

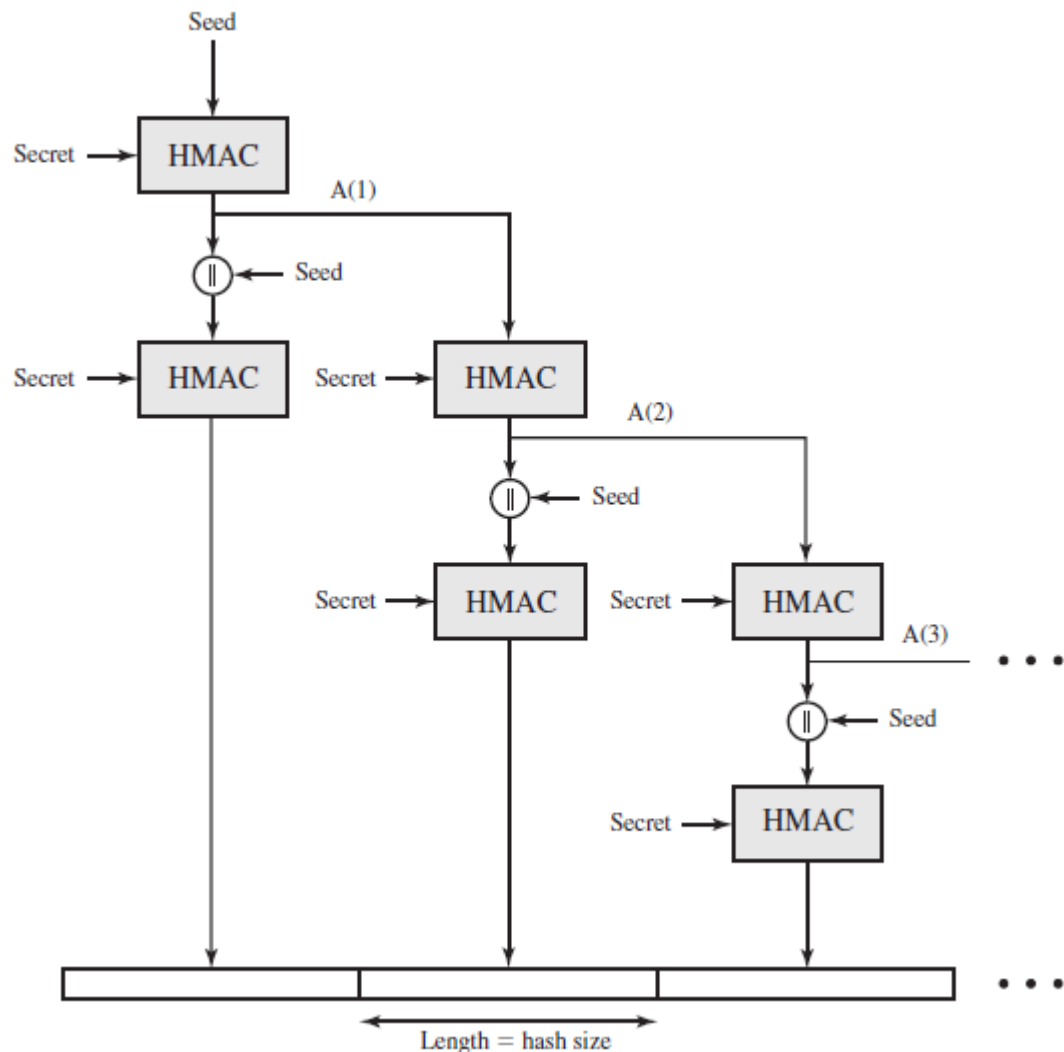
Q.No	Question & Solution
	Module-1
1.a	Discuss the four principles of security in detail. [10M]
Solution	<p>The four fundamental principles of security are:</p> <p>Confidentiality: Confidentiality refers to the protection of sensitive information from being accessed by unauthorized individuals. This ensures that only those who have the proper authorization can view or retrieve specific data. Confidentiality is maintained through encryption techniques</p> <p>Integrity: It ensures that information remains unaltered or uncorrupted during transmission or storage. This is achieved using cryptographic hashing, digital signatures, and checksums, which verify that no unauthorized changes have been made.</p> <p>Availability: It is the third principle that ensures that information and resources are accessible whenever needed by authorized users. Any disruption in system availability, whether due to cyber-attacks, hardware failures, or natural disasters, can result in a significant impact.</p> <p>Authentication: It plays a crucial role in verifying the identity of users, devices, or systems before granting access to sensitive information. Authentication prevents unauthorized access and ensures that only legitimate users can interact with a system.</p>
1.b	What are the two types of security attacks? Explain Passive attacks in detail along with classification.[10M]
Solution	<p>Security attacks are broadly categorized into two types: passive attacks and active attacks. Passive attacks involve monitoring and eavesdropping on communications without directly interfering with data transmission or modifying system resources, while active attacks involve direct modification, deletion, or disruption of data. Passive attacks are particularly challenging to detect because they do not alter the data or system functionality; instead, they focus on gathering confidential information without the knowledge of the communicating parties. Passive attacks can be classified into two main types: eavesdropping (interception attacks) and traffic analysis. Eavesdropping occurs when an attacker secretly listens to private communications over a network. This can be done through techniques such as wiretapping, network sniffing, or intercepting unencrypted data transmitted over the internet. Another form of passive attack is traffic analysis, where an attacker monitors the communication patterns between two or more parties. Even if the transmitted data is encrypted and remains unreadable, analyzing the frequency, volume, and timing of messages can provide valuable insights. In contrast, active attacks involve direct interaction with the system, where attackers modify, delete, or inject malicious data. Unlike passive attacks, active attacks can disrupt operations and are usually easier to detect.</p>
	OR
2.a	Write short Notes on Virus, Worms, and Cookies [8M]
Solution	<p>Virus: A virus is a type of malicious software that attaches itself to a legitimate program or file and spreads when the infected file is executed. Once activated, a virus can damage data, corrupt files, or even take control of system functions. It requires user intervention to spread from one system to another, often through email attachments, infected software, or removable storage devices.</p> <p>Worm: Unlike a virus, is a self-replicating malware that spreads automatically across networks without requiring user action. Worms exploit system vulnerabilities and propagate by sending copies of themselves through email or unsecured remote connections. They consume network bandwidth and overload systems, and sometimes supports to install backdoors or additional malware.</p> <p>Cookie: It is a small piece of data stored on a user's device by websites to enhance user experience and track online activities. While most cookies are harmless and used for legitimate purposes like remembering login details or personalizing web content, some tracking cookies can be used by third-party advertisers or attackers to collect sensitive user information.</p>

b.	What is packet spoofing? Mention its three possible cases. [6M]
Solution	<p>Packet Spoofing In this technique, an attacker sends packets with an incorrect source address. When this happens, the receiver (i.e. the party who receives these packets containing false addresses) would inadvertently send replies back to this forged address (called spoofed address), and not to the attacker.</p> <p>This can lead to three possible cases:</p> <p>(i) The attacker can intercept the reply If the attacker is between the destination and the forged source, the attacker can see the reply and use that information for hijacking attacks.</p> <p>(ii) The attacker need not see the reply If the attacker's intention was a Denial Of Service attack, the attacker need not bother about the reply.</p> <p>(iii) The attacker does not want the reply The attacker could simply be angry with the host, so it may put that host's address as the forged source address and send the packet to the destination. The attacker does not want a reply from the destination, as it wants the host with the forged address to receive it and get confused.</p>
c.	Explain Sniffing and Phishing Attacks [6M]
Solution	<p>Sniffing is a technique where an attacker captures and analyses network traffic to extract sensitive information. Clearly, to prevent an attacker from sniffing packets, the information that is passing needs to be protected in some ways. This can be done at two levels: (i) The data that is traveling can be encoded in some ways, or (ii) The transmission link itself can be encoded.</p> <p>Phishing: The attacker decides to create his/her own Web site, which looks very identical to a real Web site. The cloning is so clever that the human eye will not be able to distinguish between the real and fake site. The attacker sends an email to the legitimate customers of the bank. The email itself appears to have come from the bank. The customer is asked to visit a URL mentioned in the email. When the customer innocently clicks on the URL specified in the email, he is taken to the attacker's site and the customer is prompted to enter confidential information, such as password or PIN. Since the attacker's fake site looks exactly like the original bank site, the customer provides this information. The attacker now uses the victim's password or PIN to access the bank's real site and can perform any transaction.</p>
	Module-2
3.a	Explain the parameters that define the session state and connection state in the secure socket layer.[8M]
Solution	<p>An SSL session is an association between a client and a server established through a handshake protocol. A session defines a set of security parameters that can be used across multiple SSL connections.</p> <p>Key Parameters of Session State:</p> <p>Session Identifier: A unique ID assigned to the session, used to track and manage session.</p> <p>Peer Certificate: The certificate presented by the client or server to authenticate its identity.</p> <p>Compression Method: Specifies the algorithm used for data compression during transmission.</p> <p>Cipher Suite: Defines the encryption, hashing, and key exchange algorithms used to secure the communication.</p> <p>Master Secret: A 48-byte secret generated during the SSL handshake, used to derive cryptographic keys for encryption and authentication.</p> <p>Is Resumable Flag: Indicates whether the session can be resumed in the future, allowing the same security parameters to be used again without repeating the handshake process.</p> <p>An SSL connection is a secure link established between a client and a server for data transmission using the session's security parameters. It lasts after the communication session ends.</p> <p>Key Parameters of Connection State:</p> <p>Server and Client Random Values: These are random numbers generated during the handshake, used in key generation and session security.</p>

	<p>Encryption Keys: Symmetric encryption keys are derived from the master secret and used to encrypt data sent over the connection.</p> <p>Message Authentication Code (MAC) Keys: Used for integrity checks, ensuring that the data has not been altered during transmission.</p> <p>Sequence Numbers: Unique numbers assigned to messages in the session to prevent replay attacks and ensure message order.</p> <p>Compression State: Specifies the compression algorithm being used (if any) for secure data exchange.</p> <p>Read and Write States: Defines the encryption and integrity protection applied to incoming and outgoing data separately.</p>
b.	Mention the types of security threats faced when using the web. [08M]
Solution	<p>Types of Security Threats Faced When Using the Web:</p> <p>Integrity Threats: Integrity ensures that data remains unaltered and trustworthy. Threats to integrity involve unauthorized modifications of user data, programs, or system memory.</p> <p>Confidentiality Threats: Confidentiality ensures that sensitive information remains protected from unauthorized access. Threats to confidentiality typically involve eavesdropping and data theft,</p> <p>Denial of Service (DoS) Threats: DoS attacks disrupt the availability of services by overwhelming systems with excessive requests or resource consumption. Common DoS threats include- Flooding machines with bogus requests, Filling up disk or memory and Isolating machines using DNS attacks etc.</p> <p>Authentication Threats: Authentication ensures that only legitimate users can access a system. Threats in this category focus on identity theft and unauthorized access, such as Impersonation of legitimate users and data forgery.</p>
c.	With the help of a diagram, explain the alert protocol and its operation. [04M]
Solution	<p>Alert protocol consists of two bytes. The first byte may be warning or fatal to convey the severity of the message. If the level is fatal, SSL immediately terminates that connection. Other connections on the same session may continue, but no new connections on this session may be established. The second byte contains a code that indicates the specific alert.</p> <p>Some alerts are listed below: unexpected_message, bad_record_mac, decompression_failure, handshake_failure, illegal_parameter, no_certificate, bad_certificate, unsupported_certificate, certificate_revoked, certificate_expired and certificate_unknown etc.</p>
	OR
4.a	With suitable diagram, explain how the Message Authentication Code (MAC) is calculated and the generation of pseudorandom function in transport layer security. [10M]
Solution	<p>Message Authentication Code (MAC) Calculation in TLS:</p> <p>TLS uses HMAC (Hashed Message Authentication Code) which ensures data integrity and authenticity by computing a cryptographic hash using a secret key.</p> <p>The HMAC function is mathematically represented as:</p> $HMAC_K(M) = H((K^+ \oplus opad) \parallel H((K^+ \oplus ipad) \parallel M))$ <p>H = Hash function. M = Message input to HMAC K⁺ = Secret key padded with zeros to match the block length of the hash function. ipad (Inner Padding) = 00110110 in binary repeated 64 times opad (Outer Padding) = 01011100 in binary repeated 64 times.</p> <p>The MAC in TLS is computed over specific fields of the TLSCompressed message, which include:</p>

```
MAC(MAC_write_secret, seq_num || TLSCompressed.type ||
    TLSCompressed.version || TLSCompressed.length ||
    TLSCompressed.fragment)
```

Transport Layer Security (TLS) uses a Pseudorandom Function (PRF) to expand a small shared secret into larger key blocks for secure communication. The purpose of PRF is to generate cryptographically secure key material.



```
P_hash(secret, seed) = HMAC_hash(secret, A(1) || seed) ||
    HMAC_hash(secret, A(2) || seed) ||
    HMAC_hash(secret, A(3) || seed) || .
```

where A () is defined as

$A(0) = \text{seed}$

$A(i) = \text{HMAC_hash}(\text{secret}, A(i-1))$

b. Explain the connection initiation and closure of HTTPs in detail.

[10M]

Solution

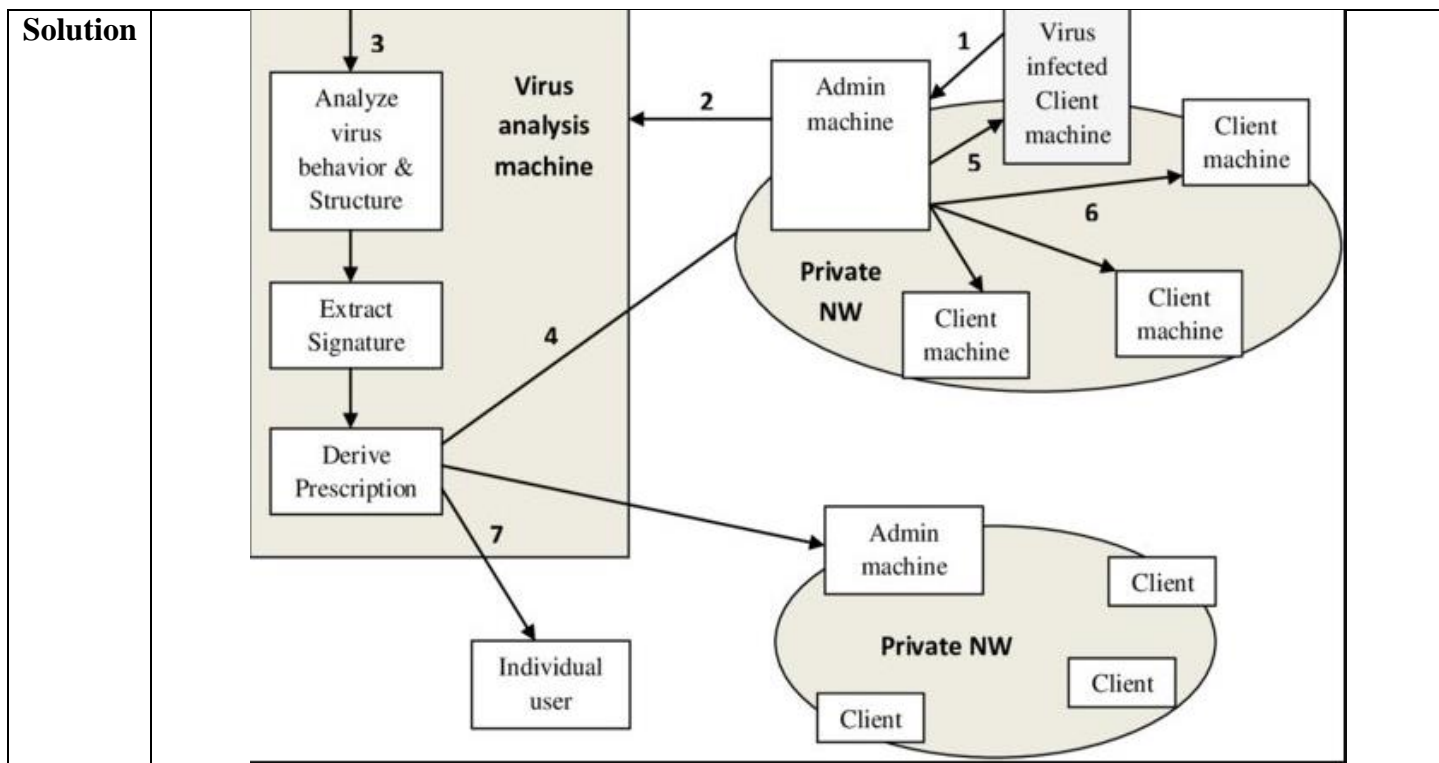
HTTPS (Hypertext Transfer Protocol Secure) ensures secure communication between a client (browser) and a web server using TLS (Transport Layer Security). The process involves two main stages: connection initiation (TLS handshake) and connection closure.

The connection initiation starts when the client sends a **ClientHello** message to the server, including supported TLS versions, cipher suites, and a random number (client nonce). The server responds with a

	<p>ServerHello, selecting a TLS version, cipher suite, and providing its digital certificate, issued by a trusted Certificate Authority (CA). The client verifies the certificate to confirm the server's authenticity.</p> <p>In TLS 1.2, the client generates a pre-master secret, encrypts it using the server's public key, and sends it to the server. Both parties then derive a master secret to generate encryption keys. Once encryption is established, both client and server send a "Finished" message, confirming a secure connection.</p> <p>The connection closure begins when the client sends a "Close Notify" message to indicate that communication has ended. The server responds with its own "Close Notify", after which both parties delete encryption keys and terminate the session. The underlying TCP connection is then closed.</p>
	Module-3
5.a	Explain the transport and tunnel modes in IP security. [10M]
Solution	<p>IP Security is a protocol suite that provides secure communication over IP networks by ensuring confidentiality, integrity, and authentication. It operates in two modes: Transport Mode and Tunnel Mode, both of which define how IP packets are protected and transmitted.</p> <p>In Transport Mode, only the payload (data portion) of the IP packet is encrypted and authenticated, while the IP header remains unchanged. This mode is mainly used for end-to-end communication between two devices, such as a client and a server.</p> <p>In Tunnel Mode, the entire IP packet (both header and payload) is encrypted and encapsulated inside a new IP packet with a different header. This mode is commonly used for network-to-network communication, such as in Virtual Private Networks.</p> <p>The entire original, inner, packet travels through a tunnel from one point of an IP network to another; no routers along the way are able to examine the inner IP header. Because the original packet is encapsulated, the new, larger packet may have totally different source and destination addresses, adding to the security</p>
b.	Mention the applications and benefits of IP security. [10M]
Solution	<p>IP Security is a set of protocols used to secure communications over IP networks by providing encryption, authentication, and integrity protection.</p> <p>Applications of IPsec:</p> <p>Secure Branch Office Connectivity: A company can create a secure VPN (Virtual Private Network) over the Internet or a public WAN, reducing the need for private networks. This lowers costs and simplifies network management.</p> <p>Secure Remote Access: Employees can securely access the company network via an Internet Service Provider (ISP) without expensive long-distance calls. This is beneficial for traveling employees and remote workers.</p> <p>Extranet and Intranet Security: IPSec ensures secure communication with external partners by providing authentication, confidentiality, and secure key exchange, making business collaborations safer.</p> <p>Enhanced E-commerce Security: While many web and e-commerce applications have built-in security, IPSec adds an extra layer by encrypting and authenticating all network traffic, ensuring better data protection.</p> <p>Benefits of IPsec:</p> <p>Strong Perimeter Security: When IPSec is implemented in a firewall or router, it secures all traffic crossing the network boundary without adding extra processing overhead to internal traffic.</p> <p>Bypass Protection: IPSec in a firewall prevents unauthorized access, ensuring that all external traffic must pass through a secure IP-based channel.</p> <p>Application Transparency: Since IPSec operates below the transport layer (TCP/UDP), it secures all network traffic without requiring changes to applications or user software.</p> <p>User-Friendly Security: IPSec is transparent to end users, eliminating the need for user training, per-user security configurations, or key revocation when employees leave.</p>
	OR
6.a	Illustrate the working of basic combinations of security associations. [10M]

Solution	<p>The combination of security associations depends on whether Authentication Header (AH) or Encapsulating Security Payload (ESP) is used and whether IPSec operates in Transport Mode or Tunnel Mode. A single security association is applied when only one security protocol, either AH or ESP, is used. For example, in Transport Mode with ESP, only the payload is encrypted while keeping the original IP header intact, making it suitable for end-to-end security between two devices. However, in scenarios requiring both authentication and encryption, a combination of security associations is used.</p> <p>One common combination is Transport Mode with AH and ESP, where AH ensures data integrity and authentication while ESP encrypts the payload for confidentiality. This combination is typically used for secure host-to-host communication. Another widely used setup is Tunnel Mode with ESP, where the entire IP packet, including its header, is encrypted and encapsulated within a new IP header. This method is commonly used in site-to-site VPNs, allowing secure communication between different networks.</p> <p>For higher security, some implementations use Tunnel Mode with both AH and ESP, where AH authenticates the outer packet to prevent spoofing, while ESP ensures encryption for confidentiality. This approach is beneficial when both authentication and encryption are necessary for highly sensitive communications. Additionally, in complex network environments, nested security associations may be applied. In this case, multiple SAs are established when data travels through multiple IPSec gateways, ensuring that information remains protected at different network layers.</p>
b.	<p>Explain the Internet Key Exchange process using Diffie-Hellman algorithm. [10M]</p>
Solution	<p>Internet Key Exchange (IKE) is a key management protocol in IPSec that establishes secure communication by determining and distributing secret keys. It uses the Diffie-Hellman algorithm to securely exchange keys without needing a pre-existing shared secret.</p> <p>In Diffie-Hellman, both users agree on two global parameters: a large prime number (q) and a primitive root (α) of that number. Each user selects a private key (X_A and X_B), computes a public key, and exchanges it. The final secret key is then computed using:</p> $K = (Y_B)^{X_A} \mod q = (Y_A)^{X_B} \mod q$ <p>This ensures that both users derive the same shared secret key for encryption.</p>
Module-4	
7.a	<p>Explain the 3 classes of intruders with examples and explain the intruder behaviour patterns. [10M]</p>
Solution	<p>Intruders, often referred to as hackers or attackers, are individuals who gain unauthorized access to computer systems and networks. They can be classified into three main categories based on their intent and expertise: masqueraders, misfeasors, and clandestine users. Each type of intruder poses a unique security threat and follows distinct behavior patterns.</p> <p>Masqueraders are unauthorized users who gain access to a system by stealing login credentials or exploiting vulnerabilities. They do not have legitimate access but use techniques such as phishing, brute-force attacks. Their behavior is often characterized by attempts to bypass authentication mechanisms and exploit weak security controls to gain entry.</p> <p>Misfeasors, on the other hand, are insiders who have legitimate access to a system but misuse their privileges for personal gain or to cause harm. These individuals may be employees who exploit their access for malicious purposes. Misfeasors are particularly dangerous because they already have access to internal systems, making it difficult to detect their activities until significant damage has been done.</p> <p>Clandestine users are highly skilled hackers who secretly access systems and avoid detection for a long time. They use advanced techniques like backdoors, hidden malware, and privilege escalation to gain control. For example, a government hacker might secretly enter a database for spying while erasing any signs of intrusion. They often disable security logs and use stealthy methods to remain undetected.</p>
b.	<p>Explain the types of malicious software in detail. [10M]</p>
Solution	<p>Malicious software, or malware, is designed to harm, steal data, or disrupt computer systems. There are several types of malware, each with different ways of attacking and affecting devices.</p> <p>One common type is a virus, which attaches itself to files and spreads when the infected file is opened. It can corrupt files, slow down the system, or even delete important data. Similar to a virus, a worm spreads across networks but does not need a host file to operate. It can multiply rapidly and consume system resources, causing network slowdowns or crashes.</p> <p>Another dangerous type of malware is a Trojan horse, which appears to be a useful program but secretly</p>

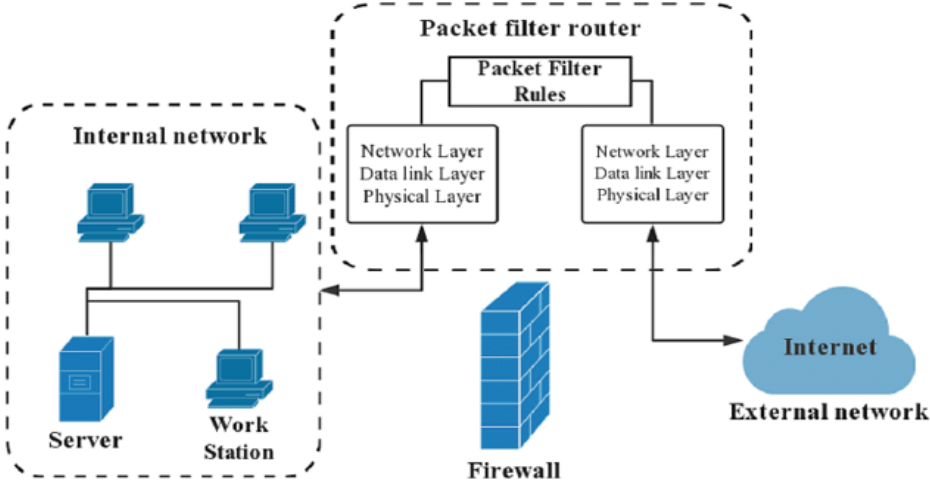
	<p>carries harmful code. Once installed, it can give hackers access to the system, allowing them to steal data or control the computer remotely. Unlike Trojans, spyware runs silently in the background, tracking user activity, collecting passwords, and stealing personal information. Spyware is often used for surveillance or fraud.</p> <p>A more aggressive type is ransomware, which locks or encrypts a user's files and demands payment to restore access. This type of malware is widely used in cyberattacks, targeting businesses and individuals by blocking access to important data. Adware is another form of malware that floods the system with unwanted advertisements, slowing down performance and sometimes leading to more harmful infections. Additionally, rootkits are used to hide malicious activities by modifying system settings, making it extremely difficult to detect or remove the malware. Botnets, on the other hand, turn infected computers into a network of bots controlled by hackers to launch attacks, such as spreading spam or performing large-scale cyberattacks.</p>
	OR
8.a	Describe the generations of antivirus software. [10M]
Solution	<p>The developments in antivirus software can be categorized into four generations, each improving security measures against different types of attacks.</p> <p>The first generation of antivirus software used signature-based detection, where predefined virus signatures were compared with files to identify known threats. This method was effective against early viruses but failed to detect new or modified malware. It required frequent updates to maintain an up-to-date virus signature database.</p> <p>To overcome the limitations of signature-based detection, the second generation introduced Heuristic-Based Detection. This approach analyzed the behavior and structure of programs to detect viruses that were not in the database. It could identify variants of known viruses by looking for suspicious patterns, but it sometimes produced false positives.</p> <p>The third generation of antivirus software focused on monitoring program behavior rather than relying solely on known patterns. It detected malware based on unusual activities, such as unauthorized file modifications, registry changes, or attempts to access critical system components. This method was more effective against polymorphic and metamorphic viruses, which frequently changed their code to avoid detection.</p> <p>Modern antivirus software combines AI (Artificial Intelligence), machine learning, and cloud-based security to detect and prevent cyber threats. These systems analyze large datasets, detect zero-day threats, and use real-time updates from cloud-based threat intelligence networks.</p>
b.	With neat diagram, explain the digital immune system approach of virus protection. [10M]



The **Digital Immune System** is an **automated security mechanism** designed to detect, analyze, and neutralize computer viruses efficiently. The process begins when a **client machine** detects suspicious activity and identifies a possible virus. This information is immediately sent to the **admin machine** within the network for verification. If the admin machine confirms the presence of a virus, it forwards the infected file to a virus analysis machine, where the virus behavior and structure are examined. Through this analysis, a unique virus signature is extracted, which helps in precisely identifying the virus and understanding its impact.

Once the virus is identified, the system derives a prescription or antivirus solution, which is then sent back to the network for implementation. The admin machine distributes the antivirus update to all connected client machines within the network, ensuring that they are protected from the newly discovered virus. This prevents further infections and stops the virus from spreading.

	Module-5	
9.a	What are the capabilities and limitations of firewall?	[10M]
Solution	<p>A firewall is a security mechanism that acts as a protective barrier between a trusted internal network and an untrusted external network, such as the internet. It monitors, filters, and controls network traffic based on predefined security rules to prevent unauthorized access and cyber threats. Firewalls are capable of blocking malicious traffic by filtering data based on IP addresses thereby preventing hacking attempts and unauthorized access to private networks. They also provide protection against known threats such as viruses and malware by restricting suspicious connections. Additionally, firewalls support Virtual Private Networks (VPNs), allowing secure remote access by encrypting data transmission. They can also mitigate Denial-of-Service (DoS) attacks by limiting excessive traffic from malicious sources. Moreover, firewalls maintain logs of network activity, enabling administrators to monitor security events and detect unusual traffic patterns.</p> <p>Despite their strong security features, firewalls have certain limitations. They cannot prevent internal threats, such as employees misusing authorized access, nor can they eliminate malware that has already entered the network through phishing emails or infected USB drives. Additionally, managing firewall configurations can be complex, and improper settings may lead to security gaps or block legitimate traffic.</p>	
b.	What are the different types of firewall? With a neat diagram, describe the working of packet filtering firewall. [10M]	
Solution	Firewalls are security mechanisms designed to monitor and control incoming and outgoing network traffic	

	<p>based on predefined rules. They act as a barrier between internal and external networks to protect systems from unauthorized access and cyber threats.</p> <p>Types of Firewalls: Packet Filtering Firewall Stateful Inspection Firewall Proxy Firewall (Application Layer Firewall) Circuit-Level Gateway Firewall Next-Generation Firewall</p> <p>Working of a Packet Filtering Firewall: A packet filtering firewall examines individual packets passing through a network and applies filtering rules based on source IP, destination IP, port number, and protocol type. If a packet matches an allowed rule, it is forwarded; otherwise, it is dropped or rejected.</p> 
	OR
10.a	With neat diagram, explain the distributed firewall configuration. [8M]
Solution	<p>A distributed firewall is a modern security system that protects computers and networks by applying security rules in multiple locations rather than just at a single entry point. Unlike traditional firewalls that are placed at the boundary of a network, distributed firewalls are installed on individual computers, servers, and network devices, ensuring protection at every level.</p> <p>In this system, a central control unit manages security rules and sends updates to all connected devices. These devices then enforce the security rules locally, blocking harmful traffic and allowing safe connections. This setup helps prevent cyberattacks from spreading within a network and ensures that every device is protected, even if one part of the system is compromised.</p>
b.	Discuss the characteristics of Bastion host. Explain the host-based and personal firewalls. [12M]
Solution	<p>A bastion host is a highly secure computer placed at the boundary of a network to filter and monitor external traffic. It is designed to withstand attacks and typically runs firewalls, proxy servers, or authentication services. Since it is directly exposed to the internet, it has minimal software, restricted access, and regular updates to reduce vulnerabilities. Its main role is to prevent attackers from accessing internal networks while allowing legitimate requests.</p> <p>A host-based firewall is software installed on individual computers or servers to monitor and control incoming and outgoing traffic. It provides an extra layer of security by blocking unauthorized access, detecting suspicious activity, and preventing malware attacks. These firewalls are commonly used in organizations to protect each device separately, even if the network firewall fails.</p> <p>A personal firewall is a simplified version of a host-based firewall, designed for individual users. It protects personal computers from internet threats, hacking attempts, and malicious software. Personal firewalls alert users when unknown applications try to access the internet and allow them to block or permit connections.</p>