CCM Question bank

Unit 1

1) What is cybercrime, and how is it defined?

Origin and Meaning

- The term **"cybercrime"** originates from *cybernetics* (Greek: *kybernetes* = steersman/governor).
- First used in the **1990s** with the rise of the internet.
- Early incidents like the **Creeper virus (1971)** and the **Morris Worm (1988)** marked its foundation.

Definitions (Multiple Perspectives)

1. **Indian Law(Information Technology Act, 2000)** – Acts that involve the use of computers, digital systems, or communication networks to commit illegal activities, including hacking, identity theft, and digital fraud.
2. **FBI** – Cybercrime is a crime that involves a computer and a network, where computers are either tools for crime, targets of crime, or both.
3. **ENISA (EU Agency)** – Cybercrime includes crimes directed at computing and communication technologies, as well as crimes where digital systems are used as a tool to commit offenses.
4. **David Wall (2007)** – Classified as:
    - Cyber-dependent (hacking, malware).
    - Cyber-enabled (fraud, identity theft).
    - Content-related (illegal content sharing).

Common Elements

- Use of digital devices/networks.
- Harm to individuals, businesses, or governments.
- Illegal exploitation of systems/data.

2) Categorization of cybercrimes. Explain each one of them briefly.

(a) Based on Target

1. **Against Individuals:** includes crimes like identity theft and cyberstalking, which cause direct harm to a person.
2. **Against Property:** involves illegal activities such as hacking and ransomware that target digital assets.
3. **Against Organizations:** consists of threats like corporate espionage that aim to damage companies.
4. **Against Government:** encompasses acts like cyber warfare that threaten national security and sovereignty.

(b) Based on Mode of Operation

- **Cyber-Dependent:** crimes can only be committed using computers and networks, such as deploying malware.
- **Cyber-Enabled:** crimes are traditional offenses like fraud that are amplified in scale by using the internet.

(c) Based on Motivation

- **Financially Motivated:** crimes, such as ransomware attacks, are driven by the goal of monetary gain.
- **Politically Motivated:** activities, including hacktivism, are carried out to promote an ideological cause.
- **Personal Revenge:** is often the driver for insider threats from disgruntled employees.
- **Recreational:** cybercrimes are committed out of curiosity or for the challenge, often by novice hackers.

(d) Based on Medium

- **Social Media Crimes:** like harassment and doxxing exploit the connectivity of these platforms.
- **Email-Driven:** attacks, including phishing, use electronic mail as their primary vector.
- **Dark Web Crimes:** operate on hidden networks to facilitate illegal marketplaces and activities.

3) Categorization of cyber criminals. Explain each one of them briefly.

Based on Motivation

- **Financial Gain:** Those motivated by **Financial Gain** include fraudsters and ransomware gangs seeking profit.
- **Political/Ideological:** actors, such as hacktivists, aim to further a cause or disrupt opponents.
- **Personal Revenge:** Criminals driven by **Personal Revenge** often include disgruntled employees or former partners.
- **Curiosity/Ego:** Those acting out of **Curiosity/Ego** are typically script kiddies testing their limited skills.

Based on Expertise

- **Novices**: or script kiddies, lack deep knowledge and rely on pre-made tools.
- **Intermediate Hackers:** possess the skill to write their own basic tools and exploits.
- **Advanced Persistent Threat (APT) Actors:** are highly skilled groups, often state-sponsored, that conduct prolonged and targeted attacks.

Based on Crimes

- **Black-Hat Hackers:** break into systems for personal or malicious gain illegally.
- **White-Hat Hackers:** use their skills ethically to help organizations find and fix security flaws.
- **Grey-Hat Hackers:** operate in a moral grey area, sometimes breaking in without permission but often reporting vulnerabilities.
- **Insiders:** are a major threat as they abuse their legitimate access to harm an organization.
- **Organized Crime Groups:** run large, sophisticated networks to conduct fraud and other illegal activities online.

4) State the difference between cybercrime and cyber fraud. Justify your answer with example.

Aspect	Cybercrime	Cyber Fraud
Scope	Broad category of all illegal online activities.	Narrow subset focused specifically on financial deception.
Primary Goal	Disruption, espionage, data theft, or causing damage.	Direct and exclusive financial gain.
Nature of Act	Can be an attack on systems, data, or national security.	Always involves deception or trickery for monetary profit.
Motivation	Political, ideological, personal revenge, or financial.	Overwhelmingly and singularly financial.
Victim Impact	Operational disruption, reputational harm, psychological distress.	Primarily direct financial loss.
Legal Focus	Computer misuse, data protection, and national security laws.	Fraud, theft, and financial crime statutes.

Examples:

- **Cybercrime without Fraud:** A **Distributed Denial-of-Service (DDoS) attack** that shuts down a hospital's network is a cybercrime. The goal is disruption and causing harm, not direct financial theft from patients.
- **Cyber Fraud as a Cybercrime:** A **phishing scam** that tricks an employee into revealing their login credentials, which are then used to transfer company funds to the criminal's account, is both a cybercrime and a specific example of cyber fraud.

5) Explain in your own words: What do you understand about global population/workforce required in fighting against cybercrime?

Growing Need: The global surge in cybercrime has created a critical shortage of expertise, with the cybersecurity workforce gap now exceeding 3.5 million professionals worldwide.

Key Roles Required:

- Cybersecurity Analysts are essential for continuously monitoring networks to identify and mitigate potential security threats.
- Incident Responders act as the emergency team that contains and eradicates security breaches during an active attack.

- Ethical Hackers proactively uncover system vulnerabilities by simulating the techniques used by malicious attackers.
- Digital Forensics Experts investigate cybercrimes after the fact to determine the cause, extract evidence, and identify the perpetrators.
- Cyber Law Experts navigate the complex legal and regulatory landscape to help prosecute cybercriminals and ensure organizational compliance.

Challenges:

- The field faces the immense challenge of defending against constantly evolving threats, such as AI-powered malware and convincing deepfakes.
- A significant barrier to filling the workforce gap is the widespread lack of public awareness and accessible, formal training pathways into the profession.

6) Define the following:
   i) **Cyberspace:** It refers to the virtual environment created by interconnected computer networks, digital systems, and the internet, which enables the global exchange of information, communication, and online interactions
   ii) **Cybersquatting:** It is the act of registering, selling, or using a domain name with the intent of profiting from the goodwill of someone else's trademark, brand, or personal name, which is illegal in many jurisdictions.
   iii) **Cyber punk:** It is a dystopian subgenre of science fiction that combines advanced technology, such as artificial intelligence and cybernetics, with a gritty world characterized by social decay and a clash between humanity and oppressive systems.
   iv) **Cyber warfare:** It involves the use of digital attacks by nations or groups to disrupt, damage, or destroy another entity's information systems and critical infrastructure for strategic, political, or military purposes.
   v) **Cyber terrorism:** It is the use of the internet and digital systems to carry out acts of terrorism, aiming to cause disruption, fear, or harm to critical infrastructure in order to achieve ideological or political objectives.

7) Explain the relationship between cyber security and information security.

- Information Security (InfoSec) is the broader practice of defending all forms of information from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Its core goal is to uphold the CIA Triad: Confidentiality, Integrity, and Availability of information, whether in digital or physical form (e.g., paper documents, oral communications).
- Cybersecurity is a critical sub-discipline of InfoSec that focuses exclusively on protecting digital assets—including computers, networks, servers, and data—from cyberattacks and unauthorized digital access.
- The key relationship is that Cybersecurity is a subset of Information Security; it applies InfoSec principles specifically to the digital, online, and cyberspace domains.
- Example: Protecting a locked filing cabinet containing employee records is an Information Security measure, whereas encrypting a database of those same employee records and defending it from hackers is a Cybersecurity measure. Both aim to protect information, but Cybersecurity deals specifically with threats in the digital realm.

8) Discuss various types of cybercrimes including their modus operandi, impact, severity level and affected cyber security principles. (Types include: fishing, ransomware, identity theft, DDoS, insider threats, social engineering, malware attacks, cyber espionage, financial fraud, and crypto jacking)

Type of Cybercrime	Modus Operandi	Impact	Severity Level	Affected Security Principles
1. Phishing	Sending fraudulent emails or messages that impersonate trusted entities (e.g., banks, colleagues) to trick victims into revealing sensitive data like login	- Loss of personal/financial data. - Unauthorized access to systems. - Initial access for larger attacks.	**Medium to High** (Depends on the scale and sensitivity of the stolen data.)	**Confidentiality, Integrity** (Credentials can be used to alter data).

	credentials or credit card details.			
2. Ransomware	Malicious software (malware) that encrypts the victim's files or locks them out of their system. Attackers then demand a ransom payment in exchange for the decryption key.	- Data unavailability, halting operations. - Financial loss from ransom payments & downtime. - Reputational damage.	**High** (Especially critical for businesses, hospitals, and critical infrastructure.)	**Availability, Integrity** (Data is altered/encrypted and made inaccessible).
3. Identity Theft	Stealing personal identifiable information (PII) such as Social Security numbers, bank details, or addresses to impersonate the victim for fraudulent activities.	- Financial losses for the victim. - Damage to credit score and reputation. - Legal complications for the victim.	**High** (Long-term consequences for the victim's financial and personal life.)	**Confidentiality, Integrity** (Personal data is exposed and can be misused to create false records).
4. DDoS Attacks	Overwhelming a target server, service, or network with a massive flood	- Service outages and downtime. - Financial losses from disrupted operations.	**Medium to High** (Depends on the target; for an e-commerce	**Availability** (The primary goal is to deny access to legitimate users).

	of internet traffic from multiple compromised systems (a botnet), making it unavailable to legitimate users.	- Reputation damage and loss of customer trust.	site, it can be crippling.)	
5. Insider Threats	Malicious or negligent actions by employees, contractors, or business partners who misuse their authorized access to steal data, sabotage systems, or leak confidential information.	- Data breaches and loss of intellectual property. - Operational disruption. - Significant financial and reputational damage.	**High** (Insiders have trusted access, bypassing many external defenses.)	**Confidentiality, Integrity, Availability** (Can view, modify, or delete sensitive data).
6. Social Engineering	Manipulating human psychology to deceive individuals into breaking security procedures. Common methods include pretexting,	- Unauthorized access to physical or digital spaces. - Data breaches. - Installation of malware.	**Medium to High** (Bypasses technical controls by exploiting human trust.)	**Confidentiality** (Trickin g individuals into disclosing secrets).

	baiting, and tailgating into secure areas.			
7. Malware Attacks	Distributing malicious software like viruses, worms, Trojans, and spyware to infiltrate, damage, or gain unauthorized control over a system.	- System corruption or failure. - Data theft or destruction. - Financial loss and unauthorized access.	**High** (Can lead to full system compromise and act as a launchpad for other attacks.)	**Confidentiality, Integrity, Availability** (Can spy on, alter, or disable systems).
8. Cyber Espionage	State-sponsored or corporate actors use advanced, persistent techniques to covertly infiltrate networks and steal sensitive information like trade secrets, government intelligence, or R&D data.	- Loss of national security secrets or competitive advantage. - Economic damage. - Undermining national security.	**Critical** (Targets high-value information with strategic long-term consequences.)	**Confidentiality** (The primary goal is the unauthorized access to and theft of sensitive information).
9. Financial Fraud	Using digital means like phishing,	- Direct financial loss for individuals and	**High** (Directly targets	**Confidentiality, Integrity** (Financial data is exposed and

	malware, or data breaches to steal financial credentials (credit card numbers, banking logins) for unauthorized transactions.	businesses. - Reputational damage for financial institutions. - Loss of customer trust.	monetary assets.)	transactions are manipulated).
10. Cryptojacking	Unauthorized use of a victim's computing resources (computers, servers) to mine cryptocurrency. This is typically done by embedding malicious code in websites or infecting devices with malware.	- Degraded system performance and speed. - Increased electricity consumption and hardware wear-and-tear. - Operational costs.	**Medium** (Does not typically steal data, but consumes resources and slows down operations.)	**Availability** (Deprives the legitimate user of full system resources).

9) Discuss various types of mitigation strategies for the following:

(i) Attacks against individuals

- Individuals should use multi-factor authentication and a VPN to significantly enhance their personal security.

- They should also avoid clicking on unknown links or attachments in emails and messages.
- Keeping software and systems regularly updated is a simple yet critical defense against known vulnerabilities.

(ii) Attacks against organization

- Organizations must conduct regular penetration testing to proactively find and fix security weaknesses.
- Employee awareness training is essential to create a human firewall against social engineering attacks.
- Implementing robust data encryption and maintaining regular backups are key to mitigating the impact of a breach.

(iii) Attacks against government

- Governments need to establish and enforce strong national cybersecurity policies and frameworks.
- A top priority must be protecting critical national infrastructure from state-sponsored and other attacks.
- International cooperation and treaties are vital for tracking and prosecuting cross-border cybercriminals.

(iv) Attacks against society

- Widespread cyber awareness campaigns are needed to educate the general public on digital risks.
- Digital literacy programs should be integrated into education to build a safer future online.
- Efforts to control the spread of fake news and disinformation are crucial for maintaining social stability.

10) Discuss any two case studies related to cybercrime. Describe the incident and its impact along with the mitigation strategy adopted.

Case Study 1: Targeted Phishing at Ubiquiti Networks (2021)

Incident:

Ubiquiti Networks, a major networking equipment manufacturer, was targeted in a phishing attack. Hackers gained unauthorized access to internal systems, including customer data stored on cloud-based services. The attackers used stolen credentials obtained through phishing.

Impact:

- Compromise of sensitive customer data.
- Damage to the company's reputation.
- Significant financial costs for investigation and mitigation.

Mitigation:

Ubiquiti implemented stronger security measures, including mandating 2FA for employee accounts, and enhanced their monitoring systems.

Case Study 2: The Google and Facebook Scam (2013-2015)

Incident:

A Lithuanian hacker impersonated a vendor and sent fake invoices to Google and Facebook employees. By using phishing emails that appeared legitimate, the attacker convinced employees to wire over $100 million to fraudulent accounts.

Impact:

- Loss of $100 million (though much of it was later recovered).
- Highlighted vulnerabilities in vendor payment processes.

Mitigation:

- Both companies strengthened their vendor verification processes.
- They implemented stricter controls for financial transactions, such as requiring multiple levels of approval.

11) Write a note on the factors causing cybercrime.

- **Security System Vulnerabilities:** Unpatched software and weak security configurations create easy entry points for attackers.

- **Lack of Security Awareness:** Users clicking suspicious links or using weak passwords unknowingly facilitate attacks.
- **Technological Advancements:** Rapid development of AI and other technologies provides new tools for sophisticated attacks.
- **Internet Anonymity:** The ability to hide identities online emboldens criminals and makes them difficult to trace.
- **Financial Motivation:** Many attacks are driven by direct monetary gain through fraud, theft, or extortion.
- **Weak Cyber Laws:** Insufficient legal frameworks and enforcement in some regions reduce risks for cybercriminals.
- **Dependence on Technology:** Widespread reliance on digital systems creates numerous attractive targets for exploitation.

12) Write a note on the impact of cybercrime on individuals and organizations at large.

- **Financial Losses:** Direct theft of funds, ransom payments, and business disruption cause significant monetary damage.
- **Data Breaches:** Exposure of sensitive personal, financial, and corporate information leads to privacy violations.
- **Critical Infrastructure Disruption:** Attacks on essential services like power grids threaten public safety and national security.
- **Psychological Impact:** Victims of cyberbullying, harassment, and identity theft suffer emotional distress and mental health issues.

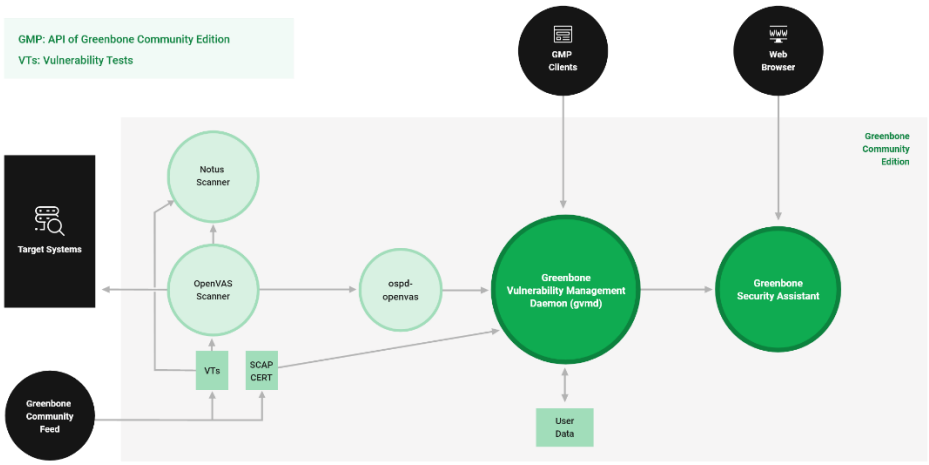
13) Discuss the survival mantra for netizens to protect themselves against cybercrime.

- Use strong, unique passwords and enable two-factor authentication (2FA) on all accounts.
- Be cautious of unsolicited emails and links - verify before clicking.
- Install and regularly update antivirus software and firewalls.
- Use VPNs on public Wi-Fi networks to encrypt connections.
- Limit personal information shared on social media platforms.
- Back up important data regularly to external drives or cloud services.
- Keep all software and operating systems updated with security patches.
- Report cybercrimes immediately to the appropriate authorities.

14) Discuss the architecture of OpenVAS and state its importance in cybercrime and mitigation.

- **OpenVAS Scanner:** The core engine that executes Network Vulnerability Tests (NVTs) to scan target systems for security weaknesses.
- **OpenVAS Manager:** A central controller that manages scan jobs, aggregates results from the scanner, and handles the vulnerability data.
- **Greenbone Security Assistant (GSA):** A user-friendly web-based interface that allows users to configure scans, view results, and generate detailed reports.
- **OpenVAS CLI:** A command-line interface providing an alternative method for interacting with the OpenVAS system.
- **Database:** A storage system that maintains scan configurations, results, and all vulnerability information for analysis and reporting.

Importance: Provides a comprehensive, open-source framework for vulnerability management, enabling organizations to proactively identify and remediate security flaws in their networks.

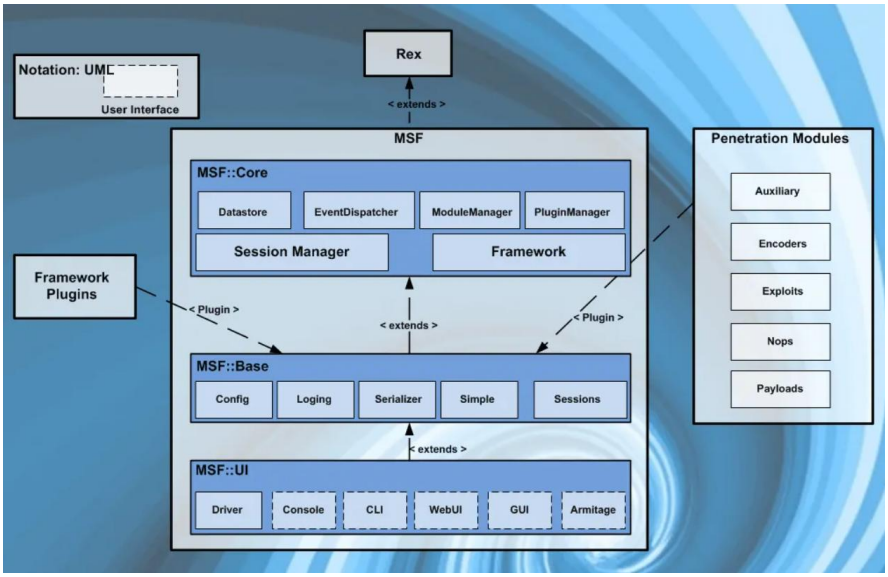


15) Discuss the architecture of Metasploit and state its usefulness in cybercrime investigation.

Metasploit consists of several integrated components:

1. **MSF Console (msfconsole)**: Primary interface for framework interaction
2. **Module System**: Categorized repositories of exploits, payloads, post modules, etc.
3. **REX Library**: Low-level tasks including networking and exploitation primitives

4. **Framework Core**: API that connects components and manages module execution
5. **Framework Base**: Provides common resources needed by modules
6. **msfdb**: Backend database for storing scan results, credentials, and hosts
7. **Plugins**: Extend functionality for specific tasks or integrations



Unit 2

1. Why should mobile devices be protected.

- They store critically sensitive business information and confidential personal data.
- Mobile devices are frequently used to access secure organizational networks and email systems.
- They are highly susceptible to being lost or stolen due to their portable nature.
- These devices are constant targets for malware infections and cyber-attacks.
- They often contain access to financial applications and banking information.
- A compromised device can serve as an entry point for attackers into a larger corporate network.
- Protecting them is essential to safeguard against identity theft and financial fraud.

2. Write a note on proliferation of mobile and wireless devices.

- There is a visible, widespread adoption of people using smartphones and tablets in public spaces like cafes and airports.
- These devices are no longer just for communication but are used for gaming, shopping, banking, and accessing corporate data on the go.
- Technological advances have led to smaller devices with significantly more processing power.
- The market has evolved from simple wireless phones and PDAs to sophisticated smartphones and high-end PDAs with integrated wireless capabilities.
- A key driver for this growth is the rapid development of business applications for handheld devices.
- Simple handheld devices now provide enough power to run applications, play media, and handle voice calls, increasing their utility and adoption.

3. Write a note on categorisation of mobile and wireless devices.

- **Portable Computer:** A general-purpose computer that can be moved but isn't used during transit and requires an AC power source.
- **Tablet PC:** A slate-shaped device with a touchscreen and stylus, capable of most laptop tasks but often lacking a physical keyboard.
- **Internet Tablet:** An internet appliance with limited computing power, primarily used for web browsing and media playback.
- **Personal Digital Assistant (PDA):** A small, pocket-sized computer for managing contacts, notes, and email, syncing with a desktop.
- **Smartphone:** A PDA that integrates full cell phone functionality, supporting a wide range of features and installable applications.
- **Ultramobile PC (UMPC):** A full-featured, PDA-sized computer running a general-purpose operating system like Windows.
- **In-car Computer:** A computing device installed in vehicles, functioning as a wireless computer, GPS, and entertainment system.

4. What are the mobility types. Quote day to day examples of your familiarity that relates to them.

- **User Mobility:** The user can access the same service from different locations or devices. *Example:* Checking your work email from your home desktop, office laptop, and personal smartphone.
- **Device Mobility:** A communication device moves between different networks while maintaining a connection. *Example:* A smartphone automatically switching from your home Wi-Fi to the cellular network as you leave your house.
- **Session Mobility:** A user session can be moved from one device to another. *Example:* Starting to watch a movie on your living room TV and resuming it on your tablet in the bedroom.
- **Service Mobility:** A user's services (like phone number) are portable across devices and networks. *Example:* Porting your mobile phone number from one telecom provider to another.
- **Code Mobility:** Software components can be dynamically downloaded and executed on different devices. *Example:* Using a web browser to run a web application that downloads and executes code (like JavaScript) on your local machine.

5. Discuss the popular types of attacks against mobile networks.

- **Malware, Viruses, and Worms:** Malicious software like the Cabir Worm or Brador Trojan designed to infect mobile operating systems (e.g., Symbian, Windows CE) to steal data or damage devices.
- **Denial-of-Service (DoS/DDoS) Attacks:** Flooding a target system or network with excessive traffic to make it unavailable to legitimate users, slowing or halting services.
- **Overbilling Attacks:** An attacker hijacks a subscriber's IP address to conduct paid downloads or use data services, causing the legitimate user to be charged for unauthorized activities.
- **Spoofed Policy Development Process (PDP) Attacks:** Exploiting vulnerabilities in the GPRS Tunneling Protocol (GTP) to intercept or manipulate data sessions on mobile networks.

- **Signaling-level Attacks:** Targeting vulnerabilities in signaling protocols like the Session Initiation Protocol (SIP), which is used for VoIP services in IP multimedia subsystems (IMS).

6. Illustrate online environment for credit card transaction and discuss the elements of credit card frauds and its types.

- **Transaction Flow:**
    1. A cardholder swipes their card at a merchant's terminal.
    2. The data is sent to the merchant server.
    3. A security module checks the PIN.
    4. The request is routed through the acquiring bank to the card-issuing bank via a back-end network.
    5. The bank approves or declines the transaction.
- **Elements of Credit Card Fraud:**
    - Fraudulently obtaining, using, or forging someone else's card or information.
    - Using one's own card knowing it is revoked, expired, or has insufficient funds.
    - Selling goods/services to someone using an illegally obtained or unauthorized card.
- **Types of Credit Card Fraud:**
    - **Lost or Stolen Cards:** Physically stealing a card to make unauthorized purchases.
    - **Account Takeover:** A fraudster obtains a cardholder's personal details, reports the card lost, and has a new one sent to a different address.
    - **Counterfeit Cards:** "Skimming" or "cloning" card data onto a fake card.
    - **"Never Received":** Intercepting a new or replacement card from the mail.
    - **Fraudulent Application:** Using another person's identity to apply for and obtain a credit card.
    - **Mail Order/Telephone Order (MO/TO) Fraud:** Using stolen card details for "card-not-present" transactions online or over the phone.

7. List down the fraud protection practices that should be followed by individual in case of credit card frauds.

- Keep a secure record of your account numbers, expiration dates, and the fraud reporting phone number for each card.
- Never lend your card to anyone and shred old receipts and statements before disposal.
- Do not give your account number to anyone who calls you; only provide it when you have initiated the call to a reputable company.
- Carry your cards separately from your wallet and only carry the card you need for a specific outing.
- During a transaction, keep your eye on your card and never sign a blank receipt.
- Save your receipts to compare with your statement and check your bills promptly, reporting any questionable charges immediately.
- Notify your card issuer immediately if your address changes or you will be traveling.

8. What are the security challenges posed by mobile devices.

- **Physical Loss or Theft:** Devices are small and portable, making them easy to lose or steal, leading to direct data loss.
- **Micro and Macro Challenges:** Includes device-level management issues ("micro") and broader organizational policy challenges ("macro").
- **Diverse Threat Vectors:** Devices face application-based, web-based, network-based, and physical threats.
- **Complex Device Management:** High cost and complexity of managing a diverse range of devices and providing user technical support.
- **Insecure Connectivity:** Multiple connection options (Cellular, Wi-Fi, Bluetooth) increase the attack surface.
- **Data Leakage:** Information is taken outside the physically secure office environment.
- **Granting Remote Access:** Devices require remote access back to the corporate network, which can be exploited if the device is compromised.

9. Discuss and describe in detail, categorisation of mobile phone security threats.

- **Application-Based Threats:** Arise from downloadable apps.
    - **Malware/Spyware:** Malicious apps that steal data or damage the device.
    - **Privacy Threats:** Apps that access and transmit personal information without consent.
    - **Zero-Day Vulnerabilities:** Exploiting unknown flaws in applications.
- **Web-Based Threats:** Occur through internet browsing.
    - **Phishing Scams:** Fake websites designed to steal login credentials.
    - **Drive-By Downloads:** Malware automatically downloaded when visiting a compromised website.
    - **Social Engineering:** Tricking users into revealing sensitive information online.
- **Network-Based Threats:** Exploit device connectivity.
    - **Wi-Fi Sniffing:** Eavesdropping on data transmitted over unsecured Wi-Fi.
    - **Cross-Platform Attacks:** Leveraging multiple network types (e.g., Cellular, Wi-Fi, Bluetooth) to launch an attack.
- **Physical Threats:** Related to the device's physical security.
    - **Loss or Theft:** The most common physical threat, leading to data and device loss.

10. List down and explain different types of attacks that can be performed on mobile phones or devices.

- **SMiShing (SMS Phishing):** Sending fraudulent text messages with links to trick users into providing sensitive data or downloading malware.
- **Man-in-the-Middle (MitM) Attacks:** Intercepting communications on unsecured networks (like public Wi-Fi) to eavesdrop or alter data.
- **Malware:** Software designed to infect a device to steal data or cause damage, often delivered via malicious apps or websites.
- **Jailbreaking/Rooting Exploits:** Taking advantage of users who bypass device security restrictions, making the device more vulnerable to attack.

- **Wi-Fi Spoofing:** Setting up a fake wireless access point with a legitimate-sounding name to trick users into connecting, allowing data interception.
- **Bluejacking:** Sending unsolicited messages to nearby Bluetooth-enabled devices.
- **Bluesnarfing:** Unauthorized access and theft of information from a wireless device via Bluetooth.

11. Explain the counter-measures to be practised for possible attacks on mobile or cell phones.

- **Use Security Software:** Install and regularly update anti-malware and firewall applications.
- **Enable Strong Authentication:** Use device passwords, PINs, and biometrics (fingerprint/face recognition).
- **Be Cautious with Connectivity:** Disable Bluetooth and Wi-Fi when not in use; avoid using public Wi-Fi for sensitive transactions without a VPN.
- **Download Apps Judiciously:** Only install applications from official and trusted app stores.
- **Keep Software Updated:** Regularly update the device's operating system and all applications to patch security vulnerabilities.
- **Educate Yourself:** Be aware of phishing and SMiShing tactics; do not click on suspicious links in emails or messages.
- **Enable Remote Wipe:** Use device tracking and remote wipe features to erase data if the device is lost or stolen.

12. What kind of cybersecurity measures an organisation should have to take in case of portable storage devices, prepare security guidelines which can be implemented in an organisation.

Security Measures:

- **Establish Clear Policy:** Create and enforce rules governing acceptable use of portable storage devices
- **Mandate Encryption:** Require all data on portable devices to be encrypted
- **Centralize Management:** Maintain inventory of all authorized portable storage devices

- **Control Physical Access:** Restrict USB and removable ports using device control software
- **Implement Access Controls:** Enforce strong passwords and multi-factor authentication
- **Conduct Training:** Educate employees about portable storage risks and policies
- **Promote Alternatives:** Encourage use of secure company cloud storage over physical devices

Implementation Guidelines:

1. **Password & Access:** Use strong passwords with password manager; enable MFA; never share credentials
2. **Device Security:** Password-protect and encrypt all devices; maintain updated software; lock screens when away
3. **Data Handling:** Store files on approved platforms only; classify data properly; avoid unauthorized USB drives
4. **Physical Security:** Use laptop lock cables; never leave devices in vehicles; shred confidential documents
5. **Incident Response:** Immediately report lost/stolen devices and security incidents to IT Help Desk
6. **Compliance:** Complete mandatory annual cybersecurity training

13. Explain the various measures for protection of laptops through physical measures and logical access control measures, prepare a laptop security check list that should be followed by an individual.

- **Physical Security Measures:**
    - Use security cables and locks (e.g., Kensington locks) to tether the laptop to a fixed object.
    - Use polycarbonate laptop safes for transport and storage.
    - Install motion sensors and alarms that trigger if the laptop is moved.
    - Apply warning labels and stamps with tracking information to deter theft.
    - Engrave the laptop with personal or company identification details.
- **Logical Access Control Measures:**

    - Use strong, unique passwords and enable full-disk encryption.
    - Install and regularly update antivirus and personal firewall software.
    - Regularly install security patches and updates for the OS and software.
    - Lock down unused ports and disable unnecessary services like IR and wireless when not needed.
    - Use an Intrusion Detection System (IDS) to monitor for unauthorized access.
- **Laptop Security Checklist for an Individual:**
    - Is the laptop secured with a strong password?
    - Is the hard drive encrypted?
    - Is antivirus software installed and up-to-date?
    - Are all OS and software security patches applied?
    - Is the laptop physically locked with a security cable when unattended?
    - Is a firewall enabled?
    - Is sensitive data backed up securely?
    - Are Bluetooth and Wi-Fi disabled when not in use?

14. Explain registry settings for mobile devices using suitable examples.

- Registry settings are a centralized database that stores configuration settings and options for the operating system and applications.
- On mobile devices, these settings control how the OS and apps behave, including security policies.
- **Example:** Microsoft ActiveSync uses registry settings to govern synchronization rules between a Windows Mobile device and a desktop PC or Exchange Server.
- These settings can enforce policies like requiring a device password, specifying which applications can be installed, or controlling how data is transferred.
- Incorrect or maliciously altered registry settings can create security loopholes, allowing unauthorized data flow or weakening the device's security posture.

- Therefore, managing and securing registry settings is crucial for maintaining the integrity and security of the mobile device.

15. Write a note on authentication service security.

- It ensures that only authorized devices and users can connect to a network or service.
- It involves **mutual authentication**, where both the device and the network (base station/web server) verify each other's identities.
- This prevents malicious code from impersonating a legitimate service provider to trick the user.
- It is crucial for defending against common wireless attacks like eavesdropping, session hijacking, and Man-in-the-Middle (MitM) attacks.
- Security measures supporting authentication include the use of **Wireless Application Protocol (WAP)**, **Virtual Private Networks (VPNs)**, and **MAC address filtering**.
- Strong authentication is a foundational element for securing both the mobile device and the network it connects to.

16. What are the common types of attacks on wireless mobile devices.

- **War Driving:** Attackers drive around to locate and exploit insecure wireless access points.
- **WEP/WPA Attack:** Exploiting weaknesses in the Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) security protocols to crack encryption keys.
- **Packet Sniffing:** Intercepting and analyzing data packets transmitted over a wireless network to capture sensitive information like emails and passwords.
- **Replay Attacks:** Intercepting and maliciously re-transmitting data to create a delay or gain unauthorized access.
- **RF Jamming:** Deliberately transmitting radio signals to create interference and disrupt wireless communications.
- **Device and OS Exploits:** Attacking vulnerabilities in the mobile device's operating system or firmware, which are often below the visibility of security software.

17. State the organisational policies for the use of mobile hand held devices.

- **Create a Specific Policy:** Develop a distinct mobile device policy or extend the existing acceptable use policy to cover mobile technology.
- **Standardize Devices and Tools:** Standardize the types of devices and security tools used to simplify management and strengthen security.
- **Implement Security Technologies:** Mandate the use of strong encryption, device passwords, and physical locks. Consider biometrics for authentication.
- **Centralize Management:** Maintain an inventory of all corporate and BYOD (Bring Your Own Device) mobile devices.
- **Establish Usage Frameworks:** Create clear guidelines for data syncing, use of firewalls/anti-malware, and the types of information allowed on devices.
- **Enforce Patching Procedures:** Integrate software patching with device syncing or centralized management systems.
- **Provide Training:** Conduct regular education and awareness training for all employees using mobile devices for work.

Unit 3

1. What are the different phases of an attack on a network, Explain with the help of illustrative diagram.

- **Reconnaissance:** The attacker gathers initial information about the target from public sources like websites to understand the network structure, domain names, and IP address ranges.
- **Network Probing (Scanning):** The attacker actively probes the network using tools like ping sweeps and port scanners to discover live hosts and identify services running on the target systems.
- **Gaining Access (Exploitation):** The attacker exploits vulnerabilities to cross the line into electronic crime, initially accessing a user account and then escalating privileges to gain administrator or "root" access.

- **Maintaining Access (Installing Backdoors):** After gaining access, the attacker installs backdoors and Trojan horses to ensure they can re-enter the system easily and maintain control, effectively "capturing" the network.
- **Data Exfiltration:** The attacker exploits their position to locate, access, and steal confidential and valuable data from the compromised network.
- **Covering Tracks:** The final phase involves the attacker removing evidence of their activities, such as clearing logs, to avoid detection and remain undetected within the system for as long as possible.

2. What is the difference between proxy server and anonymizer.

Feature	Proxy Server	Anonymizer
Primary Purpose	Acts as an intermediary for connections to improve security, performance (caching), or bypass restrictions.	Specifically designed to make a user's web activity untraceable and hide their identity.
Level of Anonymity	Can hide the user's IP address, but may still log activity and reveal it to the server or network owner.	Provides a higher degree of anonymity by hiding all identifying information (IP address, browser details, etc.).

Common Use Cases	Network security, content filtering, load balancing, caching web pages to speed up access.	Privacy protection, bypassing censorship, preventing tracking by websites.
Scope of Service	Can handle various types of traffic and protocols (FTP, HTTP, etc.).	Typically functions as a web proxy, primarily handling HTTP/HTTPS traffic for web browsing.
User Configuration	Often requires manual setup in the browser or operating system network settings.	Usually accessed by visiting a specific website that provides the anonymizing service.
Data Caching	Often caches frequently accessed web pages to improve speed and reduce bandwidth usage for all users.	Generally does not cache user data to enhance privacy and prevent storing personal information.
Visibility	The use of a proxy may be detectable by the destination server.	A good anonymizer is designed to be completely transparent and undetectable to the destination server.

3. What are the different ways of password cracking.

- **Dictionary Attack:** Uses a file containing a list of words from a dictionary, which are systematically tried as passwords.
- **Brute Force Attack:** Attempts every possible combination of letters, numbers, and special characters until the correct password is found.
- **Hybrid Attack:** Combines a dictionary attack with brute force by substituting numbers and symbols in dictionary words (e.g., "P@ssw0rd").
- **Rainbow Table Attack:** Uses precomputed tables of hash values to quickly reverse cryptographic hash functions and find passwords.
- **Social Engineering:** Manipulates individuals into revealing their passwords through deception, such as phishing emails or phone calls.

- **Shoulder Surfing:** Involves physically observing a person as they type their password on their keyboard or keypad.
- **Malware:** Uses keyloggers or other spyware to secretly record keystrokes and capture passwords as the user types them.

4. Give the categorization of password cracking methods and explain each one of them in brief.

- **Online Attacks:** Performed by interacting with the live system, such as a login portal. Attackers use automated scripts to try many passwords, but these are slower and can be blocked by account lockout policies.
- **Offline Attacks:** Occur when the attacker obtains the password file (e.g., the hash values) and works on cracking it on their own system. This method is much faster as it is not rate-limited by the target system.
- **Non-Electronic Attacks (Social Engineering):** Do not involve technical tools. These rely on human interaction and include methods like tricking a user into revealing their password or observing them type it (shoulder surfing).
- **Manual Cracking:** The attacker manually tries to log in using guessed passwords based on knowledge of the user's personal information.
- **Automated Cracking:** Uses software tools to automate the process of trying a vast number of passwords from a list or through brute force generation.
- **Rule-based Attack:** A more sophisticated form of attack where the cracking tool applies transformation rules (like adding numbers or reversing letters) to words in a dictionary.

5. List out the guidelines to ensure strong and safe passwords.

- Use a minimum of eight alphanumeric characters, including a mix of uppercase, lowercase, numbers, and symbols.
- Avoid using common words, phrases, or personal information like your name, birthdate, or pet's name.
- Use unique passwords for different accounts, especially for business email, personal email, and banking.

- Change your passwords regularly, ideally every 30 to 45 days, and do not reuse old passwords.
- Never share your passwords with friends, relatives, or colleagues.
- Avoid accessing sensitive accounts from public computers; if you do, change the password from a secure system soon after.
- Do not store passwords on your mobile phone, PDA, or in unsecured files.

6. What are key loggers, List out the different types of keyloggers and explain them in brief.

Definition: Keyloggers are tools, either hardware or software, that record every keystroke made on a keyboard, typically in a covert manner without the user's knowledge.

- **Software Keyloggers:** These are programs installed on a computer, often by Trojans or viruses. They reside between the OS and the keyboard, capturing all keystrokes, which are then saved to a file or sent to a remote attacker.
- **Hardware Keyloggers:** These are physical devices connected between the computer's keyboard and the USB port or embedded inside the keyboard. They store keystrokes in their internal memory, which the attacker must physically retrieve.
- **Kernel-Based Keyloggers:** A type of software keylogger that operates at the kernel level of the OS, making them very difficult to detect as they are disguised as device drivers.
- **API-Based Keyloggers:** These software keyloggers hook into the Windows API to intercept keystroke messages as they are passed between the application and the operating system.
- **Acoustic Keyloggers:** Analyze the sound signatures of keystrokes to determine which keys were pressed, though this is a less common method.

7. Write a note on anti-keyloggers.

- **Purpose:** Anti-keyloggers are specialized software designed to detect, block, and remove keylogging programs from a computer system.
- **Detection Capability:** They can identify keyloggers that traditional firewalls and antivirus software might miss, as they specifically look for behaviors and signatures associated with keystroke capturing.

- **Proactive Protection:** Many anti-keyloggers use behavioral analysis to monitor for suspicious activity, such as a program attempting to hook keyboard APIs, and block it in real-time.
- **Prevention of Fraud:** They are crucial for preventing Internet banking fraud and identity theft by ensuring that passwords and other sensitive data typed on the keyboard are not captured.
- **Virtual Keyboards:** Most anti-keylogger tools include an on-screen virtual keyboard feature, allowing users to enter passwords by clicking with a mouse, thus bypassing physical keyloggers.
- **Low Maintenance:** Some anti-keyloggers do not require frequent signature updates like traditional antivirus software, as they focus on the method of operation rather than specific virus definitions.

8. How can key-loggers be used to commit crimes.

- **Identity Theft:** By capturing usernames, passwords, and social security numbers, keyloggers enable criminals to assume someone's identity for fraudulent activities.
- **Financial Fraud:** Keyloggers can steal online banking credentials and credit card information, allowing criminals to make unauthorized transactions and drain victims' accounts.
- **Corporate Espionage:** Installed on corporate systems, keyloggers can capture confidential business information, trade secrets, and intellectual property.
- **Extortion and Blackmail:** Captured keystrokes from private chats, emails, or login details to sensitive accounts can be used to blackmail individuals.
- **Unauthorized Access to Systems:** By obtaining administrator passwords, attackers can gain full control over systems and networks to launch further attacks.
- **Theft of Virtual Assets:** Keyloggers can steal login information for online gaming or cryptocurrency wallets, leading to the theft of virtual goods and currencies.

9. Define the following:

a. **Spyware:** Malicious software that is secretly installed on a computer to collect information about users without their knowledge, often tracking browsing habits and

personal data.

b. **Viruses and Worms:** Viruses are malicious code that infects legitimate programs and requires user action to spread, while worms are self-replicating programs that spread automatically across networks without user intervention.

c. **Trojan Horse:** A type of malware that disguises itself as a legitimate or useful software but, once executed, performs malicious functions, such as creating a backdoor.

d. **Rootkits:** A set of software tools that enable an attacker to maintain hidden access to a computer system while actively hiding its presence from users and security programs.

e. **Backdoors:** A method of bypassing normal authentication in a computer system, allowing remote access to the attacker while remaining undetected.

f. **Botnets:** A network of private computers infected with malicious software and controlled as a group without the owners' knowledge, often used to launch DDoS attacks or send spam.

10. What is a malware. List out different types of malwares and explain each one of them in brief.

Definition: Malware, short for malicious software, is any software intentionally designed to cause damage to a computer, server, client, or computer network.

- **Viruses:** Programs that attach themselves to clean files and spread throughout a computer, infecting other files and often corrupting data or disrupting system operations.
- **Worms:** Standalone malware that replicates itself to spread to other computers, often over a network, consuming bandwidth and potentially carrying a payload.
- **Trojan Horses:** Deceptive software that appears to perform a desirable function but instead facilitates unauthorized access to the user's computer system.
- **Spyware:** Software that gathers information about a person or organization without their knowledge and sends it to another entity.
- **Rootkits:** A collection of programs that enable administrator-level access to a computer while concealing its presence, making it extremely difficult to detect and remove.

- **Ransomware:** A type of malware that locks or encrypts the victim's files and demands a ransom payment to restore access.

11. State the difference between a virus and a worm.

Feature	Virus	Worm
1. Definition	A malicious program that attaches itself to a legitimate host file or program and requires user action to spread.	A standalone malicious program that can self-replicate and spread independently without a host file.
2. Spread Mechanism	Requires a host program and user intervention to execute (e.g., a user opening an infected file).	Spreads automatically by exploiting network vulnerabilities and security weaknesses, without any user action.
3. Replication	Replicates by inserting its code into other files and programs on the same system.	Self-replicates and actively sends copies of itself to other systems over a network.
4. Speed of Spread	Generally slower, as its spread is dependent on user activity and file sharing.	Very fast, as it can automatically propagate across networks, potentially infecting millions of systems quickly.
5. Primary Target	Primarily infects files and software on the local system (e.g., .exe, .com, boot sector).	Primarily targets network resources and other systems, consuming bandwidth and overloading servers.
6. Visibility & Focus	Often tries to hide within other files to avoid detection. Its main focus is infecting local resources.	Is an independent file. Its main focus is rapid propagation and network consumption, though it can also carry a payload.

12. What is a virus. State different actions that can be executed by a virus and explain how a virus can spread through internet and through stand-alone systems.

- **Definition:** A computer virus is a program that can 'infect' other legitimate programs by modifying them to include a copy of itself, often with malicious intent.

- **Actions:** A virus can display annoying messages, delete or corrupt files, scramble data on a hard disk, cause erratic screen behavior, halt the system, or simply replicate to cause further harm.
- **Spreading via Internet:** Viruses spread through the internet via email attachments, downloaded files from malicious or compromised websites, and through instant messaging links.
- **Spreading via Stand-alone Systems:** On stand-alone systems, viruses spread through infected removable media like USB drives, CDs, or DVDs. An infected disk introduced to a clean system will infect its hard drive, and any clean disk used on that infected system will, in turn, become infected.
- **Network Propagation:** On networked systems, a virus can infect files on a network drive, which are then accessed and executed by other users on the network, spreading the infection.
- **Social Engineering:** Viruses often rely on social engineering to trick users into executing them, such as by masquerading as a legitimate software update or a interesting file.

13. List out different types of viruses and explain them in brief.

- **Boot Sector Virus:** Infects the master boot record of storage devices, making it active every time the computer starts up.
- **Program/File Virus:** Attaches itself to executable files (like .exe or .com) and becomes active when the infected program is run.
- **Multipartite Virus:** A hybrid virus that can infect both boot sectors and program files, making it more persistent and difficult to remove.
- **Stealth Virus:** Uses various techniques to hide itself from detection by antivirus software, such as altering file sizes or redirecting disk reads.
- **Polymorphic Virus:** Changes its code (virus signature) each time it infects a new file, making it difficult for signature-based antivirus to detect.
- **Macro Virus:** Written in a macro language and embedded in documents (like Microsoft Word or Excel), infecting the system when the document is opened.

14. What is virus hoax.

- A virus hoax is a false warning about a non-existent computer virus, typically spread through email or social media.
- It often urges recipients to forward the message to everyone they know, causing unnecessary panic and wasted time.
- Hoaxes may describe a terrifying but fake virus with extreme destructive capabilities.
- They sometimes instruct users to delete critical system files, mistakenly claiming they are viruses, which can damage the operating system.
- The primary goal is deception and creating disruption, not actual system infection.
- Reputable sources like antivirus vendor websites should be checked to verify the legitimacy of any virus warning.

15. State the difference between trojan horse and backdoors.

Feature	Trojan Horse	Backdoor
1. Primary Nature	A type of malware that disguises itself as legitimate or useful software to trick users into installing it.	A method or vulnerability that bypasses normal authentication to provide hidden access to a system.
2. Main Function	To deceive the user and perform malicious actions, such as stealing data, deleting files, or spying.	To create a secret channel for remote, unauthorized access, allowing an attacker to control the system.
3. Method of Spread	Relies on social engineering and user deception (e.g., downloading a fake program). It does not self-replicate.	Often installed by other malware (like a Trojan) or by an attacker exploiting a vulnerability. It does not spread by itself.
4. Relationship	Often acts as the **delivery mechanism** or the **carrier** for a backdoor.	Is the **payload** or the **functionality** provided by a Trojan or other malware.

5. Visibility to User	Has a visible, often benign-looking, interface or function to appear legitimate and avoid suspicion.	Designed to be completely invisible and hidden from the user, operating silently in the background.
6. Key Threat	The deception and the variety of its malicious payload (which can include data theft, system damage, etc.).	The persistent, remote, and unauthorized access it grants to an attacker, compromising system integrity.

16. What are the functionalities of a backdoor.

- Allows an attacker to execute arbitrary commands on the compromised system.
- Enables file manipulation, including creating, deleting, renaming, copying, or editing any file.
- Provides the ability to install additional malicious software or parasites onto the system.
- Can log user activity, capture keystrokes, and take screenshots to steal sensitive information.
- Allows the attacker to control hardware devices, change system settings, and shutdown or restart the computer without user permission.
- Facilitates the exfiltration of gathered data by sending it to a predefined email address or uploading it to a remote server.

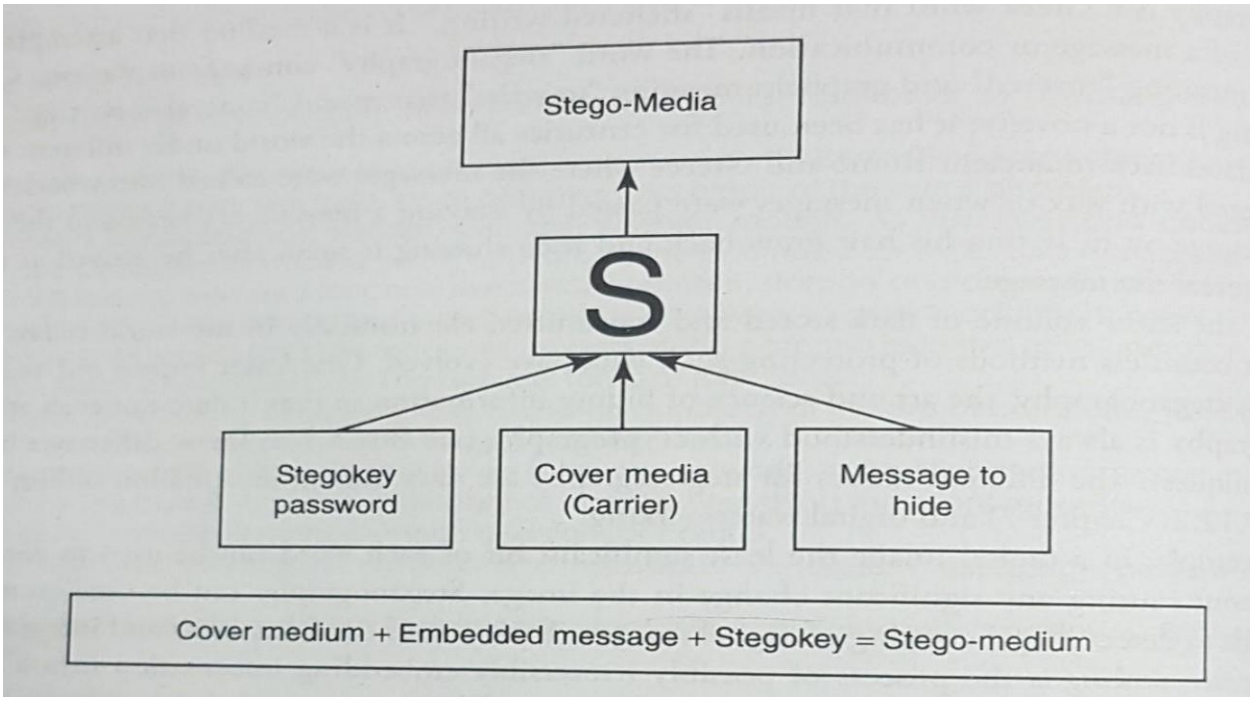
17. What is the difference between steganography and cryptography.

Feature	Steganography	Cryptography
1. Primary Goal	To hide the very **existence** of the message or communication.	To hide the **content** or meaning of the message, making it unreadable.
2. Method	Conceals a secret message within an innocent-looking cover file (e.g., image, audio, video).	Transforms a plaintext message into an unreadable ciphertext using algorithms and keys.

3. Output	A **stego-file** (e.g., stego-image) that looks and functions almost identically to the original file.	**Ciphertext**, which is a scrambled and obviously encrypted version of the original message.
4. Focus	**Secrecy through obscurity**; the communication does not attract attention.	**Security through mathematical complexity**; the communication is visible but protected.
5. If Discovered	If the stego-file is discovered, the secret message may still be safe if it was also encrypted.	If the ciphertext is discovered, it is clear that a secret message is being sent, inviting attack.
6. User Awareness	The recipient and sender know a message is hidden, but a third party is unaware of any communication.	Anyone who sees the ciphertext is aware that a secret message is being transmitted.

18. Explain how steganography works with the help of illustrative diagram.

- **The Process:** Steganography works by embedding a secret message within a harmless-looking cover medium (like an image or audio file).
- **The Carrier:** A cover file (e.g., a digital image) is selected. This file will carry the hidden message.
- **The Secret:** The confidential message that needs to be hidden is prepared. It is often encrypted first for additional security.
- **The Key:** A stegokey (password) may be used to control the embedding process, so only someone with the key can extract the message.
- **Embedding:** Using a steganography tool, the secret message is embedded into the cover file by altering the insignificant bits of the carrier file (e.g., the least significant bits of an image's pixels).
- **The Result:** The output is a stego-medium, which looks and functions almost identically to the original cover file but contains the hidden message. This stego-file is then sent to the recipient.



19. Define steg analysis.

- Steganalysis is the art and science of detecting messages hidden using steganography.
- It is the counter-technique to steganography.
- The primary goal is to identify suspected files and determine whether they contain a hidden payload.
- If a hidden message is detected, steganalysis may also attempt to extract or destroy it.
- It uses statistical analysis to find subtle distortions or patterns in the carrier file that are inconsistent with normal files.
- Automated tools are often used to scan and analyze large numbers of image, audio, and video files for signs of hidden data.

20. Are counter measures employed against steganography. Explain.

Yes, countermeasures exist, primarily in the form of steganalysis tools that scan files for statistical anomalies indicating hidden data.

- **Traffic Monitoring:** Monitoring network traffic for the transfer of file types commonly used in steganography (like high-quality images) from sensitive areas.
- **File Size and Hashing:** Comparing file sizes and checksums against known, clean originals; a larger-than-expected file size can be a red flag.
- **Deep Packet Inspection (DPI):** Using advanced firewalls and intrusion detection systems that can perform DPI to analyze the content of network packets for steganographic signatures.
- **Policy and Training:** Implementing organizational policies that restrict the uploading or downloading of certain file types and training employees to be aware of the risks.
- **Quarantine and Analysis:** Suspicious files can be quarantined and subjected to detailed steganalysis before being allowed into a secure network.

21. What are the different types of DoS attacks, explain them in brief.

- **Flood Attack (e.g., Ping Flood):** Overwhelms the target with a high volume of traffic, such as ICMP echo requests (pings), consuming its bandwidth.
- **Ping of Death:** Sends malformed or oversized ping packets to crash or freeze the target system due to improper handling of the packets.
- **SYN Flood:** Exploits the TCP three-way handshake by sending a flood of SYN requests but never completing the handshake, exhausting the server's connection resources.
- **Teardrop Attack:** Sends fragmented IP packets with overlapping offsets that the target system cannot reassemble properly, causing it to crash.
- **Smurf Attack:** Sends spoofed ping packets to a network's broadcast address, causing all devices on the network to reply to the victim, amplifying the attack traffic.
- **Application Layer Attack:** Targets specific applications (like web servers) with seemingly legitimate but resource-intensive requests, exhausting the application's capacity.

22. Give the types or levels of DoS attack.

- **Bandwidth Attacks:** Aim to consume all the available network bandwidth of the target, making it unavailable for legitimate traffic.

- **Protocol Attacks:** Exploit weaknesses in network protocols (like TCP/IP) to consume resources on the target server or intermediate communication equipment (e.g., firewalls).
- **Logic Attacks (or Application Layer Attacks):** Target the application layer by sending malicious requests that consume excessive resources (CPU, memory) of a specific application or service.
- **Flood Attacks:** A general category where the attacker simply floods the target with a massive volume of packets to saturate its resources.
- **Fragmentation Attacks:** A type of protocol attack that sends invalid or overlapping fragments that the target cannot reassemble, causing crashes (e.g., Teardrop).
- **Amplification Attacks:** A technique where the attacker uses a small amount of bandwidth to trigger a large amount of traffic to be sent to the victim (e.g., Smurf attack).

23. List down the tools used to launch DoS attack.

- **Jolt2:** A tool that causes a DoS on Windows machines by sending a stream of illegal fragmented packets, consuming 100% of the CPU.
- **Nemesy:** Generates random packets with spoofed source IP addresses to flood a target network.
- **Targa:** A program that can launch eight different DoS attacks, allowing the attacker to try multiple methods until one is successful.
- **Crazy Pinger:** A simple tool used to send large volumes of ICMP packets to a remote target.
- **SomeTrouble:** A remote flooder and mail bomber used to overwhelm targets with data or spam.
- **Trinoo/TFN/Stacheldraht:** These are DDoS tools used to coordinate attacks from multiple compromised systems (a botnet) to launch floods like SYN, UDP, and ICMP.

24. Explain and state the difference between DoS and DDoS.

Feature	Denial-of-Service (DoS) Attack	Distributed Denial-of-Service (DDoS) Attack
Definition	An attack that floods a target system with traffic from a **single machine** to make it unavailable.	An attack that floods a target system with traffic from **multiple, geographically distributed machines** (a botnet).
Source of Attack	Originates from **one** malicious system with one IP address.	Originates from **hundreds or thousands** of compromised systems (zombies) with different IP addresses.
Complexity & Control	Simpler to execute, as it involves only one attacking machine and requires less technical skill to launch.	More complex, as it requires building, controlling, and synchronizing a network of zombie systems (a botnet) using handlers.
Traffic Volume	Generally has **lower volume**, limited by the bandwidth and resources of the single attacking machine.	Generates an **extremely high, overwhelming volume** of traffic due to the combined power of many machines, making it more powerful.
Traceability	**Easier to trace and block** because the attack comes from a single source IP address.	**Very difficult to trace** the real attacker and block, as the traffic is distributed and comes from many legitimate-but-compromised IPs.
Mitigation Difficulty	Relatively easier to mitigate by simply identifying and blocking the single malicious IP address.	Much harder to mitigate, as it requires advanced filtering to distinguish malicious traffic from thousands of IPs without blocking legitimate users.
Attack Speed & Onset	The attack can be launched quickly but may also be stopped quickly.	The attack can escalate to maximum intensity almost instantly due to the pre-positioned botnet.
Impact & Severity	Typically affects smaller targets; easier for robust networks to absorb and defend against.	Capable of taking down major corporate and government infrastructure due to the massive scale of the attack.

Resource Exhaustion	Primarily consumes the target's resources (e.g., bandwidth, CPU).	Consumes the target's resources and also the resources of the intermediary network infrastructure (e.g., routers, firewalls).
Attack Architecture	Simple, single-tier architecture: **Attacker → Target**.	Complex, multi-tier architecture: **Attacker → Handlers → Zombies/Botnet → Target**.

25. Explain how to protect the network from DoS and DDoS attack.

- **Implement Router Filters:** Use ingress and egress filtering on routers to block spoofed IP packets.
- **Install Patches:** Apply security patches to protect against known vulnerabilities that can be exploited for DoS, such as TCP SYN flooding.
- **Disable Unused Services:** Reduce the attack surface by turning off any network services that are not essential.
- **Use DoS Protection Solutions:** Employ dedicated anti-DDoS hardware or cloud-based mitigation services that can absorb and filter attack traffic.
- **Enable Quota Systems:** Use OS-level quota systems to limit resource consumption by any single process or user.
- **Network Monitoring:** Continuously monitor network performance to establish a baseline and quickly identify unusual traffic patterns indicative of an attack.

26. What is SQL Injection and what are the different countermeasures to prevent this attack.

Definition: SQL Injection is a code injection technique that exploits vulnerabilities in a web application's database layer, allowing attackers to execute malicious SQL statements.

- **Input Validation/Sanitization:** Check and clean all user inputs to remove or escape potentially malicious characters like single quotes and SQL commands (e.g., SELECT, INSERT).
- **Use Prepared Statements (Parameterized Queries):** This method ensures that user input is treated strictly as data and never as executable SQL code, separating the SQL logic from the data.

- **Stored Procedures:** Use stored procedures in the database, which can also help to encapsulate the SQL logic and define parameters safely.
- **Least Privilege Principle:** Configure the database user account for the web application with the minimum privileges necessary, not as a database administrator.
- **Custom Error Messages:** Avoid displaying detailed database error messages to users, as they can provide clues to attackers. Use generic error messages instead.

27. Write down the steps for SQL Injection attack.

- **Reconnaissance:** The attacker identifies a potential target, such as a login page, search field, or any page that submits data to a database.
- **Probe for Vulnerabilities:** The attacker tests the input fields by entering special characters like a single quote (') to see if it generates a database error, indicating a potential vulnerability.
- **Check Source Code:** The attacker may view the HTML source code to find form fields and parameters (POST or GET) that interact with the database.
- **Craft the Injection:** Based on the error, the attacker crafts an SQL injection string, such as ' OR '1'='1'--, to manipulate the original SQL query.
- **Exploit the Vulnerability:** The attacker injects the malicious string into the input field to bypass authentication, extract data (using UNION SELECT), or modify the database.
- **Extract Data:** If successful, the attacker can retrieve sensitive information like usernames, passwords, credit card numbers, or even gain administrative control of the database.

28. What do you mean by Blind SQL Injection.

- Blind SQL Injection is a type of SQL injection where the attacker does not receive a visible error message or direct output from the database.
- The vulnerable page may not display data, but it will behave differently based on the truth or falsity of an injected logical statement.
- Attackers ask the database a series of "true or false" questions to infer information piece by piece.

- For example, an attacker might ask, "Is the first letter of the database name 'A'?" based on the page's response time or a subtle change in behavior.
- This technique is much slower and more labor-intensive than classic SQL injection.
- Specialized automated tools are often used to speed up the process of data extraction in blind SQL injection attacks.

29. What is Buffer Overflow, give the types of Buffer Overflow attacks and explain how to minimize and prevent buffer overflow attack.

Definition: A software vulnerability where a program writes data beyond the allocated memory buffer, corrupting adjacent memory. This can crash the program or allow execution of malicious code.

Types of Buffer Overflow Attacks

Type	Description
Stack-Based	Overflows a buffer on the call stack, often overwriting the return address to hijack program flow.
Heap-Based	Overflows a buffer in the dynamically allocated heap memory, corrupting data structures.
Integer Overflow	Arithmetic operations create a value too large for its variable, leading to incorrect buffer size calculations.

Minimization and Prevention

Method	Description
Secure Coding	Use bounds checking and safe functions (strncpy instead of strcpy).
Compiler Protections	Enable stack canaries, Data Execution Prevention (DEP), and Address Space Layout Randomization (ASLR).
Code Analysis	Use static/dynamic analysis tools and fuzz testing to find vulnerabilities.
Input Validation	Strictly validate and sanitize all user input to reject malicious data.

30. List down the different components of wireless networks and give the types of mobile workers in wireless networks.

- **Access Points (APs):** Hardware devices that connect wireless devices to a wired network and broadcast the wireless signal.
- **Wireless Network Interface Cards (NICs):** Hardware in devices like laptops and PDAs that allows them to connect to the wireless network.
- **SSID (Service Set Identifier):** The unique name that identifies a wireless network.
- **Security Protocols (WEP, WPA, WPA2):** Encryption standards designed to secure wireless communications.
- **Tethered/Remote Worker:** An employee who works from a fixed remote location, like a home office.
- **Roaming User:** An employee who moves within a building or campus, connecting from different locations.
- **Nomad:** A user who works from semi-tethered environments, frequently using modems or different networks.
- **Road Warrior:** A highly mobile employee who spends little time in the office and connects from various external locations.

31. List down the tools for hacking wireless networks.

- **NetStumbler:** A Windows-based tool for detecting wireless networks and their SSIDs (war driving).
- **Kismet:** A powerful wireless network detector, sniffer, and intrusion detection system that can find hidden (non-broadcast) SSIDs.
- **Airsnort:** A tool used to recover encryption keys by passively monitoring transmissions and cracking WEP encryption.
- **CowPatty:** A brute-force tool used to crack WPA-PSK (Pre-Shared Key) passwords.
- **Wireshark:** A network protocol analyzer that can capture and analyze wireless traffic, including management frames.
- **Aircrack-ng:** A complete suite of tools to assess Wi-Fi network security, capable of cracking WEP and WPA keys.

32. What the different traditional approaches of attack on wireless networks.

- **Sniffing:** Using a wireless sniffer to passively capture network traffic, including SSIDs, MAC addresses, and data frames to crack encryption.
- **Spoofing (Evil Twin Attack):** Creating a rogue access point with the same SSID as a legitimate network to trick users into connecting.
- **MAC Address Spoofing:** Changing the MAC address of a wireless device to bypass MAC address filtering.
- **Denial-of-Service (DoS):** Flooding the wireless spectrum or an access point with deauthentication frames to disrupt service for legitimate users.
- **Man-in-the-Middle (MITM) Attack:** Intercepting communication between a wireless client and the access point to eavesdrop or alter the data.
- **Encryption Cracking:** Using tools like Aircrack-ng or CowPatty to break weak encryption protocols like WEP or weak WPA passwords.

33. Give the different counter measures to secure wireless networks.

- **Use Strong Encryption:** Always use WPA2 or WPA3 with a strong, complex passphrase. Avoid using WEP.
- **Change Default Settings:** Change the default SSID, administrator username, and password on the wireless router/access point.
- **Disable SSID Broadcast:** Prevent the network name from being broadcast to make it less visible to casual scanners.
- **Enable MAC Address Filtering:** Restrict network access to only pre-approved MAC addresses.
- **Position the Router Safely:** Place the access point in the center of the building to limit signal leakage to outside areas.
- **Keep Firmware Updated:** Regularly update the router's firmware to patch known security vulnerabilities.

34. Define the following:

a. Warwalking: The act of searching for wireless networks while moving **on foot**. It is the pedestrian equivalent of "wardriving," where individuals use handheld devices to detect and map Wi-Fi signals.

b. Warbiking: The act of searching for wireless networks while riding a **bicycle or motorcycle**. This method allows for covering a larger area than war walking while still maintaining a degree of stealth.

c. Warkitting: A combination of **wardriving and rootkitting**. An attacker sets up a malicious rogue access point that, when users connect to it, automatically installs a rootkit on their device to gain hidden, administrator-level control.

d. WAPKitting: An attack where external software **seizes control of a router's firmware**. This can be easily accomplished by exploiting open or weak administrative access to the Wireless Access Point (WAP).

e. WAPjacking: This attack is similar to DNS poisoning. It involves **changing the settings of a router's existing firmware**, such as the DNS server settings, to redirect users to malicious websites without their knowledge.

35. Explain the different ways in which identity theft can be performed.

- **Phishing:** Sending deceptive emails that trick recipients into revealing personal information on fake websites.
- **Dumpster Diving:** Searching through trash to find discarded documents containing personal information like bank statements or pre-approved credit offers.
- **Skimming:** Using a small device to steal credit/debit card numbers during legitimate transactions, often at ATMs or gas stations.
- **Hacking:** Gaining unauthorized access to computer systems or databases to steal large volumes of personal data.
- **Stealing Mail:** Taking mail from mailboxes to obtain bank statements, credit cards, or tax information.
- **Shoulder Surfing:** Observing a person as they enter their PIN at an ATM or type a password on their computer.

- **Pretexting:** Using a false pretext or fabricated story to obtain personal information from companies or individuals over the phone.

36. What are the different methods of phishing.

- **Deceptive Phishing (Dragnet):** The most common type, using bulk emails that impersonate legitimate companies to steal user credentials.
- **Spear Phishing:** Highly targeted phishing attacks aimed at specific individuals or organizations, using personalized information to appear more legitimate.
- **Whaling:** A type of spear phishing that specifically targets high-level executives like CEOs or CFOs.
- **Clone Phishing:** An attacker creates a nearly identical copy of a legitimate email the user has already received, but with malicious links or attachments.
- **Smishing/Vishing:** Phishing conducted via SMS (text messages) or voice calls (phone phishing).
- **Pharming:** Redirecting users from a legitimate website to a fraudulent one by poisoning the DNS (Domain Name System) cache.

37. Give the categorization of phishing techniques and explain each one of them in brief.

- **Dragnet:** A wide-net approach using spammed emails with falsified corporate IDs sent to a large group, relying on volume to find victims.
- **Rod-and-Reel:** A targeted approach where phishers identify specific victims in advance and convey false information (e.g., a fake sale) to prompt disclosure of data.
- **Lobsterpot:** Involves creating spoofed websites that mimic legitimate ones, targeting a specific class of victims who are likely to seek out that site.
- **Gillnet:** Relies less on social engineering and more on injecting malicious code into emails or websites to install Trojans or keyloggers on the victim's system.
- **URL Manipulation:** Using misleading or misspelled URLs in emails that direct users to fake websites.
- **Website Forgery:** Using JavaScript or other techniques to forge the browser's address bar, making a fake site appear to have a legitimate URL.

38. Explain the sanitizing proxy system algorithm used for web phishing attack. Explain it with the help of illustrative flow-chart.

- **Two-Level Filtering:** The SPS uses strict URL filtering and HTTP response sanitizing to block and clean malicious content.
- **Strict URL Filtering:** It first checks the URL against a blacklist of known phishing sites and blocks access if a match is found.
- **HTTP Response Sanitizing:** If the URL is not blocked, the SPS fetches the webpage and scans its content (HTML, scripts) for phishing indicators.
- **Content Removal:** It removes or neutralizes parts of the content that encourage users to enter personal information, such as fake login forms.
- **Flexible Rule Set:** The algorithm uses a set of rules that can be updated to adapt to new phishing techniques and evasion methods.
- **Robustness:** It is designed to be robust against both novice user mistakes and advanced evasion techniques used by phishers.

39. List down the different information that can an attacker can steal from an individual.

An attacker can steal the following Personally Identifiable Information (PII) to commit identity theft and fraud:

- Full Name
- National Identification Number (e.g., Social Security Number - SSN, Aadhaar Number)
- Telephone and Mobile Phone Numbers
- Driver's License Number
- Credit Card and Debit Card Numbers
- Digital Identity (e.g., Email Address, Online Account IDs and Passwords)
- Birth Date and Birthplace
- Biometric Data (e.g., Face, Fingerprints)
- Bank Account Details and financial records.

40. List down the different types of identity theft.

The different types of identity theft are:

- **Financial Identity Theft:** Using someone's identity to obtain credit, loans, goods, or services.
- **Criminal Identity Theft:** Pretending to be someone else when apprehended for a crime. This category also includes computer crimes, organized crime, drug trafficking, alien smuggling, and money laundering.
- **Identity Cloning:** Using another person's information to assume their identity in daily life.
- **Business/Commercial Identity Theft:** Using a business's name to obtain credit or commit fraud.
- **Medical Identity Theft:** Using someone's identity to obtain medical care, drugs, or to make false insurance claims.
- **Synthetic Identity Theft:** Combining real (e.g., SSN) and fake information to create a new, fictional identity.
- **Child Identity Theft:** Using a child's clean SSN and identity to commit fraud.

41. Give the categorization of techniques for performing identity theft.

Identity theft techniques can be broadly categorized into two main groups:

A. Human-Based (Non-Technical) Methods:

i. **Direct Access to Information:** Physically stealing documents from offices, homes, or bags.

ii. **Dumpster Diving:** Searching through trash to find discarded documents containing personal information.

iii. **Theft of Purse or Wallet:** Directly stealing a person's physical possessions containing IDs, cards, and documents.

iv. **Mail Theft and Rerouting:** Stealing mail from mailboxes to obtain bank statements, credit cards, or tax information.

v. **Shoulder Surfing:** Observing a person as they enter their PIN at an ATM or type a password on their computer.

vi. **Dishonest or Mistreated Employees:** Insiders with access to personal data stealing and misusing it.

vii. **Telemarketing and Fake Telephone Calls (Vishing):** Using the phone to trick individuals into revealing personal information.

B. Computer-Based (Technical) Techniques:

i. **Backup Theft:** Stealing physical backup tapes or hard drives containing large datasets.

ii. **Hacking and Unauthorized Access:** Gaining illicit access to computer systems or databases to steal personal information in bulk.

iii. **Phishing:** Sending deceptive emails that trick recipients into revealing personal information on fake websites.

iv. **Pharming:** Redirecting users from a legitimate website to a fraudulent one without their knowledge, often by poisoning the DNS.

v. **Hardware Theft:** Stealing laptops, smartphones, or other devices that contain personal data.