CNS TT2

MODULE 3: 5 marks

(---Aman)

Q.1. List and explain all types of Malwares in detail. Differentiate between Virus and Worms.

Ans. Malware is a software that gets into the system without user consent to steal the user's private and confidential data, including bank details and passwords. They also generate annoying pop-up ads and change system settings. Malware includes computer viruses, worms, Trojan horses, ransomware, spyware, and other malicious programs.

Types of Malwares and their operations:

Viruses – A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.

Worms – Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.

Trojan horse – A Trojan horse is a malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, and audio files.

Adware – It displays unwanted ads and pop-ups on the computer. It comes along with software downloads and packages. It generates revenue for the software distributer by displaying ads.

Spyware – Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.

Worms	Viruses
A Worm is a form of malware that replicates itself and can spread to different computers via a Network.	A Virus is a malicious executable code attached to another executable file that can be harmless or can modify or delete data.
The main objective of worms is to eat the system's resources.	The main objective of viruses is to modify the information.
It doesn't need a host to replicate from one computer to another.	It requires a host is needed for spreading.
It is less harmful as compared.	It is more harmful.
Worms can be detected and removed by the Antivirus and firewall.	Antivirus software is used for protection against viruses.
Worms can be controlled by remote.	Viruses can't be controlled by remote.
Worms are executed via weaknesses in the system.	Viruses are executed via executable files.
Worms generally come from the downloaded files or through a network connection.	Viruses generally come from shared or downloaded files.

Q.2. Define Malware. Explain at least five types with example.

Ans. REFER Q.1

MODULE 4: 5 marks

Q.1. Explain how Network Management security is implemented using SNMP v3.

Ans.

Q.2. Discuss/Explain different NAC enforcement methods.

Ans. Network Access Control (NAC) enforcement methods are crucial for ensuring that only authorized devices and users can access a network.

Here are the main NAC enforcement methods:

1. Pre-Admission Control: Evaluates devices before network access is granted, denying or restricting non-compliant devices. This proactive approach ensures that only secure devices can connect, keeping threats at bay.

2. Post-Admission Control: Continuously monitors devices after they are connected. If a device becomes non-compliant (e.g., missing patches), it is quarantined or restricted, ensuring ongoing network security and compliance.

3. Layer 2 Enforcement: Utilizes VLANs and port-based access control at the switch level. Devices are assigned to specific VLANs based on compliance, segregating and controlling access to critical network resources effectively.

4. Layer 3 Enforcement: Implements IP-based controls like Access Control Lists (ACLs) and firewall rules. Manages network access through routing and firewall policies, adding an extra layer of security.

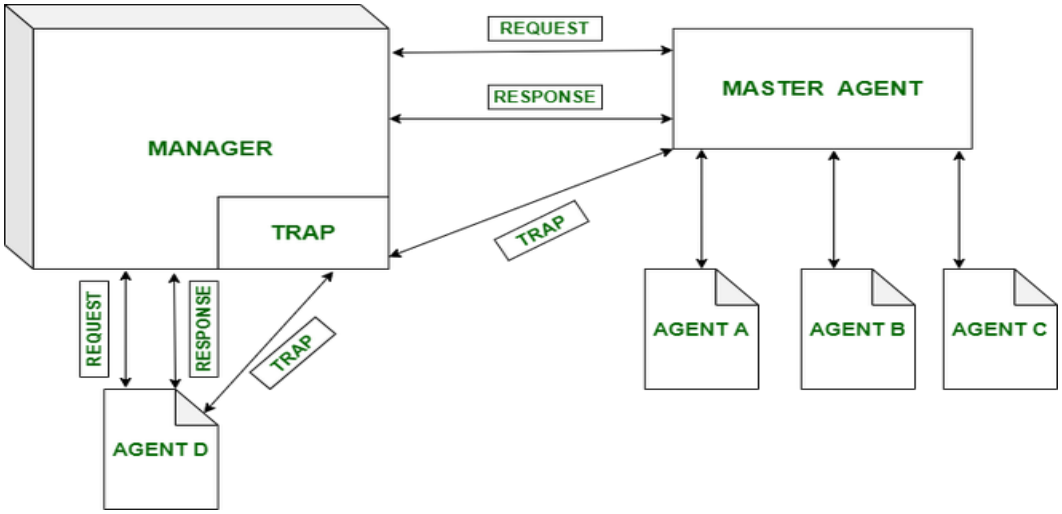
5. Agent-Based Enforcement: Involves installing software agents on devices to monitor and report their compliance status. This method provides detailed visibility into device health and security status, allowing for granular control.

6. Agentless Enforcement: Uses network-based techniques such as scanning and monitoring to assess device compliance without the need for installed agents. This is particularly useful for non-agent-compatible devices like IoT devices.

7. Hybrid Enforcement: Combines various enforcement methods to create a tailored NAC solution, providing flexibility and robust security across diverse network environments. This approach adapts to different needs, enhancing overall security.

Q.3. Explain SNMP v3.

Ans. SNMP stands for Simple Network Management Protocol. It is basically an Internet Standard Protocol which is used for monitoring and organizing information about the devices on IP network by sending and receiving requests. This protocol is used for organizing information from devices like switches, modems, routers, servers, printers etc. Currently, there are 3 versions of SNMP – SNMPv1, SNMPv2, SNMPv3.



Uses of SNMP in Networking:

1. It is mainly used for monitoring and organizing networking resources.

2. It is a standard internet protocol which is to be followed by everyone. It sets a standard for everyone network management, database management, and organizing data objects.

Special Features about SNMPv3:

1. v3 is the latest version of SNMP which involves great management services with enhanced security.

2. The SNMPv3 architecture makes the use of **User-based Security Model (USM)** for security of the messages & the **View-based Access Control Model (VACM)** for accessing the control over the services.

3. USM – For facilitating remote configuration and management of the security module.

4. VACM – For facilitating remote configuration & management for accessing the controlling module.

5. SNMP v3 security models supports authentication and encrypting.

6. SNMPv3 supports Engine ID Identifier, which uniquely identifies each SNMP identity.

SNMPv3 Architecture: The architecture of the v3 consists of –	**Mechanism of version 3:**
1. Data definition language **2.** Definition of MIB **3.** Protocol definition **4.** Security and administration.	**1.** 16-byte key between sender & receiver **2.** Triple Data Encryption Standard **3.** Advanced Encryption Standard **4.** Data Encryption Standard (DES) in Cipher Block Chaining (CBC) mode

Q.4. Explain the need of Network Access Control in Enterprise Networks. Explain the major NAC enforcement methods.

Ans. In enterprise networks, the growing number of devices, users, and security threats makes it imperative to control who and what can access the network.

Here's why NAC is essential:

1. Security: NAC ensures only authorized users and compliant devices access the network, reducing unauthorized access, data breaches, and cyber threats.

2. Compliance: Helps organizations meet regulatory requirements by enforcing security policies consistently across all devices and users.

3.Endpoint Visibility: Provides visibility into all devices connected to the network, aiding in identifying and managing unknown or rogue devices.

4. Access Control: Enforces access policies to ensure users access only necessary resources, minimizing internal threats.

5. Incident Response: Quarantines compromised devices quickly, preventing malware spread or further damage.

Major NAC Enforcement Methods: -

1. Pre-Admission Control: Evaluates devices before network access, denying or restricting non-compliant devices, ensuring only secure devices connect.

2. Post-Admission Control: Continuously monitors devices post-connection, restricting access for non-compliant devices to maintain ongoing security.

3. Layer 2 Enforcement: Uses VLANs and port-based access control at the switch level, placing compliant devices in specific VLANs for enhanced network segmentation.

4. Layer 3 Enforcement: Implements IP-based controls like ACLs and firewall rules, managing network access through routing and firewall policies for added security.

5. Agent-Based Enforcement: Involves installing software agents on devices to monitor and report compliance status, providing detailed visibility into device health and security.

6. Agentless Enforcement: Uses network-based techniques, such as scanning, to assess device compliance without installed agents, useful for IoT devices.

7. Hybrid Enforcement: Combines various methods to tailor NAC solutions to specific needs, providing robust security across diverse environments.

Q.5. What is Network Management Security?

Ans. Network Management Security involves safeguarding network infrastructure and data from threats and unauthorized access. It's about ensuring that the network operates reliably, securely, and efficiently.

Core Aspects of Network Management Security

Authentication: Verifying the identity of users and devices before granting access to the network. This ensures that only authorized users can access the network resources.

Authorization: Determining what resources and services an authenticated user or device is allowed to access. This involves setting permissions and access controls.

Encryption: Protecting data transmitted over the network by converting it into a secure format that can only be read by authorized parties. This prevents eavesdropping and data breaches.

Monitoring and Auditing: Continuously observing network activities to detect and respond to suspicious behaviour or anomalies. Auditing involves keeping logs of network activities for analysis and compliance purposes.

Intrusion Detection and Prevention: Systems that identify and block malicious activities and potential security breaches. These systems can be network-based or host-based.

Patch Management: Regularly updating and applying patches to network devices and software to fix vulnerabilities and enhance security.

Access Control: Implementing policies and mechanisms that control who or what can view or use resources in a network. This includes firewalls, VPNs, and NAC (Network Access Control).

MODULE 5: 2 marks

Q.1. How does IPSec help to achieve authentication and confidentiality?

Ans. Authentication: IPSec uses Authentication Header (AH) and Internet Key Exchange (IKE) to verify the identity of communicating parties and ensure data integrity. AH provides data integrity and authenticates IP packets, while IKE sets up a secure channel for exchanging encryption keys and authenticates the parties involved using pre-shared keys or digital certificates.

Confidentiality: IPSec ensures data confidentiality by using Encapsulating Security Payload (ESP), which encrypts the payload of IP packets, making the data unreadable to unauthorized parties. ESP supports various encryption algorithms like DES, 3DES, and AES to protect data during transmission.

By combining these protocols, IPSec achieves both authentication and confidentiality, ensuring secure and private communication over IP networks.

Q.2. How is security achieved in the transport and tunnel modes of IPSEC?

Ans. A) Transport Mode:

Encryption and Authentication: Encrypts and authenticates only the payload of the IP packet, not the header.

Use Case: Ideal for end-to-end communication between two devices, such as a client and a server within a private network.

B) Tunnel Mode:

Encryption and Authentication: Encrypts and authenticates the entire IP packet, including both the payload and the header, then adds a new IP header.

Use Case: Perfect for VPNs (Virtual Private Networks) where secure communication is needed between two networks over an untrusted network, like the internet.

Both modes use:

Authentication Header (AH): Ensures data integrity and authenticity.

Encapsulating Security Payload (ESP): Provides encryption and optional data integrity and authenticity.

By using these mechanisms, IPSec ensures secure, authenticated, and confidential communication in both transport and tunnel modes.

Q.3. Explain the challenges of using VPN.

Ans.

1. Performance Issues: VPNs can slow down internet speeds due to encryption and rerouting of traffic, affecting high-bandwidth activities like streaming and gaming.

2. Complexity in Setup: Setting up a VPN can be complex, requiring configuration of both client and server software, and ensuring device compatibility.

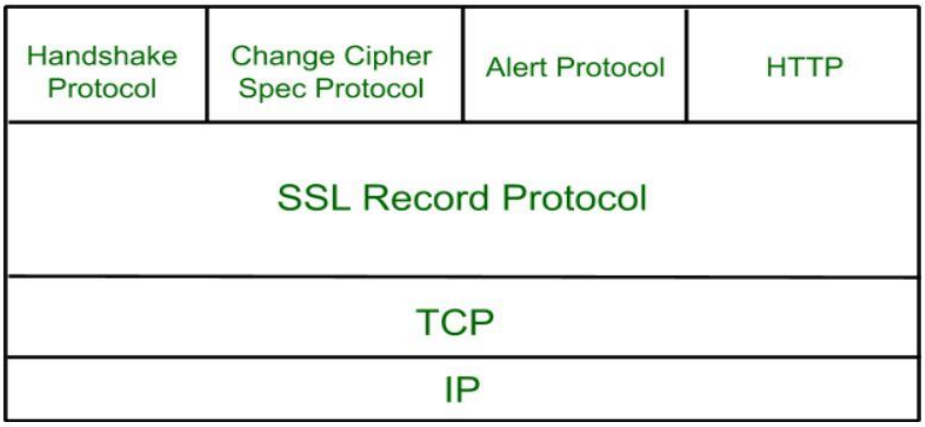
3. Security Concerns: VPNs can introduce vulnerabilities. If a provider has weak security, it can expose users to risks. Trusting the provider with your data is crucial.

4. Legal and Regulatory Issues: Some countries restrict or prohibit VPN use, leading to potential legal implications for users.

5. Cost: Free VPN plans often come with limitations. Premium services can be expensive, especially for businesses needing multiple licenses.

Q.4. Describe different types of protocol offered by SSL.

Ans.



Types of Protocols Offered by SSL: -

1. Handshake Protocol: Establishes a secure session between client and server, negotiating security parameters and authenticating the server (and optionally the client).

2. Record Protocol: Ensures confidentiality and integrity of data using encryption and Message Authentication Code (MAC).

3. Alert Protocol: Handles error messages and alerts, communicating issues like security failures or session terminations.

4. Change Cipher Spec Protocol: Updates the cipher suite being used, informing the other party that subsequent records will be protected under the new encryption and hashing algorithms.

Q.5. Explain the function of SSH connection protocol.

Ans. 1. Authentication: Verifies the identities of client and server using methods like passwords or public key authentication, ensuring both parties are legitimate.

2. Encryption: Encrypts all data transmitted over the SSH connection, preventing eavesdropping and ensuring data confidentiality.

3. Data Integrity: Uses hashing algorithms to detect any alterations in data during transmission, protecting against tampering.

4. Secure Tunnelling: Allows secure transmission of other protocols over an insecure network, enabling safe remote access to applications and services.

5. Remote Command Execution: Enables users to execute commands on a remote server, facilitating management and administration from any location.

Q.6. What is the significance of transport layer security?

Ans. Significance of Transport Layer Security (TLS): -

1. Data Encryption: Encrypts data during transmission, ensuring confidentiality and protecting sensitive information from unauthorized access.

2. Authentication: Uses certificates to verify the identities of communicating parties, preventing man-in-the-middle attacks and ensuring trust.

3. Data Integrity: Employs cryptographic hash functions to detect tampering, maintaining the integrity of data in transit.

4. Secure Communication: Provides a secure channel for communications over insecure networks, essential for online activities like banking and shopping.

5. Standardization: Widely adopted and standardized, making it a reliable and trusted method for securing network communications across various platforms.

Q.7. Differentiate between HTTP and HTTPs.

Ans.

HTTP	HTTPS
The full form of HTTP is the Hypertext Transfer Protocol.	The full form of HTTPS is Hypertext Transfer Protocol Secure.
It is written in the address bar as http://.	It is written in the address bar as https://.
The HTTP transmits the data over port number 80.	The HTTPS transmits the data over port number 443.
It is unsecured as the plain text is sent, which can be accessible by the hackers.	It is secure as it sends the encrypted data which hackers cannot understand.
It is mainly used for those websites that provide information like blog writing.	It is a secure protocol, so it is used for those websites that require to transmit the bank account details or credit card numbers.
It is an application layer protocol.	It is a transport layer protocol.
It does not use SSL.	It uses SSL that provides the encryption of the data.
Google does not give the preference to the HTTP websites.	Google gives preferences to the HTTPS as HTTPS websites are secure websites.
The page loading speed is fast.	The page loading speed is slow as compared to HTTP because of the additional feature that it supports, i.e., security.

Q.8. Explain how VPN can be used to encrypt your personal data.

Ans. Using a VPN (Virtual Private Network) to encrypt personal data involves several key steps, which are as follows:

1. Secure Tunnel: VPN creates an encrypted tunnel between your device and the VPN server, protecting data from unauthorized access.

2. Data Encryption: Uses strong encryption protocols like AES-256 to ensure data remains unreadable to interceptors.

3. IP Address Masking: Hides your real IP address, showing the VPN server's location instead, masking your online identity.

4. Secure Transmission: Encrypts all internet activity, including browsing and emails, protecting data from hackers and surveillance.

5. Public Wi-Fi Security: Adds an extra layer of protection when using public Wi-Fi, safeguarding personal information from potential attackers.

Q.9. Explain Email Security Process.

Ans. 1. Authentication: Uses SPF, DKIM, and DMARC protocols to verify the sender's legitimacy and prevent email spoofing.

2. Encryption: Encrypts email content during transit using TLS, and provides end-to-end encryption with PGP or S/MIME to ensure confidentiality.

3. Digital Signatures: Utilizes digital signatures to verify the sender's identity and ensure the email content hasn't been altered.

4. Spam and Phishing Filters: Detects and filters out spam, phishing attempts, and malicious emails to protect recipients from fraudulent messages.

5. Anti-Malware Scanning: Scans email attachments and links for malware and viruses to prevent harmful software from infecting the recipient's device.

Q.10. Explain how S/MIME can be used for Digital Signature and verification operations on email messages.

Ans. S/MIME for Digital Signature and Verification: -

1. Generate Digital Signature: The sender creates a hash of the email message and encrypts it with their private key, forming a unique digital signature.

2. Send Email: The email, digital signature, and sender's public key certificate are sent to the recipient.

3. Verification: The recipient uses the sender's public key to decrypt the digital signature and compares it with the hash of the received email. If the hashes match, the email is verified as authentic and unaltered.

Benefits:

1. Authentication: Confirms the sender's identity.

2. Integrity: Ensures the message hasn't been tampered with.

3. Non-Repudiation: Prevents the sender from denying the email's origin.

Q.11. Explain Transport Layer Security.

Ans. 1. Encryption: TLS encrypts data during transmission, ensuring confidentiality and protecting sensitive information from eavesdropping.

2. Authentication: Uses digital certificates to authenticate the parties involved, verifying identities and preventing man-in-the-middle attacks.

3. Data Integrity: Employs cryptographic hash functions to ensure data hasn't been tampered with during transmission.

4. Secure Communication: Establishes a secure channel for communications over insecure networks, essential for activities like online banking and shopping.

5. Standardization: Widely adopted and standardized, making it a trusted and reliable method for securing communications across various platforms.

Q.12. What are the goals of secure socket layer (SSL)?

Ans. 1. Data Confidentiality: Encrypts data to ensure privacy and protect it from eavesdropping.

2. Data Integrity: Ensures data is not altered during transmission using cryptographic checksums.

3. Authentication: Verifies the identities of communicating parties using digital certificates.

4. Secure Communication: Provides a secure channel over an insecure network, safeguarding data exchanges.

5. Non-Repudiation: Prevents denial of involvement by either party in the communication.

Q.13. Explain SSH protocol stack in brief.

Ans. Transport Layer Protocol (SSH-TRANS): Provides server authentication, data confidentiality, and integrity. Establishes a secure, encrypted channel between the client and server, handling key exchange and encryption.
User Authentication Protocol (SSH-AUTH): Authenticates the user to the server using methods like passwords, public keys, or certificates, ensuring only authorized users access the server.
Connection Protocol (SSH-CONN): Manages multiple logical channels over a single SSH connection, enabling tunnelling, port forwarding, and remote command execution.
This layered stack ensures secure and authenticated communication for remote access and administration.