Saveetha School of Engineering

Saveetha Institute of Medical and Technical Sciences

Department of Computer Science Engineering

Engineer to Excel

CSA54 - Computer and Internet Security

Viva Questions

UNIT I MANAGING INTERNET SECURITY

Exploring Addresses, Subnets, and Hostnames, Networking Configuration files, Network access files, Examining TCP/IP Daemons, Examining the system Daemons, creating Daemons.

1. What is an IP address?
   Answer: An IP address is a unique number assigned to a device on a network to identify it.
2. What is a subnet?
   Answer: A subnet is a smaller network created from a larger network to improve efficiency and security.
3. What does a subnet mask do?
   Answer: It separates the network and host parts of an IP address.
4. What is a hostname?
   Answer: A hostname is a human-readable name assigned to a computer or device on a network.
5. What is the /etc/hosts file used for?
   Answer: It maps hostnames to IP addresses for local name resolution.
6. What is the purpose of the /etc/resolv.conf file?
   Answer: It defines the DNS servers used for domain name resolution.
7. What is a network daemon?
   Answer: A daemon is a background process that provides network services, such as SSH or FTP.
8. What is the role of the SSH daemon (sshd)?
   Answer: It allows secure remote access to a computer over a network.
9. How do you check running daemons in Linux?
   Answer: By using systemctl list-units --type=service or ps aux.
10. What command is used to restart a daemon?
    Answer: sudo systemctl restart <daemon_name>.
11. What is a configuration file?
    Answer: A file that stores settings for a program or system service.

12. What is the purpose of the /etc/network/interfaces file?
    Answer: It configures network interfaces on a Linux system.
13. What is TCP/IP?
    Answer: TCP/IP is a set of protocols that allows computers to communicate over networks.
14. What is the function of a firewall?
    Answer: A firewall protects a network by blocking unauthorized access.
15. How do you check active network connections in Linux?
    Answer: Using the netstat -tulnp or ss -tulnp command.
16. What is DHCP?
    Answer: DHCP assigns IP addresses to devices automatically.
17. What is the difference between a static and a dynamic IP address?
    Answer: A static IP does not change, while a dynamic IP is assigned by DHCP and may change.
18. What is the role of the /etc/hosts.allow and /etc/hosts.deny files?
    Answer: They control which devices can access network services.
19. What is the difference between a TCP and UDP connection?
    Answer: TCP is connection-based and reliable, while UDP is connectionless and faster.
20. How do you stop a running network daemon?
    Answer: Using sudo systemctl stop <daemon_name>.

UNIT II GAINING ACCESS AND SECURING THE GATEWAY

Sniffing, Spoofing, Configuring TCP/IP, Configuring Telnet, Configuring FTP, Configuring Send mail, SSL, SATAN, Encryption. Cryptography, PGP Keys, Key management, Security of PGP.

1. What is packet sniffing?
   Answer: Packet sniffing is monitoring and capturing network traffic using tools like Wireshark.
2. What is IP spoofing?
   Answer: IP spoofing is sending data with a fake IP address to disguise the sender's identity.
3. How can packet sniffing be prevented?
   Answer: By using encryption, VPNs, and secured protocols like HTTPS.
4. What is MAC spoofing?
   Answer: Changing a device's MAC address to bypass network restrictions or hide identity.
5. What is TCP/IP?
   Answer: TCP/IP (Transmission Control Protocol/Internet Protocol) is a set of protocols used for communication over the internet.
6. How do you check the IP configuration in Linux?
   Answer: Using the command ifconfig or ip addr show.
7. How do you assign a static IP address?
   Answer: By configuring the /etc/network/interfaces file or using nmcli in Linux.

8. Which file stores TCP/IP settings in Windows?
   Answer: The settings are managed under Control Panel → Network and Sharing Center.
9. What is Telnet?
   Answer: Telnet is a protocol used for remote command-line access to a system.
10. How do you enable Telnet in Linux?
    Answer: By installing the Telnet server (sudo apt install telnetd) and starting the service.
11. Why is Telnet considered insecure?
    Answer: It transmits data in plaintext without encryption, making it vulnerable to attacks.
12. What is FTP?
    Answer: FTP (File Transfer Protocol) is used to transfer files between computers over a network.
13. Which command is used to connect to an FTP server?
    Answer: ftp <server_address>
14. How do you secure FTP?
    Answer: By using SFTP (Secure FTP) or FTPS (FTP with SSL encryption).
15. What is Sendmail?
    Answer: Sendmail is a mail transfer agent (MTA) used for sending emails on Linux.
16. Which file is used to configure Sendmail?
    Answer: The configuration file is /etc/mail/sendmail.cf.
17. How do you restart the Sendmail service?
    Answer: Using the command sudo systemctl restart sendmail.
18. What is SSL?
    Answer: SSL (Secure Sockets Layer) encrypts data transmitted between a web server and a client for security.
19. What is the difference between SSL and TLS?
    Answer: TLS (Transport Layer Security) is an improved version of SSL, offering better security and encryption.
20. What is an SSL certificate?
    Answer: It is a digital certificate that validates the identity of a website and enables encryption.
21. What is SATAN used for?
    Answer: SATAN (Security Administrator Tool for Analyzing Networks) is a security tool used for scanning networks to detect vulnerabilities.
22. Is SATAN a hacking tool?
    Answer: No, it is a network analysis tool, but it can be misused if not used ethically.
23. What is encryption?
    Answer: Encryption converts data into a secure format that can only be read with a decryption key.
24. What is symmetric encryption?
    Answer: It uses a single key for both encryption and decryption (e.g., AES, DES).
25. What is asymmetric encryption?
    Answer: It uses a public key for encryption and a private key for decryption (e.g., RSA, ECC).

26. What is PGP?
    Answer: PGP (Pretty Good Privacy) is an encryption program used for securing emails and files.
27. What are PGP keys?
    Answer: PGP uses a public key for encryption and a private key for decryption.
28. How do you generate PGP keys?
    Answer: Using the command gpg --gen-key in Linux.
29. How does PGP ensure security?
    Answer: By combining encryption, authentication, and digital signatures.
30. What is key management in cryptography?
    Answer: It involves generating, storing, distributing, and revoking encryption keys securely.

UNIT III JAVA & CGI SECURITY

Java's functionality, JVM, Setting up java security features. CGI security: Understanding Vulnerability, Minimizing Vulnerability SSI, Protecting Sensitive Data.

1. What is Java Security?
   Answer: Java security refers to the built-in mechanisms that protect Java applications from threats such as unauthorized access, malicious code execution, and data breaches.
2. What is JVM?
   Answer: JVM (Java Virtual Machine) is a runtime environment that executes Java bytecode and provides platform independence.
3. How does JVM contribute to security?
   Answer: JVM enforces security by using a bytecode verifier, class loader, and security manager to prevent harmful code execution.
4. What is the purpose of the Java Security Manager?
   Answer: The Security Manager restricts access to system resources like file operations, network access, and external processes based on security policies.
5. What are Java security policies?
   Answer: Security policies define permissions for Java applications, specifying what resources they can access.
6. Where is Java security policy stored?
   Answer: In the java.policy file located in the Java installation directory.
7. How can you enable a security manager in Java?
   Answer: By using System.setSecurityManager(new SecurityManager()); in the Java program.
8. What is CGI?
   Answer: CGI (Common Gateway Interface) is a standard for running external programs or scripts on a web server to generate dynamic content.

9. What are CGI vulnerabilities?
   Answer: CGI scripts can be vulnerable to code injection, command injection, and unauthorized access if not properly secured.
10. What is SSI in CGI?
    Answer: SSI (Server-Side Includes) is a method for including dynamic content in web pages but can pose security risks if misconfigured.
11. How can you minimize CGI vulnerabilities?
    Answer: By validating user input, restricting script execution permissions, and avoiding shell commands in CGI scripts.
12. What is path traversal in CGI security?
    Answer: It is an attack where an attacker accesses restricted files by manipulating file paths in a CGI request.
13. How does HTTPS improve CGI security?
    Answer: HTTPS encrypts data between the client and server, preventing interception and man-in-the-middle attacks.
14. What is protecting sensitive data in Java and CGI security?
    Answer: It involves encrypting user data, restricting access permissions, and securely storing credentials to prevent data leaks.
15. What is the difference between GET and POST in CGI?
    Answer: GET sends data in the URL, making it less secure, while POST sends data in the request body, providing better security for sensitive information.
16. What is a session hijacking attack in CGI?
    Answer: It is an attack where an attacker steals a user's session ID to gain unauthorized access to their account.
17. How can Java prevent SQL injection?
    Answer: By using Prepared Statements instead of directly embedding user input in SQL queries.
18. What is sandboxing in Java?
    Answer: Sandboxing is a security mechanism that restricts Java applets from accessing system resources beyond their permissions.
19. How can Java applications protect sensitive user data?
    Answer: By using encryption, hashing passwords, and implementing access control mechanisms.
20. What is the main purpose of Java security updates?
    Answer: To fix vulnerabilities and improve protection against new security threats.

UNIT IV MESSAGE AUTHENTICATION AND INTEGRITY

Authentication function – MAC – Hash function – Security of hash function and MAC – SHA –Digital signature and authentication protocols – DSS- Entity Authentication: Biometrics, Passwords, Challenge Response protocols- Authentication applications - Kerberos, X.509

1. What is message authentication?
   Answer: Message authentication ensures that a message has not been altered and verifies the sender's identity.
2. What is a MAC?
   Answer: MAC (Message Authentication Code) is a small piece of information generated from a message and a secret key to verify data integrity and authenticity.
3. How does a MAC work?
   Answer: A MAC is created by applying a secret key to a message using a cryptographic algorithm. The receiver uses the same key to verify the MAC.
4. What is a hash function?
   Answer: A hash function converts input data into a fixed-length string, ensuring data integrity.
5. How is a hash function different from a MAC?
   Answer: A hash function does not use a key, while a MAC requires a secret key for authentication.
6. Why is security important for hash functions and MACs?
   Answer: If a hash function or MAC is weak, attackers can modify data without detection or forge valid authentication codes.
7. What is SHA?
   Answer: SHA (Secure Hash Algorithm) is a family of cryptographic hash functions used for securing data.
8. What are some versions of SHA?
   Answer: SHA-1, SHA-256, SHA-384, and SHA-512.
9. What is a digital signature?
   Answer: A digital signature is a cryptographic method that verifies the authenticity and integrity of a message using encryption.
10. What is the main purpose of digital signatures?
    Answer: To ensure that a message is authentic, unaltered, and sent by the claimed sender.
11. What is DSS?
    Answer: DSS (Digital Signature Standard) is a federal standard for digital signatures, using the DSA (Digital Signature Algorithm).
12. What is entity authentication?
    Answer: Entity authentication verifies the identity of a person or system before allowing access.
13. What are some types of entity authentication?
    Answer: Biometrics, passwords, challenge-response protocols, and token-based authentication.

14. What is biometric authentication?
    Answer: Biometric authentication verifies identity using unique biological traits like fingerprints, iris scans, or facial recognition.
15. How do challenge-response protocols work?
    Answer: The system sends a challenge (random number), and the user must provide a correct response using a cryptographic key.
16. What is Kerberos?
    Answer: Kerberos is a network authentication protocol that uses secret-key cryptography to verify user identities securely.
17. What is a key component of Kerberos authentication?
    Answer: The Ticket Granting Ticket (TGT), which allows users to access multiple services without repeated logins.
18. What is X.509?
    Answer: X.509 is a standard that defines the format of public key certificates for authentication in networks.
19. What is stored in an X.509 certificate?
    Answer: The public key, certificate holder details, issuer information, expiration date, and digital signature.
20. Why is X.509 important in authentication?
    Answer: It provides a standardized way of managing and verifying digital identities in secure communications.

UNIT V SECURITY PRACTICE

Electronic Mail security – PGP, S/MIME – IP security – Web Security - SYSTEM SECURITY: Intruders – Malicious software – viruses – Firewalls

1. **What is email security?**
   Answer: Email security protects emails from threats like phishing, spam, malware, and unauthorized access.
2. **What is PGP?**
   Answer: PGP (Pretty Good Privacy) is an encryption program used to secure emails and files.
3. **How does PGP ensure email security?**
   Answer: PGP uses **public-key encryption** to encrypt messages and **digital signatures** to verify authenticity.
4. **What is S/MIME?**
   Answer: S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for encrypting and signing emails.
5. **What is the difference between PGP and S/MIME?**
   Answer: PGP uses a **web of trust** for key management, while S/MIME relies on **certificate authorities (CAs)**.
6. **What is IP security (IPSec)?**
   Answer: IPSec is a protocol suite that secures internet communication by encrypting and authenticating data packets.

7. **What are the two modes of IPSec?**
   Answer: Transport mode (encrypts only the data) and **Tunnel mode** (encrypts the entire packet).
8. **What is the purpose of a VPN?**
   Answer: A VPN (Virtual Private Network) uses IPSec or SSL to create a secure, encrypted connection over a public network.
9. **What is web security?**
   Answer: Web security protects websites and users from cyber threats like hacking, malware, and phishing.
10. **What is HTTPS?**
    Answer: HTTPS (HyperText Transfer Protocol Secure) encrypts web traffic using SSL/TLS for secure communication.
11. **What is a web application firewall (WAF)?**
    Answer: A WAF filters and blocks malicious traffic to protect websites from attacks like SQL injection and cross-site scripting (XSS).
12. **What is system security?**
    Answer: System security involves protecting a computer system from unauthorized access, malware, and cyber threats.
13. **Who are intruders in cybersecurity?**
    Answer: Intruders are unauthorized users who try to gain access to systems to steal or damage data.
14. **What are malicious software (malware)?**
    Answer: Malware includes viruses, worms, Trojans, ransomware, and spyware that harm or exploit systems.
15. **What is a computer virus?**
    Answer: A virus is a malicious program that spreads by attaching itself to files and infecting systems when executed.
16. **What is the difference between a virus and a worm?**
    Answer: A **virus** needs a host file to spread, while a **worm** can spread independently over a network.
17. **What is ransomware?**
    Answer: Ransomware encrypts a user's files and demands payment to restore access.
18. **What is a firewall?**
    Answer: A firewall is a security system that filters network traffic to block unauthorized access.
19. **What are the types of firewalls?**
    Answer: Packet-filtering firewalls, Stateful firewalls, Proxy firewalls, and Next-Generation Firewalls (NGFWs).
20. **How does a firewall improve security?**
    Answer: By monitoring and controlling incoming and outgoing network traffic based on security rules.