UNIT 4:

1. How Secure Electronic Transaction (SET) Protocol enhance the online payment security:
- SET makes online payments safer by using digital certificates to verify the identities of both the buyer and the seller.
- It encrypts the payment information during transmission, keeping it safe from hackers.
- SET also provides a secure way to handle credit card information without exposing it to potential theft.

2. Elaborate the working and types of Biometric authentication:
- Biometric authentication uses unique physical characteristics or behavioral traits to verify identity.
- Types include fingerprint recognition, facial recognition, iris recognition, voice recognition, and even DNA matching.
- The process involves capturing the biometric data, converting it into a digital format, and comparing it against stored templates to authenticate the user.

3. Outline the need of Transport layer security and explain the Secure Socket Layer (SSL) protocol:
- Transport Layer Security (TLS) ensures secure communication over a computer network.
- SSL is an earlier version of TLS and is used to encrypt data transmitted between a web server and a web browser.
- It prevents eavesdropping and tampering by encrypting the data during transmission, making it unreadable to anyone except the intended recipient.

4. Discover the role of intrusion detection system (IDS) to analyze the network traffic and how it helps strengthen security on the network:
- IDS monitors network traffic for suspicious activity or signs of intrusion.
- It analyzes patterns and behaviors to detect potential threats such as unauthorized access, malware, or denial-of-service attacks.
- IDS alerts administrators when it detects suspicious activity, allowing them to take action to prevent or mitigate security breaches.

5. Discussed the different Threats to Information Security:
- Threats to information security include malware such as viruses, worms, and Trojans that can infect computers and steal data.
- Phishing attacks trick users into revealing sensitive information such as passwords or credit card numbers.
- Denial-of-service (DoS) attacks overwhelm a system with traffic, making it inaccessible to legitimate users.
- Insider threats involve employees or other trusted individuals intentionally or unintentionally compromising security.
- Other threats include data breaches, identity theft, and social engineering tactics aimed at manipulating people into divulging confidential information.

Sure, let's break it down:

6. How Smart Cards are used in security along with its uses and types:
- Smart cards are like small computers that store data securely.
- They're used for things like access control, electronic payments, and identification.
- Types include contact smart cards (inserted into a card reader) and contactless smart cards (used by waving near a reader).

7. Explain the role of proxy servers in network security. How do they enhance privacy and security?
- Proxy servers act as intermediaries between users and the internet.
- They can hide users' IP addresses, making it harder for hackers to track them.
- Proxy servers can also filter web content, block malicious sites, and cache frequently accessed data to speed up browsing.

8. Explain the components of the IPsec protocol suite and its role in providing security at the network layer:
- IPsec includes protocols for encrypting and authenticating data at the network layer.
- Components include Authentication Header (AH) for authentication and Encapsulating Security Payload (ESP) for encryption.
- IPsec ensures that data sent over a network is secure from eavesdropping and tampering.

9. Explain the use of smart cards in enhancing security in various applications, including authentication and access control:
- Smart cards can be used for secure login to computers or networks, replacing passwords with more secure authentication methods.
- They're also used for physical access control, like swiping into buildings or secure areas.
- Smart cards enhance security by storing sensitive information securely and requiring physical possession for access.

10. Explain the Security in Wireless Communication and its protocols:
- Wireless communication security involves protecting data transmitted over wireless networks.
- Protocols like WPA2 and WPA3 encrypt data to prevent unauthorized access.
- Techniques like MAC filtering and disabling SSID broadcasting can also enhance wireless security.

11. Identify and discuss common threats in computer networks, including malware, phishing, and denial-of-service attacks:
- Malware includes viruses, worms, and Trojans that infect computers and steal data.
- Phishing involves tricking users into revealing sensitive information like passwords.
- Denial-of-service attacks overwhelm networks or servers, making them unavailable to legitimate users.
- These threats can lead to data breaches, financial loss, and disruption of services.

UNIT 5:

1. Email security is about keeping your emails safe from hackers and other prying eyes. It's useful because it helps protect your personal information and sensitive data from being accessed or stolen by unauthorized people.

2. PGP, or Pretty Good Privacy, is a system used to encrypt and decrypt email messages. It works by using a combination of public and private keys. The sender uses the recipient's public key to encrypt the message, and only the recipient's private key can decrypt it, ensuring only the intended recipient can read it. This is how PGP achieves end-to-end encryption, meaning the message is encrypted from the sender's end to the recipient's end, making it very secure.

3. PGP and S/MIME are both methods used to secure email communications, but they have some differences. PGP uses public-key cryptography and is more commonly used for personal emails and small-scale encryption. S/MIME, on the other hand, relies on certificates issued by a trusted authority and is often used in corporate environments or for large-scale email encryption.

4. HTTPS, or Hypertext Transfer Protocol Secure, plays a crucial role in securing web communication by encrypting data transmitted between a web browser and a website. It ensures confidentiality by encrypting the data using SSL/TLS protocols, making it unreadable to anyone who might intercept it while it's being transmitted over the internet. This helps protect sensitive information like passwords, credit card numbers, and personal details from being stolen by hackers.

5. Honeypots are like traps set up by cybersecurity professionals to detect and observe intruders or attackers. They work by mimicking vulnerable systems or networks, enticing attackers to interact with them. Once an attacker interacts with the honeypot, security professionals can monitor their behavior, study their tactics, and gather valuable information to improve overall cybersecurity defenses. Honeypots don't contain any real data or services, so any activity detected within them is likely malicious, making them valuable tools for detecting and analyzing cyber threats.

6. What are the types of IPSec protocol modes?
- IPSec has two main modes: Transport mode and Tunnel mode.
- Transport mode encrypts only the data payload of each packet, leaving the original IP header intact.
- Tunnel mode encrypts the entire IP packet and adds a new IP header, which encapsulates the original packet.

7. List the types of firewalls and explain the design principles of firewalls in network security.
- Types of firewalls include packet-filtering firewalls, stateful inspection firewalls, proxy firewalls, and next-generation firewalls.
- Design principles of firewalls involve creating a security perimeter around a network, controlling traffic based on predefined rules, and monitoring and logging network activity.

- Firewalls act as gatekeepers, inspecting incoming and outgoing traffic to block unauthorized access and prevent malicious activities.

8. Consider you are the owner of ABC Company and you are using network layer for security then how IPsec Protocol work for network.
- If ABC Company is using IPsec at the network layer, it means encrypting and authenticating data packets sent over the network.
- IPsec encrypts data at the IP layer, ensuring that only authorized parties can access the information.
- It also provides authentication to verify the identities of communicating parties and prevent data tampering during transmission.

9. Decide how S/MIME Work does for “end-to-end” encryption solution used for email messages.
- S/MIME (Secure/Multipurpose Internet Mail Extensions) is an email encryption standard.
- It uses digital certificates to encrypt and sign email messages, ensuring confidentiality and authenticity.
- S/MIME provides end-to-end encryption by encrypting the message contents and attachments at the sender's device and decrypting them at the recipient's device using their private key.

10. Justify the term with proper examples: Intruders, Honeypots, and Email security.
- Intruders are individuals or automated programs that attempt to gain unauthorized access to computer systems or networks.
- Honeypots are decoy systems designed to lure intruders and gather information about their tactics and techniques.
- Email security involves protecting email messages from unauthorized access and malicious attacks, such as phishing and malware attachments.

11. Construct the working, design, and types of firewalls.
- Firewalls monitor and control incoming and outgoing network traffic based on predefined security rules.
- Packet-filtering firewalls inspect individual packets and make decisions based on IP addresses, ports, and protocols.
- Stateful inspection firewalls track the state of active connections and make decisions based on the context of the traffic.
- Proxy firewalls act as intermediaries between clients and servers, inspecting and filtering traffic at the application layer.
- Next-generation firewalls combine traditional firewall functionalities with advanced features like intrusion prevention, application awareness, and deep packet inspection.

UNIT 6:

1. Buffer overflows happen when a program tries to put too much data into a limited space in its memory, called a buffer. This can cause the extra data to overflow into adjacent memory areas, potentially leading to crashes, security vulnerabilities, and even allowing attackers to take control of the software.

2. Attackers exploit buffer overflow vulnerabilities by sending more data than a program expects, causing it to overflow. By carefully crafting this extra data, attackers can overwrite important information in the program's memory, such as return addresses or function pointers, to redirect the program's execution flow to malicious code they control.

3. Buffer overflows are a big deal for software security because they can let attackers take control of a program or system. There are two main types: stack-based buffer overflows, where attackers overflow buffers located on the program's call stack, and heap-based buffer overflows, where attackers overflow buffers allocated in the program's heap memory.

4. Malicious code, or malware, is software designed to harm or infiltrate computer systems. There are different types, like viruses, which infect other programs and spread when those programs are run; worms, which can spread independently over networks; and Trojans, which disguise themselves as legitimate software but actually have malicious intent, like stealing data or giving attackers backdoor access to a system.

5. The goals of security controls are to protect systems and data from unauthorized access, alteration, or destruction. Administrative security controls are measures put in place by organizations to manage and enforce security policies and procedures. They include things like user authentication, access control, security training, and incident response planning, all aimed at keeping systems and data safe from threats.6. Trapdoors in computer security are secret ways to access a system or software that aren't meant to be there. Attackers can exploit trapdoors by finding or creating them, giving them unauthorized access to systems. They might use them to bypass security measures or steal sensitive information without being detected.

7. Cross-site scripting (XSS) is a type of security vulnerability found in web applications. It occurs when attackers inject malicious scripts into web pages viewed by other users. These scripts can then execute in the browsers of other users, potentially stealing information, hijacking sessions, or defacing websites.

8. Malicious code, or malware, is software designed to harm computer systems or steal data. There are different types: viruses infect other programs and spread when those programs are run; worms can spread independently over networks; and Trojans disguise themselves as legitimate software but have malicious intent, like stealing data or giving attackers backdoor access.

9. There are various types of security controls to protect systems and data. They include technical controls like encryption, firewalls, and antivirus software, which use technology to prevent and detect security threats. Administrative controls, such as policies, procedures, and training, are put in place by organizations to manage security. Physical controls, like locks and surveillance systems, protect physical assets from unauthorized access.

10. In computer security, a virus is a type of malware that infects other programs and spreads when those programs are run. Trapdoors are secret ways to access systems or software, often used by attackers to gain unauthorized access. Worms are malware that can spread independently over networks, infecting vulnerable systems. Each of these poses different threats to computer systems and data security.

11. Attackers exploit buffer overflow vulnerabilities by sending more data than a program expects. This extra data can overflow into adjacent memory areas, overwriting important information like return addresses. By doing this carefully, attackers can redirect the program's execution flow to malicious code they control, compromising the system.

12. Administrative controls are rules and procedures set up by organizations to manage security. They're crucial because they establish guidelines for things like user access, password policies, and incident response. By enforcing these controls, organizations can reduce the risk of security breaches and ensure everyone follows security best practices.

13. Non-malicious program errors are mistakes or bugs in software that aren't caused by malicious intent. They can include things like logic errors, syntax errors, or runtime errors. While they may not be intentionally harmful, these errors can still cause software to behave unexpectedly or crash, potentially leading to security vulnerabilities if not addressed properly.