#CSES (23CP310T)

Name: Jatin Prajapati
Roll No: 21BCP452D
Semester: 6th
Division: 5th (G-10)

PANDIT DEENDAYAL ENERGY UNIVERSITY
COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

CHAPTER 1

- ## Cyber security introduction

  - "Cyber Security" is combination of two words "Cyber and Security"
  - Within the context of cybersecurity, "cyber" specifically refers to the digital realm, including online activities, electronic systems, and virtual spaces where data is stored, processed, and transmitted.
  - In the context of cybersecurity, "security" focuses on safeguarding digital assets, systems, and information from unauthorized access, manipulation, disruption, or destruction.
  - IEEE definetion: Cybersecurity is the practice of protecting computer systems, networks, programs, and data from digital threats, including unauthorized access, exploitation, and manipulation.

- ## What is virus?

  - A computer virus is a program that can copy itself and infect a computer without the permission or knowledge of the user.
  - A computer virus has 2 major Characteristics:
    a) The ability to replicate itself.
    b) The ability to attach itself to another computer file.

- ## Warning bells / Symptoms for virus

  - Frequent pop-up windows.
  - Mass emails being sent from your email account.
  - Frequent crashes.
  - Unusually slow computer performance.
  - Unknown programs that start up when you turn on your computer.
  - Unusual activities like password changes.

- ## Hacker and Hacking

  - HACKING is the gaining of access to a computer and viewing, copying, or creating data without the intention of destroying data or maliciously harming the computer.
  - A hacker is a person skilled in information technology who uses their technical knowledge to achieve a goal or overcome an obstacle within a computerized system by non-standard means.
  - Someone who utilizes their technical know-how of bugs or exploits to break into computer systems and access data which would otherwise be unavailable to them.

- ## Types of Hacker

  - There are three types of hacker:
  - White hat hacker: It involves performing a security evaluation and testing with complete knowledge of the network infrastructure.
  - Gray hat hacker: It involves performing a security evaluation and testing internally. It examines the extent of access by insiders within the network.
  - Black hat hacker: Testing with no prior knowledge of the network infrastructure or systems. It takes the longest amount of time and most effort.

- ## Types of Hacking

  - Website Hacking: Web hacking refers to the exploitation of applications via HTTP, which can be done by manipulating the application through its graphical web interface, tampering with the Uniform Resource Identifier (URI), or tampering with HTTP elements not contained in the URI.
  - Network Hacking: Network hacking generally involves gathering information about a domain using tools like Nmap, Wireshark, and Metasploit.
  - Password Hacking: Password hacking refers to the unauthorized access to a system, network, or account by obtaining or guessing someone else's password through various methods such as brute force attacks, dictionary attacks, phishing, social engineering, or exploiting vulnerabilities in authentication systems.
  - Social engineering attack: Social engineering attack is a type of cyberattack that involves manipulating individuals into divulging confidential information, performing actions, or compromising security protocols through psychological manipulation and deception. This can include techniques such as pretexting, phishing, baiting, tailgating, or impersonation to exploit human vulnerabilities and gain unauthorized access to systems, networks, or sensitive information.
  - Phishing: Phishing is a type of cyber-attack where attackers impersonate legitimate entities, such as banks, social media platforms, or government agencies, to trick individuals into divulging sensitive information such as login credentials, credit card numbers, or personal details. Phishing attacks typically occur via email, instant messaging, or fraudulent websites, and often employ tactics like urgency, fear, or curiosity to manipulate victims into clicking on malicious links, downloading malware-infected attachments, or providing confidential information.

- ## What is Malware?

  - Malware is intrusive software designed to damage and destroy computers and computer systems. It is a contraction for "malicious software."
  - Malware encompasses a wide range of harmful programs, including viruses, worms, trojans, ransomware, spyware, and adware.
  - While some malware variants focus on transmitting information about web browsing habits to third parties, others may aim to encrypt files for ransom, disrupt system operations, steal personal information, or compromise network security.
  - Each type of malware serves different purposes and can have varying impacts on affected systems.
  - It's essential to recognize the diverse functionalities and potential threats posed by different forms of malware to effectively protect against them.

- ## Internet governance

  - Internet governance involves the development and application by:
    - → Governments,
    - → the private sector, and
    - → civil society,

    In their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.
  - The Internet is a decentralized network of computers. No single entity, whether it be a company, government, or organization, controls the internet. However, to ensure its operation, certain rules must be established.
  - ARPANET is one of the components that eventually evolved to become the Internet.

- ## Self-regulation

  - Self-regulation functions effectively within groups with strong community ties, employing mechanisms such as peer pressure or exclusion.
  - Internet Service Providers (ISPs) attempt to self-regulate by enforcing standards of behavior for their customers.
  - However, self-regulation does not always succeed, especially in cases where things are expected to be managed automatically.

- Policy making

  - Promote the open, distributed, and interconnected nature of the Internet.
  - Ensure transparency and accountability.

- Challenges and constraints

  - Ransomware Evolution: Ransomware is a type of malware that locks the data on a victim's computer, demanding payment before unlocking the ransomed data.
  - Blockchain Revolution: A blockchain is a database that stores data in chained blocks, offering a secure and transparent method of recording transactions.
  - IoT Threats: IoT stands for Internet of Things, a system of interconnected physical devices accessible through the internet, posing various security threats due to their connectivity and vulnerability to cyberattacks.
  - AI Expansion: Artificial Intelligence (AI) is a field of computer science focused on creating intelligent machines capable of performing tasks and exhibiting behavior similar to humans. Activities related to artificial intelligence include speech recognition, learning, planning, problem-solving, and more.
  - Serverless Apps Vulnerability: Serverless architecture and apps are applications that rely on third-party cloud infrastructure or backend services, such as Google Cloud Functions or Amazon Web Services (AWS) Lambda. However, they may be vulnerable to security risks due to their reliance on external services and the potential for misconfigurations or vulnerabilities in the cloud infrastructure.

- Cyber warfare

  - Cyber Warfare is Internet-based conflict involving politically motivated attacks on information systems.
  - It also involves the actions by nation-states or international organizations to attack and damage another nation's computers and information systems in an attempt to achieve strategic goals.

- Cyber warfare types:

1. Espionage
2. Sabotage
3. DoS Attack (Denial of Service Attack)
4. Electrical Power Grid
5. Propaganda Attacks
6. Economic Disruption
7. Sunrise Attack

- Espionage: This involves gaining unauthorized access to confidential information or data with the intention of gathering intelligence or spying on individuals, organizations, or governments.
- Sabotage: Sabotage involves insiders intentionally causing harm or disruption within their organization, often due to personal reasons or financial incentives. These individuals exploit their knowledge of the organization's systems to carry out attacks, which can range from data breaches to physical damage. To prevent this, companies need strong security measures like access controls and employee training.
- DoS Attack (Denial of Service Attack): In a DoS attack, the attacker floods a target system or network with an overwhelming amount of traffic, requests, or data, causing it to become slow, unresponsive, or completely unavailable to legitimate users.
- Electrical Power Grid: This refers to the network of power generation, transmission, and distribution systems that supply electricity to homes, businesses, and infrastructure. Attacks on the electrical power grid can disrupt electricity supply, leading to widespread outages and affecting critical services and infrastructure.
- Propaganda Attacks: Propaganda attacks involve spreading false or misleading information, often through digital channels such as social media, websites, or online forums, with the aim of influencing public opinion, stirring up social unrest, or causing confusion and mistrust.
- Economic Disruption: Many modern economic systems rely on computers. Attackers can target the computer networks of economic institutions like stock markets, payment systems, and banks to steal money or prevent people from accessing their funds.
- Sunrise Attack: These cyber-attacks are akin to events like Pearl Harbor and 9/11 in the sense that they aim to deliver a significant and unexpected blow, catching the target off guard and exploiting vulnerabilities in their defenses. The goal is to cause widespread disruption and weaken the opponent's ability to defend against subsequent attacks.

- Cyber Crime

  - Cybercrime refers to criminal activities that involve the use of a computer and a network.
  - This can include using a computer to commit a crime or targeting a computer as the victim of a crime. Cybercrime poses threats to individuals' security and financial well-being, as it can lead to identity theft, financial fraud, data breaches, and other harmful consequences.

- Cyber crime case study **Air India**

  - On May 21, 2021, reports emerged indicating that Air India had fallen victim to a cyberattack. The attack resulted in the compromise of personal details belonging to approximately 4.5 million customers globally.
  - The compromised information included sensitive data such as passport details, credit card information, birth dates, names, and ticket details. This breach highlighted the significant security risks faced by organizations in the aviation industry and underscored the importance of robust cybersecurity measures to protect customer data from malicious actors.
  - The compromised servers by hackers were later secured by Air India.
  - Air India engaged external data security specialists to address the cyberattack.
  - The airline assured passengers that there was no conclusive evidence of any misuse of the compromised personal data.
  - As a precautionary measure, Air India urged passengers to immediately change their passwords to enhance personal security.

- Cyber-crime case study **Oswaal books**

  - A security researcher has claimed that vulnerabilities in the e-commerce domain of Indian bookseller Oswaal Books could have enabled attackers to seize control of the website.
  - The researcher claims to have gained control of the administrator account via SQL injection, subsequently achieving remote code execution (RCE) and bypassing one-time password (OTP) authentication. Additionally, the researcher uncovered a cross-site request forgery (CSRF) bug during their investigation.

- Cyber-crime classification

  - Against individual:
    a) EMAIL Spoofing: Email spoofing is a cyber-attack where a hacker sends an email that appears to come from a trusted source, but has actually been manipulated.
    b) Phishing: Phishing is a cybercrime where individuals are contacted via email, phone, or text by someone posing as a legitimate entity to trick them into sharing sensitive information like personal data, banking details, and passwords.
    c) Spamming: Spamming involves using messaging systems to send numerous unsolicited messages to a large audience, typically for commercial advertising, non-commercial proselytizing, or any other prohibited purpose. It can also involve repeatedly sending the same message to the same user.
    d) Password Sniffing: Password sniffing is an internet attack aimed at intercepting usernames and passwords from network traffic. This is often accomplished through man-in-the-middle attacks, where an attacker secretly intercepts and records data as it passes between two parties, allowing them to steal sensitive credentials.
  - Against property:
    a) Credit Card Fraud: Credit card fraud refers to the unauthorized use of a credit or debit card, or similar payment method such as ACH or EFT, to deceitfully obtain money or property. This can involve various fraudulent activities, including unauthorized transactions, identity theft, and counterfeit card usage.
    b) Intellectual Property: Intellectual property (IP) refers to creations of the mind, such as inventions, literary and artistic works, designs, symbols, names, and images used in commerce, which are protected by law.
    c) Internet Time Theft: Internet time theft refers to the unauthorized use of internet hours paid for by another person. This typically involves individuals or employees using internet services, such as accessing websites or online resources, without permission or beyond the allocated time, resulting in financial losses or unauthorized usage.
  - Against Organization:
    a) Unauthorized accessing of computer: Illegally entering a computer system or network without proper authorization.
    b) Virus Attacks: Introducing malicious software into a computer system to cause damage or compromise security.
    c) E-Mail bombing: Overwhelming a victim's email inbox with a large number of emails, disrupting email service.
    d) Trojan Horse: Malicious software disguised as legitimate programs to trick users into installing and executing them, often leading to unauthorized access or data theft.
    e) Software piracy: Illegally copying, distributing, or using software without proper permission from the copyright holder.

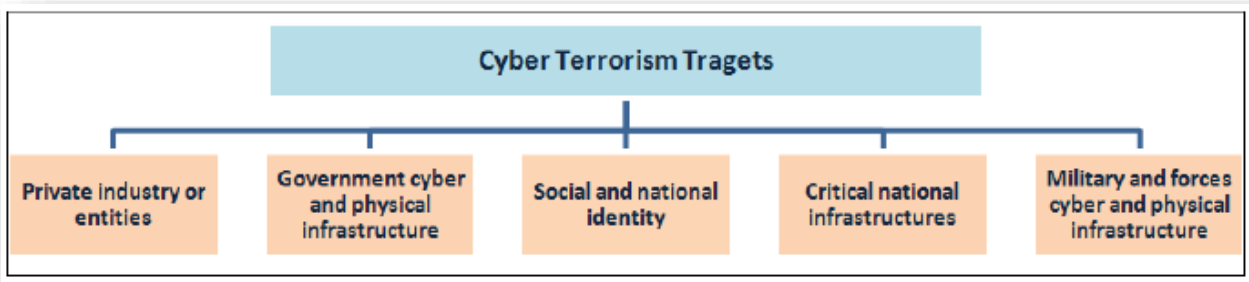
- Against Society:
    a) Forgery: Creating or altering documents, signatures, or other items with the intent to deceive or defraud.
    b) Cyber Terrorism: Using computer technology to conduct terrorist activities, such as hacking into systems, spreading malware, or disrupting critical infrastructure.
    c) Web Jacking: Unauthorized access to and control of a website, often for the purpose of defacement or to display unauthorized content.

- Indian ITA 2000

Section Ref & Title	Chapter of the Act & Title	Crime	Punishment
Section 43	Chapter IX: Penalty & Adjudication	Unauthorized Access to Computer Resource	Fine up to INR 1 crore; or Imprisonment up to 3 years; or both.
Section 66	Chapter XI: Offences	Computer-related Offences	Imprisonment up to 3 years; or Fine up to INR 5 lakh; or both.
Section 67	Chapter XI: Offences	Publishing or Transmitting Obscene Material	Imprisonment up to 3 years; or Fine up to INR 5 lakh; or both.
Section 68	Chapter XI: Offences	Unauthorized Alteration or Deletion of Data	Imprisonment up to 3 years; or Fine up to INR 2 lakh; or both.
Section 70	Chapter XI: Offences	Breach of Confidentiality and Privacy	Imprisonment up to 2 years; or Fine up to INR 1 lakh; or both.
Section 72	Chapter XI: Offences	Disclosure of Information in Breach of Contract	Imprisonment up to 2 years; or Fine up to INR 1 lakh; or both.
Section 73	Chapter XI: Offences	Publishing Digital Signature Certificate False in Certificates	Imprisonment up to 2 years; or Fine up to INR 1 lakh; or both.
Section 74	Chapter XI: Offences	Publication for Fraudulent Purpose	Imprisonment up to 2 years; or Fine up to INR 1 lakh; or both.

- Cyber terrorism

  - Cyberterrorism involves premeditated and politically motivated attacks targeting information, computer systems, programs, and data, resulting in violence against noncombatant targets or sub-national groups.
  - The prevalence of cybercrimes is often attributed to the lack of information security measures.
  - The Indian Information Technology Act (ITA) 2000 introduces a renewed focus on information security within India.
  - Targets: Targets of cyberterrorism may include critical infrastructure such as power plants, military installations, the banking industry, and air traffic control centers.



- Cyber terrorism challenges

  - Difficulty Identifying Attackers: Identifying the initiators of cyber-attacks remains challenging due to factors such as anonymity and sophisticated techniques used by attackers.
  - Lack of Boundaries: Cyber-attacks can originate from anywhere globally and from multiple locations simultaneously, making it challenging to attribute them to specific entities or geographic locations.
  - Speed of Development: The rapid development of new tools and techniques to exploit vulnerabilities shortens the time between vulnerability discovery and exploitation, posing significant challenges for cybersecurity defenses.
  - Low-Cost Tools: Cyber attackers utilize technology that is easy to access, inexpensive, and readily available, enabling them to execute attacks without significant financial investment.
  - Automated Methods: Cyber-attacks have become increasingly automated and sophisticated, allowing attackers to cause greater damage with minimal manual intervention, resulting in more significant impacts from individual attacks.

- Cyber terrorism forms

  - Privacy Violation: Breaching individuals' privacy by accessing or disclosing personal information without consent.
  - Secret Information Appropriation and Data Theft: Illegally obtaining and stealing sensitive data or proprietary information for unauthorized use or disclosure.
  - Demolition of E-Governance Base: Disrupting or dismantling electronic governance systems, hindering government operations, and undermining public services.
  - Distributed Denial of Service (DoS) Attack: Overwhelming a network or website with high volumes of traffic or requests, rendering it unavailable to legitimate users.
  - Network Damage and Disruptions: Causing harm to computer networks, infrastructure, or systems, leading to downtime, service disruptions, or loss of data.
  - Use of Cyber Communication for Terrorism: Exploiting digital platforms and communication channels for the planning, coordination, or execution of terrorist activities.

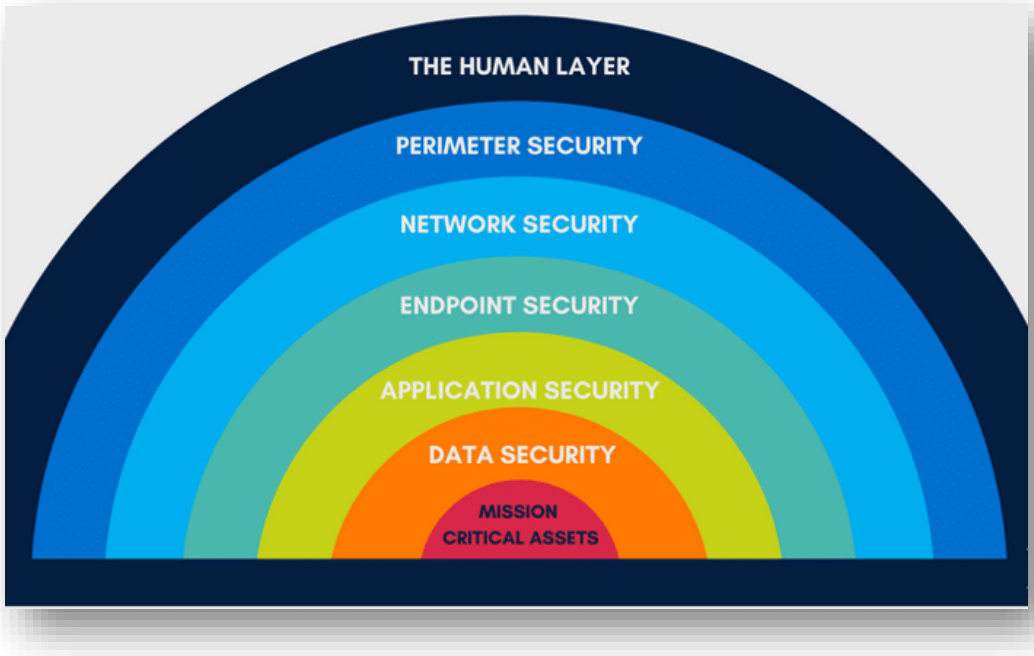
- Attack methods

  - Physical Attack: Attack against computer facilities or transmission lines, often employing conventional weapons to destroy or seriously damage computer systems and their infrastructure.
  - Electronic Attack: Utilizing the power of electromagnetic energy or electromagnetic pulse (EMP) to overload computer circuitry, disrupting or damaging electronic devices.
  - Cyber Attack: malicious code or software vulnerabilities to compromise computer systems, networks, or data, often with the intent of causing damage, theft, or disruption to operations.

- Types of malware / cyber terrorism tools

  - Virus
  - Worms
  - Trojan Horse
  - Logic Bombs
  - Trap Doors
  - DoS (Denial of Service)
  - Cryptography
  - Steganography

- 7 layers of cyber security



1. Mission Critical Assets - Data that requires protection due to its critical importance to the organization's operations or sensitive nature.
2. Data Security - Controls implemented to safeguard the storage and transmission of data, ensuring confidentiality, integrity, and availability.
3. Application Security - Measures to protect applications from unauthorized access, secure access to sensitive data within applications, and maintain the internal security of applications to prevent exploitation.
4. Endpoint Security - Security measures deployed to protect the connection points (endpoints) between devices (e.g., computers, mobile devices) and the network, safeguarding against threats such as malware, unauthorized access, and data breaches.
5. Network Security - Measures implemented to safeguard an organization's network infrastructure, preventing unauthorized access, detecting and responding to threats, and ensuring the confidentiality, integrity, and availability of network resources.
6. Perimeter Security - Comprehensive security measures, including physical and digital controls, deployed to protect the outer boundaries of an organization's network or premises, defending against unauthorized access, external threats, and potential breaches.
7. The Human Layer - Recognizing humans as potential vulnerabilities in cybersecurity, human security controls encompass strategies such as phishing simulations and access management measures to mitigate threats posed by cybercriminals, malicious insiders, and negligent users, thereby safeguarding mission critical assets.

- Terms related to cyber security

  - Inadvertent actions, typically by insiders, are unintentional or non-malicious actions that can still cause harm. Examples include accidental data leaks or clicking on harmful links.
  - Deliberate actions, by insiders or outsiders, are intentional and aimed at causing harm, such as hacking for theft or planting malware for disruption.
  - Inaction, typically by insiders, refers to a failure to act in a given situation. This may occur due to a lack of appropriate skills, knowledge, guidance, or the unavailability of the correct person to take action. It is of primary concern in cybersecurity
  - Political motivations encompass various actions, such as destroying, disrupting, or seizing control of targets; engaging in espionage; and making political statements, protests, or retaliatory actions.
  - Economic motivations involve various actions, such as theft of intellectual property or other economically valuable assets (e.g., funds, credit card information), fraud, industrial espionage, sabotage, and blackmail.
  - Socio-cultural motivations encompass a range of objectives, including attacks driven by philosophical, theological, political, and humanitarian goals. Additionally, socio-cultural motivations may involve actions driven by fun, curiosity, or a desire for publicity or ego gratification.

- Types of malware / attacks

  - Injection Attack:
    - → Injection attacks involve injecting malicious data into a web application.
    - → The aim is to manipulate the application's behavior to retrieve desired information.
    - → Examples include:
      - SQL Injection
      - Code Injection
      - Log Injection
      - XML Injection
    - → These attacks exploit vulnerabilities in the application.
    - → Prevention methods such as input validation are crucial to mitigate injection attacks.

  - DNS Spoofing:
    - → DNS Spoofing is a type of computer security hacking.
    - → It involves introducing false data into a DNS resolver's cache.
    - → This false data causes the name server to return an incorrect IP address.
    - → As a result, traffic is diverted to the attacker's computer or another specified destination.
    - → DNS spoofing attacks can persist for extended periods without detection.
    - → They pose serious security risks and can lead to various malicious activities.

  - Session Hijacking:
    - → Session hijacking is a security attack that targets user sessions over protected networks.
    - → Web applications utilize cookies to store user session information and state.
    - → By stealing these cookies, attackers can gain unauthorized access to the user's data and session.
    - → This breach of session integrity can lead to serious privacy and security concerns for the affected user.

- Phishing:
  - → Phishing is a type of attack aimed at stealing sensitive information such as user login credentials and credit card numbers.
  - → It occurs when an attacker impersonates a trustworthy entity in electronic communication.
  - → The attacker typically employs deceptive tactics, such as fake emails or websites, to trick victims into divulging their confidential information.
  - → Phishing attacks pose significant risks to individuals and organizations, leading to identity theft, financial loss, and compromised data security.

- Brute Force:
  - → Brute force is a type of attack that employs a trial and error method.
  - → This attack generates a large number of guesses and systematically validates them to obtain sensitive data such as user passwords and personal identification numbers.
  - → Criminals may use this attack to crack encrypted data, while security analysts may utilize it to assess an organization's network security.
  - → Brute force attacks can be resource-intensive and time-consuming, but they can potentially compromise systems with weak or easily guessable credentials.

- Denial of Service (DoS):
  - → Denial of Service is an attack intended to render a server or network resource unavailable to users.
  - → It achieves this by flooding the target with excessive traffic or sending information that triggers a crash.
  - → Typically, a DoS attack utilizes a single system and a single internet connection to overwhelm the targeted server.
  - → These attacks disrupt normal operations, causing inconvenience to users and potential financial losses for affected organizations.

- Dictionary Attacks:
  - → Dictionary attacks are a type of cyber attack that involves systematically trying all possible words or combinations of characters in an attempt to guess passwords or encryption keys.
  - → Unlike brute force attacks, which try all possible combinations of characters, dictionary attacks use precompiled lists of commonly used passwords, words from dictionaries, or variations thereof.
  - → These attacks are effective against weak passwords that are easily guessable, such as common words, phrases, or easily predictable patterns.
  - → Dictionary attacks are commonly used by cybercriminals to gain unauthorized access to accounts or sensitive information.
  - → To defend against dictionary attacks, it's crucial to use strong and unique passwords, employ multi-factor authentication, and regularly update security measures.

- URL Interpretation:
  - → URL interpretation is a type of attack where certain parts of a URL can be modified to manipulate the behavior of a web server.
  - → Attackers exploit vulnerabilities in URL handling mechanisms to access unauthorized web pages or resources.
  - → By altering parameters or path components within the URL, attackers can trick the server into delivering content that the user is not authorized to access.
  - → This attack can lead to unauthorized data disclosure, privilege escalation, or other security breaches.
  - → Proper input validation and access control mechanisms are essential to mitigate the risk of URL interpretation attacks.

- File Inclusion Attacks:
  - → File Inclusion Attacks are a type of cyber attack that enables an attacker to access unauthorized or critical files stored on a web server.
  - → This attack can also allow the execution of malicious files on the web server by exploiting the server's include functionality.
  - → Attackers typically exploit vulnerabilities in web applications that improperly handle user-supplied input to include files from the server's filesystem.
  - → By manipulating input parameters or exploiting insecure file inclusion methods, attackers can access sensitive files, such as configuration files or source code, and potentially execute arbitrary code on the server.
  - → Proper input validation, secure coding practices, and regular security audits are essential to mitigate the risk of file inclusion attacks.

- Man-in-the-Middle (MitM) Attacks:
  - → Man-in-the-Middle Attacks are a type of cyber attack where an attacker intercepts the communication between a client and a server and acts as an intermediary or "middleman."
  - → By inserting themselves into the communication flow, the attacker can eavesdrop on, alter, or inject data exchanged between the client and server without their knowledge.
  - → This attack can compromise the confidentiality, integrity, and authenticity of the communication, allowing the attacker to read, insert, or modify sensitive information.
  - → MitM attacks are commonly executed in insecure or unencrypted network environments, such as public Wi-Fi networks, where communication is not adequately protected.
  - → To mitigate the risk of MitM attacks, secure communication protocols like TLS/SSL should be used, and network security measures such as encryption and authentication should be implemented.

- Virus:
  - → A virus is a type of malicious software program that spreads throughout computer files without the user's knowledge.
  - → It is a self-replicating malicious computer program that propagates by inserting copies of itself into other computer programs when executed.
  - → In addition to replication, viruses can also execute instructions that cause harm to the infected system, such as deleting files, stealing information, or disrupting system functionality.
  - → Viruses can be spread through various means, including infected email attachments, compromised websites, or infected removable storage devices.
  - → To protect against viruses, users should regularly update their antivirus software, exercise caution when opening email attachments or downloading files from the internet, and maintain strong security practices.

- Worm:
  - → A worm is a type of malware with the primary function of replicating itself to spread to uninfected computers.
  - → Similar to computer viruses, worms propagate through self-replication, but unlike viruses, they do not need to attach themselves to existing files or programs.
  - → Worms can spread rapidly across networks and the internet by exploiting vulnerabilities in operating systems, network protocols, or software applications.
  - → They often originate from email attachments, malicious links, or compromised websites that trick users into executing or downloading the worm payload.

- Trojan Horse:
  - → A Trojan horse is a type of malicious program that disguises itself as a legitimate application or file to deceive users about its true purpose.
  - → Unlike viruses or worms, Trojans do not self-replicate but rely on social engineering tactics to trick users into executing them.
  - → Once executed, Trojans can perform various malicious activities, such as modifying computer settings, stealing sensitive information, or allowing remote access to the infected system.
  - → Trojans often exhibit unexpected changes to computer settings and unusual activity, even when the computer appears to be idle.
  - → They can masquerade as legitimate software, games, or utilities and may be distributed through email attachments, malicious websites, or software downloads.
  - → To protect against Trojans, users should exercise caution when downloading files from the internet, avoid clicking on suspicious links or email attachments, and use reputable antivirus software with real-time protection

- Backdoors:
  - → Backdoors are methods to bypass normal authentication.
  - → They're often created for legitimate purposes like troubleshooting.
  - → However, if exploited, they pose significant security risks.
  - → Proper security measures are crucial to detect and mitigate unauthorized access.

- Bots:
  - → Bots, short for "robots," are automated processes that interact with network services.
  - → They can operate autonomously or respond to specific input.
  - → Common examples include crawlers, chatroom bots, and malicious bots.

- Session Replay:
  - → In this type of attack, a hacker steals an authorized user's login information, typically by obtaining the session ID.
  - → With this stolen session ID, the intruder gains unauthorized access to the website and can perform any actions the legitimate user could.
  - → This attack allows the attacker to mimic the actions of the authorized user, potentially leading to unauthorized transactions, data breaches, or other malicious activities.

- Message Modification:
  - → In this attack, an intruder manipulates packet header addresses to redirect a message to a different destination or modify the data on a target machine.
  - → By altering the packet headers, the attacker can intercept and modify the content of the message, potentially leading to data corruption, unauthorized access, or other security breaches.

- Distributed Denial-of-Service (DDoS) Attack:
  - → In a DDoS exploit, large numbers of compromised systems (sometimes called a botnet or zombie army) alter packet header addresses to direct a barrage of messages to a single target or modify data on the target machine.
  - → By coordinating these compromised systems to flood the target with traffic, the attacker overwhelms its resources, causing service disruption or complete downtime.

- Eavesdropping (Tapping):
  - → In this attack, the attacker simply listens to messages exchanged between two entities.
  - → For the attack to be successful, the traffic must be unencrypted.
  - → Any unencrypted information, such as passwords sent in response to HTTP requests, can be intercepted and retrieved by the attacker.

- Traffic Analysis:
  - → In this attack, the attacker examines the metadata transmitted in traffic to deduce information about the communication and the entities involved.
  - → This includes analyzing factors such as the form of the exchanged traffic (rate, duration, etc.).
  - → When encrypted data is used, traffic analysis can lead to attacks by cryptanalysis, enabling the attacker to obtain information or successfully decrypt the traffic.

- Software Attacks:
  - → Malicious code, also known as malware, is a type of software designed to infiltrate or harm a computer user's operating system without their knowledge or consent.
  - → Malware can be challenging to detect and remove, and it can cause significant damage to the system and compromise the user's privacy and security.

- Policy and its type

- Need for Security Policies:
  - → Enhances efficiency.
  - → Upholds discipline and accountability.
  - → Critical for successful business deals.
  - → Educates employees on security literacy.

- Virus and Spyware Protection Policy:
  - → Detects threats in files and identifies applications exhibiting suspicious behavior.
  - → Removes and repairs the side effects of viruses and security risks using signatures.

- Firewall Policy:
  - → Blocks unauthorized users from accessing systems and networks connected to the Internet.
  - → Detects cybercriminal attacks and removes unwanted sources of network traffic.

- Intrusion Prevention Policy:
  - → Automatically detects and blocks network attacks and browser attacks.
  - → Protects applications from vulnerabilities.
  - → Checks the contents of data packets and detects malware attempting to infiltrate through legitimate means.

- Application and Device Control Policy:
  - → Protects a system's resources from applications.
  - → Manages peripheral devices that can connect to a system.
  - → Device control policy applies to both Windows and Mac computers, while application control policy applies only to Windows clients.