this type are SQL injection

Session Hijacking:

This is a complex attack that involves actually taking over an authenticated session.

DNS Poisoning:

- This involves altering DNS records on a DNS server to redirect client traffic to malicious websites, usually for identity theft.

Classification of Cyber Crimes:

Insider Attack:

- ❑ Person with authorized system access
- ❑ Dissatisfied or unhappy inside employees or contractors
- ❑ Motive could be revenge or greed
- ❑ Well aware of the policies, processes, IT architecture and weakness of the security system
- ❑ Comparatively easy for an insider attacker to steel sensitive information, crash the network, etc.
- ❑ Could be prevented by using IDS/IPS (IDS (Intrusion Detection & Prevention System)

External Attack:

- Hired by an insider or an external entity to the organization
- Organization not only faces financial loss but also the loss of reputation
- Attackers usually scan and gathering information
- Keeps regular eye on the log and carefully analyzing these firewall logs
- IDS/IPS can also protect from external attackers.

- Cyber attacks can also be classified as:
    - Unstructured attacks
        - Generally person who don't have any predefined motives to perform the cyber attack
        - Try to test a tool readily available over the internet
    - Structure attacks:
        - Performed by highly skilled and experienced people
        - Motives of these attacks are clear in their mind
        - Access to sophisticated tools and technologies to gain access to other networks without being noticed
        - Expertise to develop or modify the existing tools to satisfy their purpose
        - Usually performed by professional criminals, by a country on other rival countries, politicians to damage the image of the rival person or the country, terrorists, rival companies, etc.

Reasons for Commission of Cyber Crimes:

- Money:
    - People are motivated towards committing cyber crime is to make quick and easy money.
- Revenge:
    - Take revenge with other person/organization/society/caste or religion
    - Defaming its reputation or bringing economical or physical loss.
    - This comes under the category of cyber terrorism.
- Fun:
    - The amateur do cyber crime for fun.
- Recognition:
    - It is considered to be pride if someone hack the highly secured networks
- Anonymity:

    - Anonymity that a cyber space provide motivates the person to commit cyber crime
- Cyber Espionage:
    - At times the government itself is involved in cyber trespassing to keep eye on other person/network/country

Kinds of Cyber Crimes:

- Cyber Stalking
    - Stalking, harassing, threatening someone, or defame a person
    - The behavior includes false accusations, threats, sexual exploitation to minors, monitoring, etc.

Child Pornography

- Possessing image or video of a minor (under 18), engaged in sexual conduct.

- Forgery and Counterfeiting
    - Produce counterfeit which matches the original document
    - Not possible to judge the authenticity of the document
- Software Piracy and Crime related to IPRs: (Intellectual Property Rights)
    - An illegal reproduction and distribution
- Cyber Terrorism
    - Use of computer resources to intimidate or force government, the civilian population or any segment thereof in furtherance of political or social objectives
- Phishing
    - Acquiring personal and sensitive information of an individual via email
    - Vishing (voice phishing), Smishing
- Computer Vandalism
    - Physical destroying computing resources using physical force or malicious code
- Computer Hacking
    - Modifying computer hardware and software to accomplish a goal
    - Simply demonstrations of the technical ability, to sealing, modifying or destroying information for social, economic or political reasons

- Creating and distributing viruses over internet
    - Spreading of an virus can cause business and financial loss
- Spamming

- ❑ Sending of unsolicited and commercial bulk message
- ❑ Spams not only irritate the recipients and overload the network but also waste the time and occupy the valuable memory space

Cross Site Scripting

- ❑ Injecting a malicious client side script into a trusted website
- ❑ Malicious script gets access to the cookies and other sensitive information and sent to remote servers

- ■ Online Auction Fraud
  - ❑ Online auction fraud schemes which often lead to either overpayment of the product or the item is never delivered
- ■ Cyber Squatting
  - ❑ Reserving the domain names of someone else's trademark
  - ❑ Sell it afterwards at higher price

Basic Security Terminology:

Hackers (General Term)

A **hacker** is someone skilled in **computer programming, networking, and security**, who can exploit or protect systems. Hackers can be ethical or malicious.

White Hat Hackers (Ethical Hackers)

- Work **legally** to **test and improve cybersecurity**.
- Help organizations by finding and fixing vulnerabilities.
- Often hired as **penetration testers** or **security experts**.
- **Example:** Ethical hackers working for companies like Google or Microsoft.

Black Hat Hackers (Malicious Hackers)

- Break into systems **illegally** for personal gain, destruction, or espionage.
- Involve in **data theft, malware attacks, and financial fraud**.
- **Example:** Cybercriminals launching ransom ware attacks.

Gray Hat Hackers (Neutral Hackers)

- Operate between **white hat and black hat** ethics.

- Find vulnerabilities **without permission** but often report them instead of exploiting them.
- May still break laws but not always for harmful intent.
- **Example:** A hacker discovering a system flaw and notifying the company without prior approval.

Script Kiddies (Unskilled Hackers)

- Use **pre-made hacking tools and scripts** without deep technical knowledge.
- Often hack **for fun, fame, or minor attacks** like defacing websites or running small-scale DDoS attacks.
- **Example:** A teenager using a hacking tool to break into a school's system.