🦚 राधे राधे 🦚

Top Cyber Security & Networking Questions

Basic Concepts

1. **What is cybersecurity, and why is it important?**
    - Protection of internet-connected systems, including hardware, software, and data, from cyberattacks. It's important to protect sensitive data and maintain the functionality and integrity of systems.
2. **Define CIA Triad.**
    - The CIA Triad stands for Confidentiality, Integrity, and Availability, which are the three core principles of cybersecurity:
        - **Confidentiality:** Ensuring that information is accessible only to those authorized to have access.
        - **Integrity:** Maintaining the accuracy and completeness of data.
        - **Availability:** Ensuring that authorized users have access to the information and resources they need when they need them.
3. **What is a firewall? Why is it used?**
    - A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on predetermined security rules.
    - A firewall establishes a barrier between a trusted internal network and internet.
    - Firewalls can be hardware, software, or both.
    - Firewalls are mainly used to protect the system/network from viruses, worms, malware, etc. Firewalls can also be to prevent remote access and content filtering.
4. **Explain encryption.**
    - Encryption is the process of converting plaintext data into an unreadable form called ciphertext.
    - This process uses an algorithm and an encryption key.
    - Encryption is used to protect the confidentiality of data both in transit and at rest.
    - Only those with the correct decryption key can convert the ciphertext back into readable plaintext.
    - Common encryption algorithms include AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and DES (Data Encryption Standard).
5. **What is the difference between symmetric and asymmetric encryption?**

- **Symmetric encryption** uses a single key for both encryption and decryption of data. It is fast and efficient for bulk data encryption but requires securely sharing the key between the sender and receiver.
- **Asymmetric encryption** uses a pair of keys: a public key for encryption and a private key for decryption. It solves the key distribution problem of symmetric encryption but is slower due to the complexity of the encryption process.

6. **What is a VPN?**

   - A Virtual Private Network (VPN) extends a private network across a public network, enabling users to send and receive data as if their devices were directly connected to the private network.
   - VPNs use encryption to secure data transmission, ensuring confidentiality and integrity.
   - **It is used to create a safe and encrypted connection. When you use a VPN, the data from the client is sent to a point in the VPN where it is encrypted and then sent through the internet to another point. At this point, the data is decrypted and sent to the server. When the server sends a response, the response is sent to a point in the VPN where it is encrypted and this encrypted data is sent to another point in the VPN where it is decrypted. And finally, the decrypted data is sent to the client. The whole point of using a VPN is to ensure encrypted data transfer.**

7. **What is an Intrusion Detection System (IDS)?**

   - An IDS is a device or software application that monitors a network or systems for malicious activity or policy violations. An IDS can be configured to detect specific types of activities, log events, and generate alerts. It does not take direct action to stop attacks but provides information to security personnel.

8. **What is an Intrusion Prevention System (IPS)?**

   - An IPS is a proactive network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Unlike IDS, an IPS takes action to prevent detected threats by dropping malicious packets, blocking traffic, and resetting connections.

9. **What is the difference between IDS and IPS?**

   - IDS is Intrusion Detection System and it only detects intrusions and the administrator has to take care of preventing the intrusion. Whereas, in IPS i.e., Intrusion Prevention System, the system detects the intrusion and also takes actions to prevent the intrusion.

10. **What is a DDoS attack? how to prevent it**

    - A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.
    - **DDOS attack can be classified into two types:**
    - 1. **Flooding attacks:** In this type, the hacker sends a huge amount of traffic to the server which the server can not handle. And hence, the server stops functioning. This type of

attack is usually executed by using automated programs that continuously send packets to the server.

2. **Crash attacks:** In this type, the hackers exploit a bug on the server resulting in the system to crash and hence the server is not able to provide service to the clients.

- You can **prevent** DDOS attacks by using the following practices:
  - Use Anti-DDOS services
  - Configure Firewalls and Routers
  - Use Front-End Hardware
  - Use Load Balancing
  - Handle Spikes in Traffic

Network Security

11. **What is a proxy server?**

- A proxy server acts as an intermediary between a client and a server. It receives client requests, forwards them to the appropriate server, and then sends the server's response back to the client.

12. **Explain SSL/TLS.**

- Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols designed to provide secure communication over a computer network. TLS is the successor to SSL. They use encryption to ensure that data transferred between a client and a server is private.

13. **What is a honeypot?**

- A honeypot is a security mechanism that creates a virtual trap to lure attackers. It simulates vulnerabilities to attract and study hacking attempts. The primary purpose of a honeypot is to detect and analyze intrusions, understand attacker behavior, and develop defensive strategies.

14. **What is a man-in-the-middle attack? how to prevent it**

- A man-in-the-middle (MITM) attack occurs when an attacker secretly intercepts and possibly alters the communication between two parties who believe they are directly communicating with each other. This can allow the attacker to steal sensitive information, inject malicious data, or impersonate one of the parties.
- You can prevent MITM attack by using the following practices:
  - Use VPN
  - Use strong WEP/WPA encryption
  - Use Intrusion Detection Systems
  - Force HTTPS
  - Public Key Pair Based Authentication

15. **What is ARP spoofing?**

- ARP spoofing is a type of attack in which an attacker sends falsified ARP messages over a local network, The aim is to link the attacker’s MAC address with the IP address of a legitimate user.

- **ARP:** Address Resolution Protocol (ARP)is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.

16. **Explain the OSI model.**

- The OSI (Open Systems Interconnection) model is a conceptual framework used to understand and implement network protocols in seven layers:
    1. **Physical Layer:** Transmits raw bitstreams over a physical medium.
    2. **Data Link Layer:** Provides node-to-node data transfer and error detection.
    3. **Network Layer:** Handles routing and forwarding of data packets.
    4. **Transport Layer:** Ensures reliable data transfer with error recovery.
    5. **Session Layer:** Manages sessions and controls connections between computers.
    6. **Presentation Layer:** Translates data formats and encryption.
    7. **Application Layer:** Provides network services to applications.

17. **What is port scanning?**

- Port scanning is a method used to identify open ports and services available on a host, often used by attackers to find vulnerabilities.
- Administrators use Port Scanning to verify the security policies of the network.

18. **What are the common types of network attacks?**

- Common network attacks include:
    - **DDoS attacks:** Overwhelm a network or service with traffic.
    - **Man-in-the-Middle attacks:** Intercept and alter communications.
    - **ARP Spoofing:** Map an attacker’s MAC address to a legitimate IP address.
    - **DNS Spoofing:** Redirect traffic to malicious sites.
    - **SQL Injection:** Insert malicious SQL queries to access data.

19. **Explain MAC flooding.**

- MAC flooding is an attack that involves sending numerous packets to a switch, causing it to enter into a fail-open mode and forward packets to all ports.

20. **What is DNS spoofing?**

- DNS spoofing involves corrupting the DNS (Domain Name System) cache or responses to redirect traffic from legitimate websites to malicious ones. This can lead to phishing attacks, data theft, or spreading malware.

Application Security

21. **What is SQL injection? How to Prevent it?**

- SQL injection is a code injection technique that exploits a security vulnerability in an application’s software by injecting malicious SQL code into a query. This can allow attackers to view, modify, or delete database data, and in some cases, gain administrative control of the database.
    - Use prepared statements
    - Use Stored Procedures

        - Validate user input

22. **What is XSS (Cross-Site Scripting)? how to prevent it**

    - XSS is a security vulnerability that allows an attacker to inject malicious scripts into content from otherwise trusted websites.These scripts can be executed in the context of another user's session, potentially stealing cookies, session tokens, or other sensitive information.
    - You can prevent XSS attacks by using the following practices:
        - Validate user inputs
        - Sanitize user inputs
        - Encode special characters
        - Use Anti-XSS services/tools
        - Use XSS HTML Filter

23. **Explain CSRF (Cross-Site Request Forgery).**

    - CSRF is an attack that tricks a user into performing actions they did not intend to perform by exploiting the user's authenticated session. It forces a user to execute unwanted actions on a web application in which they are currently authenticated.

24. **What is input validation?**

    - Input validation is the practice of ensuring that a program operates on clean, correct, and useful data. It involves checking user input to prevent malicious data from being processed, which helps prevent many types of attacks such as SQL injection, XSS, and buffer overflows.

25. **What are the common security vulnerabilities in web applications?**

    - Common vulnerabilities include:
        - **SQL Injection:** Injecting malicious SQL code.
        - **Cross-Site Scripting (XSS):** Injecting malicious scripts.
        - **Cross-Site Request Forgery (CSRF):** Forcing user actions.
        - **Insecure Direct Object References:** Exposing internal objects.
        - **Security Misconfiguration:** Incorrectly configured settings.
        - **Sensitive Data Exposure:** Improper handling of sensitive data.

26. **What is session hijacking?**

    - Session hijacking is an attack where an attacker takes over a user session by obtaining the session ID. This allows the attacker to impersonate the user and access their data and functionalities on the application.

27. **What is a secure coding practice?**

    - Secure coding practices involve writing software with security in mind to prevent vulnerabilities, such as validating input, using secure functions, and managing sessions securely.

28. **What is OWASP?**

- The Open Web Application Security Project (OWASP) is a nonprofit organization focused on improving software security.
- OWASP produces freely available tools, documentation, and methodologies, including the widely recognized OWASP Top 10, which lists the most critical web application security risks.

29. **What are the OWASP Top 10?**

- The OWASP Top 10 is a standard awareness document for developers and web application security, representing a broad consensus about the most critical security risks to web applications:
    1. Injection
    2. Broken Authentication
    3. Sensitive Data Exposure
    4. XML External Entities (XXE)
    5. Broken Access Control
    6. Security Misconfiguration
    7. Cross-Site Scripting (XSS)
    8. Insecure Deserialization
    9. Using Components with Known Vulnerabilities
    10. Insufficient Logging and Monitoring

30. **Explain the principle of least privilege.**

- The principle of least privilege means giving users and systems the minimum levels of access—or permissions—necessary to perform their functions.
- By limiting access rights for users, applications, and systems to the bare minimum, the risk of malicious activities and accidental data breaches is reduced.

Endpoint Security

31. **What is antivirus software?**

- Antivirus software is a program designed to detect and remove malicious software, such as viruses, worms, and trojans.
- It scans files and systems for known malware signatures and behaviors, providing real-time protection and periodic scans to ensure system integrity.

32. **What is endpoint detection and response (EDR)?**

- EDR is a cybersecurity technology that monitors and responds to threats on endpoint devices in real-time. EDR solutions provide continuous monitoring and data collection, threat detection, and automated response and analysis capabilities to detect and mitigate advanced threats.

33. **Explain patch management.**

- Patch management is the process of managing a network of computers by regularly performing system updates, patches, and security fixes.

34. **What is malware?**

- Malware, short for malicious software, is software specifically designed to disrupt, damage, or gain unauthorized access to computer systems.
- Common types of malware include viruses, worms, trojans, ransomware, spyware, adware, and rootkits.

35. **What is ransomware?**

- Ransomware is a type of malware that encrypts a victim's files and demands payment to restore access.(usually in cryptocurrency).
- Ransomware attacks can result in significant downtime, data loss, and financial impact if the ransom is paid.

36. **What is spyware?**

- Spyware is software that secretly monitors and collects information about a user's activities without their knowledge or consent. It can capture sensitive data such as passwords, credit card numbers, and personal information.

37. **What is a rootkit?**

- A rootkit is a collection of software tools that enable an unauthorized user to gain control of a computer system without being detected.
- Rootkits are designed to hide their presence and can intercept and modify system calls, making them difficult to detect and remove.

38. **What is a zero-day exploit?**

- A zero-day exploit is a vulnerability in software that is unknown to the vendor and is exploited by attackers before the vendor has issued a fix.

39. **What is sandboxing?**

- Sandboxing is a security mechanism for separating running programs, often to execute untested code or untrusted applications in a controlled environment. By isolating applications in a sandbox, potential malware and exploits are contained and cannot affect the host system.

40. **What is endpoint security?**

- Endpoint security refers to securing end-user devices like desktops, laptops, and mobile devices from cyber threats.

Incident Response and Management

41. **What is incident response?**

- Incident response is a structured approach to handling security incidents, breaches, and cyber threats. The goal is to manage the situation to limit damage, reduce recovery time and costs, and prevent future incidents. It involves detecting, investigating, containing, eradicating, recovering from, and learning from incidents.

42. **Explain the steps of incident response.**

1. **Preparation:** Develop and implement incident response policies, procedures, and training.
2. **Identification:** Detect and determine if an incident has occurred.
3. **Containment:** Limit the impact of the incident by isolating affected systems.
4. **Eradication:** Remove the root cause of the incident and eliminate malicious components.
5. **Recovery:** Restore and validate system functionality, ensuring systems are clean.
6. **Lessons Learned:** Analyze the incident to improve response and prevent recurrence.

43. **What is a security incident?**

    - A security incident is any event that indicates a potential compromise of information integrity, availability, or confidentiality.

44. **What is a breach?**

    - A breach is an incident where data, applications, networks, or devices are accessed without authorization. Data breaches can lead to the exposure of sensitive information, financial loss, and damage to reputation.

45. **What is a security operations center (SOC)?**

    - A SOC is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture. The SOC is responsible for detecting, analyzing, and responding to cybersecurity incidents.

46. **What is a cyber threat?**

    - A cyber threat is any malicious act that seeks to damage data, steal data, or disrupt digital life in general.

47. **What is a vulnerability assessment?**

    - A vulnerability assessment is the process of identifying, quantifying, and prioritizing vulnerabilities in a system. It involves scanning and testing systems to find weaknesses that could be exploited by attackers.

48. **What is penetration testing?**

    - Penetration testing is a simulated cyber attack against your system to check for exploitable vulnerabilities. It involves attempting to breach various application systems (e.g., APIs, frontend/backend servers) to find and fix security flaws.

49. **What is the difference between vulnerability assessment and penetration testing?**

    - **Vulnerability assessment:** is the process of finding flaws on the target. Here, the organization knows that their system/network has flaws or weaknesses and want to find these flaws and prioritize the flaws for fixing.
    - **Penetration testing:** is the process of finding vulnerabilities on the target. In this case, the organization would have set up all the security measures they could think of and would want to test if there is any other way that their system/network can be hacked.

50. **What is a threat intelligence?**

- Threat intelligence is information about threats and threat actors that helps mitigate harmful events in cyberspace. It involves collecting, analyzing, and disseminating data on current and emerging threats to improve an organization's defenses and incident response capabilities.

Compliance and Standards

51. **What is GDPR?**

    - The General Data Protection Regulation (GDPR) is a regulation in European Union law on data protection and privacy for all individuals within the European Union.

52. **What is HIPAA?**

    - The Health Insurance Portability and Accountability Act (HIPAA) is a US law designed to provide privacy standards to protect patients' medical records and other health information. It mandates secure handling of patient data and patient rights to access their information

53. **What is PCI DSS?**

    - The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

54. **What is SOX?**

    - The Sarbanes-Oxley Act (SOX) is a US law that mandates certain practices in financial record keeping and reporting for corporations.

55. **What is ISO 27001?**

    - ISO/IEC 27001 is an international standard for managing information security.
    - It provides a framework for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS).
    - ISO 27001 helps organizations protect their information assets by implementing appropriate security controls.

56. **What is NIST?**

    - The National Institute of Standards and Technology (NIST) is a US federal agency that develops and promotes measurement standards and technology.
    - In the context of cybersecurity, NIST provides frameworks, guidelines, and best practices for improving cybersecurity posture and managing risks.

57. **What is a security policy?**

    - A security policy defines what is expected in terms of security for an organization. It outlines the rules and guidelines for employees, systems, and networks to ensure the security and integrity of data and resources.

58. **What is a risk assessment?**

    - A risk assessment is the process of identifying, analyzing, and evaluating risks.

59. **What is data protection?**

    - Data protection involves safeguarding important information from corruption, compromise, or loss. It involves:
    - **Confidentiality:** Ensuring that data is accessible only to authorized individuals.
    - **Integrity:** Maintaining the accuracy and consistency of data over its lifecycle.
    - **Availability:** Ensuring data is accessible and usable when needed.

60. *What is a security audit?**

    - A security audit is a systematic evaluation of an organization's information systems, policies, and procedures to assess security vulnerabilities and compliance with security standards and regulations. It helps identify weaknesses, gaps, and areas for improvement in the organization's security posture.
    - Types of audits include:

1. **Security Audit:** Evaluates the effectiveness of an organization's security policies and controls.
2. **Compliance Audit:** Ensures adherence to regulatory requirements and standards (e.g., GDPR, PCI DSS).
3. **Internal Audit:** Conducted by an organization's internal auditors.
4. **External Audit:** Conducted by independent third-party auditors.

Advanced Concepts

61. **What is the principle of defense-in-depth?**

    - Defense-in-depth is a cybersecurity strategy that employs multiple layers of security controls and mechanisms to protect systems and data. By using a combination of preventive, detective, and corrective controls at different layers, organizations can increase the overall security posture and resilience against attacks.

62. **What is digital signature?**

    - A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital message, document, or software. It provides non-repudiation, ensuring that the sender cannot deny sending the message and that the message content has not been altered.

63. **What is hashing?**

    - Hashing is the process of converting data (of any size) into a fixed-size string of characters (hash value) using a mathematical algorithm. Hash functions are used in data integrity verification, password storage, and digital signatures.

64. **Explain the difference between hashing and encryption.**

    - **Hashing:** One-way function that converts data into a fixed-size string (hash value). It is used for data integrity verification and password storage. Hashing is irreversible.
    - **Encryption:** Two-way process that converts data (plaintext) into an unreadable form (ciphertext) using an encryption algorithm and a key. Encryption is reversible with the correct

decryption key.
- **Both Encryption and Hashing are used to convert readable data into an unreadable format. The difference is that the encrypted data can be converted back to original data by the process of decryption, but the hashed data cannot be converted back to original data.**

65. **What is a certificate authority (CA)?**

- A certificate authority is a trusted entity that issues digital certificates used to verify the identity of individuals, organizations, and devices on the internet. CAs validate the identity of the certificate holder and sign the certificate to establish trust in the certificate's authenticity.

66. **What is a digital certificate?**

- A digital certificate is an electronic document that binds a public key to an identity, verifying the authenticity of the public key holder. It is issued by a certificate authority (CA) and used to establish secure communications and verify the identity of websites, individuals, or organizations.

67. **What is multi-factor authentication (MFA)?**

- MFA is a security system that requires more than one method of authentication to verify the user's identity.
- in access to a resource, such as a system, network, or application. The factors typically include something the user knows (e.g., password), something the user has (e.g., security token), or something the user is (e.g., biometric verification). MFA enhances security by adding an extra layer of protection against unauthorized access, even if one factor (e.g., password) is compromised.

68. **What is network segmentation?**

- Network segmentation involves splitting a computer network into subnetworks, each being a network segment, to enhance security.

69. **What is social engineering?**

- Social engineering is a technique used by attackers to manipulate individuals into confidential information, performing actions, or compromising security. It relies on psychological manipulation and often exploits human emotions, trust, or curiosity to deceive targets into revealing sensitive information or performing actions that benefit the attacker.

70. **What is a security token?**

- A security token is a physical device or digital token used to authenticate a person’s identity electronically.

Emerging Threats and Technologies

71. **What is cloud security?**

- Cloud security involves a set of policies, controls, procedures, and technologies that work together to protect cloud-based systems, data, and infrastructure.

72. **What is DevSecOps?**

- DevSecOps is an approach to culture, automation, and platform design that integrates security as a shared responsibility throughout the entire IT lifecycle.

73. **What is a security incident response plan?**

- A security incident response plan is a documented set of procedures and guidelines for responding to and managing security incidents effectively. It outlines the roles and responsibilities of incident response team members, steps for detecting and containing incidents, communication protocols, and strategies for minimizing damage and restoring normal operations.

74. **What is a data breach response plan?**

- A data breach response plan is a specific type of incident response plan that focuses on managing and mitigating the impact of a data breach. It includes procedures for identifying the breach, containing the incident, assessing the scope and impact, notifying affected parties (e.g., customers, regulators), and implementing measures to prevent future breaches.

75. **What is threat modeling?**

- Threat modeling is a structured approach to identifying and evaluating potential security threats and vulnerabilities in an application, system, or network. It involves analyzing the system's architecture, components, and potential attack vectors to prioritize security controls and mitigation strategies. Threat modeling helps organizations proactively design and build security into their systems.

76. **What is a denial-of-service (DoS) attack?**

- A denial-of-service (DoS) attack is an attempt to make a computer resource unavailable to its intended users by overwhelming the target system with a flood of illegitimate requests or traffic. This can result in service disruption, making the system slow, unresponsive, or completely unavailable to legitimate users.

77. **What is threat hunting?**

- Threat hunting is the proactive search for malware or attackers that are lurking in a network without the knowledge of the organization's security team.

78. **What is a botnet?**

- A botnet is a network of private computers infected with malicious software and controlled as a group without the owners' knowledge.

79. **What is an insider threat?**

- An insider threat is a security risk that comes from within the organization, such as employees or contractors who have access to sensitive data.

80. **What is biometric security?**
    - Biometric security involves using unique biological characteristics, such as fingerprints, facial recognition, or iris scans, to verify identity.

Security Tools and Technologies

81. **What is Wireshark?**
    - Wireshark is a network protocol analyzer that captures and interactively analyzes network traffic.
82. **What is Metasploit?**
    - Metasploit is a penetration testing framework that helps security professionals find, exploit, and validate vulnerabilities.
83. **What is Snort?**
    - Snort is an open-source network intrusion detection system (NIDS) capable of performing real-time traffic analysis and packet logging.
84. **What is Nessus?**
    - Nessus is a vulnerability scanner used to identify vulnerabilities, configuration issues, and malware.
    - Nessus is a widely used vulnerability scanner that identifies security vulnerabilities, misconfigurations, and malware on systems, networks, and applications. It performs automated scans and provides detailed reports to help organizations prioritize and remediate security risks.
85. **What is Burp Suite?**
    - Burp Suite is a web vulnerability scanner and testing tool used for web application security testing. It helps identify and exploit security vulnerabilities such as SQL injection, XSS, and CSRF in web applications by simulating attacks and assessing their impact.
86. **What is Splunk?**
    - Splunk is a platform for searching, monitoring, and analyzing machine-generated big data via a web-style interface.
87. **What is Kali Linux?**
    - Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing.
88. **What is Nmap?**
    - Nmap (Network Mapper) is a network scanning tool used to discover hosts and services on a computer network.
89. **What is a SIEM system?**

- A Security Information and Event Management (SIEM) system is a comprehensive security solution that aggregates and analyzes log data and security events from across an organization's IT infrastructure. It provides real-time monitoring, threat detection, incident response, and compliance reporting capabilities.

90. **What is a vulnerability scanner?**

    - A vulnerability scanner is a software tool used to detect vulnerabilities in computers, networks, or applications.

Security Best Practices

91. **What is a security baseline?**

    - A security baseline is a set of basic security objectives that must be met to ensure a minimum level of security across the organization.

92. **What is a security assessment?**

    - A security assessment is the process of identifying and evaluating risks to the organization's information assets.

93. **What is security awareness training?**

    - Security awareness training is a formal process for educating employees about computer security.

94. **What is a security audit?**

    - A security audit is a comprehensive assessment of an organization's information system to ensure compliance with security policies and procedures.

95. **What is a disaster recovery plan?**

    - A disaster recovery plan is a documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster.

96. **What is a security framework?**

    - A security framework is a structured set of guidelines that outlines how an organization can manage its information security risk and improve its security posture.

97. **What is encryption at rest?**

    - Encryption at rest is the practice of encrypting data stored on disk or other storage devices to protect it from unauthorized access. It ensures that data remains encrypted and unreadable to anyone without the correct decryption key, even if physical access to the storage device is gained.

98. **What is encryption in transit?**

    - Encryption in transit is the process of encrypting data as it is transmitted between devices or across networks. It protects data from being intercepted and read by unauthorized parties

during transmission, ensuring data confidentiality and integrity.

99. **What is a password policy?**
    - A password policy is a set of rules designed to enhance security by encouraging users to create secure passwords and use them properly.

100. **What is phishing? how to prevent it?** - Phishing is a type of social engineering attack where attackers impersonate legitimate entities (e.g., companies, colleagues) to deceive individuals into providing sensitive information, such as login credentials, credit card numbers, or personal details. Phishing attacks are commonly delivered via email, text messages, or malicious websites.
    - Don't enter sensitive information in the webpages that you don't trust
    - Verify the site's security
    - Use Firewalls
    - Use AntiVirus Software that has Internet Security
    - Use Anti-Phishing Toolbar

101. **What is the difference between a vulnerability, threat, and risk?**

- **Vulnerability:** Weakness in a system that can be exploited by a potential hacker
- **Threat:** Someone with the potential to harm a system or an organization
- **Risk:** the potential for loss or damage when a threat exploits a vulnerability.

102. **What are the different types of hackers?**

- **White Hat:** Ethical hackers; Authorized testing
    - White hat hackers use their powers for good deeds and so they are also called Ethical Hackers.These are mostly hired by companies as a security specialist that attempts to find and fix vulnerabilities and security holes in the systems. They use their skills to help make the security better.
- **Black Hat:** Malicious hackers; Illegal hacking
    - Black hat hackers are known for having vast knowledge about breaking into computer networks. They can write malware which can be used to gain access to these systems. This type of hackers misuse their skills to steal information or use the hacked system for malicious purpose.
- **Gray Hat:** Hackers with ambiguous ethics; May violate laws or ethical standards without malicious intent
    - They look for system vulnerabilities without the owner's permission. If they find any vulnerabilities, they report it to the owner. Unlike Black hat hackers, they do not exploit the vulnerabilities found.

103. **What is the difference between TCP and UDP?**

- **TCP (Transmission Control Protocol)**
    - **Connection-Oriented:** Establishes a connection before data transfer.
    - **Reliable:** Ensures delivery, order, and error correction.
    - **Flow & Congestion Control:** Manages data rate and network congestion.
    - **Higher Overhead:** More complex due to reliability features.
    - **Use Cases:** Web browsing, email, file transfers.

- **UDP (User Datagram Protocol)**
  - **Connectionless:** Sends data without establishing a connection.
  - **Unreliable:** No guarantee of delivery, order, or error correction.
  - **No Flow or Congestion Control:** Transmits data as-is.
  - **Low Overhead:** Simpler and faster due to lack of reliability features.
  - **Use Cases:** Live streaming, online gaming, VoIP, DNS queries.

104. **What are the differences between a stateful and stateless firewall?**

- **Stateful Firewall**
  - **Tracks Connections**: Monitors and maintains the state of active connections.
  - **Context-Aware**: Makes decisions based on the entire traffic flow.
  - **Higher Security**: Provides detailed analysis and better protection.
  - **Complex**: More resource-intensive and can be slower.
  - **Use Cases**: High-security environments like corporate networks and data centers.
- **Stateless Firewall**
  - **No Connection Tracking**: Evaluates each packet independently.
  - **Rule-Based**: Decisions are made based on predefined rules (IP, port, protocol).
  - **Basic Security**: Less granular control compared to stateful firewalls.
  - **Simple**: Faster and less resource-intensive.
  - **Use Cases**: Smaller, simpler networks where high performance is prioritized.

105. **What is a DMZ in network security?**

- A DMZ (Demilitarized Zone) in network security is a subnetwork that provides an additional layer of protection by isolating external-facing services (like web servers) from an organization's internal network

106. **What are the differences between HTTP and HTTPS?**

- **HTTP (HyperText Transfer Protocol)**
  - **Unencrypted**: Data transferred is in plain text.
  - **Less Secure**: Vulnerable to eavesdropping and man-in-the-middle attacks.
  - **Port**: Uses port 80 by default.
  - **Use Cases**: Suitable for non-sensitive information where security is not a primary concern.
- **HTTPS (HyperText Transfer Protocol Secure)**
  - **Encrypted**: Data is encrypted using SSL/TLS, providing confidentiality and integrity.
  - **More Secure**: Protects against eavesdropping, man-in-the-middle attacks, and tampering.
  - **Port**: Uses port 443 by default.
  - **Use Cases**: Essential for sensitive information like login credentials, payment transactions, and personal data.

107. **What is public key infrastructure (PKI)?**

- Public Key Infrastructure (PKI) is a framework that uses cryptographic keys and digital certificates to secure communications and authenticate identities over networks.
- **Key Components:**

    - **Digital Certificates**: Bind a public key to an entity's identity.
    - **Certificate Authority (CA)**: Issues and manages digital certificates.
    - **Registration Authority (RA)**: Verifies identities before certificates are issued.
    - **Public and Private Keys**: Used for encrypting, decrypting, and signing data.
    - **Certificate Revocation List (CRL)**: Lists invalidated certificates.

- **Benefits:**

    - **Confidentiality**: Protects data from unauthorized access.
    - **Integrity**: Ensures data has not been tampered with.
    - **Authentication**: Verifies the identity of users and devices.
    - **Non-repudiation**: Ensures actions cannot be denied after the fact.

108. **Explain what PGP is and how it works.**

- Pretty Good Privacy: Encryption program for secure email communication using asymmetric encryption.

109. **Explain what a Trojan horse is.**

- Malicious software disguised as legitimate software to trick users into installing it.

110. **What is a worm in cybersecurity?**

- Self-replicating malware that spreads across networks without human intervention.

111. **What is a red team/blue team exercise?**

- Red team simulates attacks, blue team defends; used to test and improve security.

112. **Explain what log management is.**

- Collecting, storing, and analyzing log data for security monitoring and compliance.

113. **What is data loss prevention (DLP)?**

- Technologies and strategies to prevent sensitive data from being lost, stolen, or misused.

114. **What is a buffer overflow?**

- A vulnerability where a program writes more data to a buffer than it can hold, potentially leading to arbitrary code execution.

115. **What are the best practices for securing web applications?**

- Regular updates, input validation, secure coding practices, WAFs, and following the OWASP Top 10 guidelines.

Identity and Access Management

116. **What is IAM (Identity and Access Management)?**

- Framework for managing digital identities and controlling access to resources.

117. **What is the difference between authentication and authorization?**

- **Authentication:** Verifying identity;
- **Authorization:** Granting access to resources based on identity.

118. **What is SSO (Single Sign-On)?**

- A user authentication process that allows access to multiple applications with one set of login credentials.

119. **What is LDAP, and how is it used?**

- Lightweight Directory Access Protocol: Used to access and manage directory information services.

120. **Explain what OAuth is.**

- Open authorization framework allowing third-party applications to access user resources without sharing credentials.

121. **What are the principles of access control?**

- Policies, procedures, and technologies to manage who can access resources and under what conditions.

122. **What is a privilege escalation?**

- Exploiting a vulnerability to gain higher access privileges than intended.

123. **What is AAA in Cyber Security?**

    - AAA stands for Authentication, Authorization, and Accounting. It is a framework used to control access to computer resources, enforce policies, and audit usage.

        - **Authentication:** Verifies the identity of a user or device.
        - **Authorization:** Determines the permissions and access levels for authenticated users.
        - **Accounting:** Tracks user activities and resource usage for auditing and reporting purposes.

124. **Can you explain the difference between Authentication and Authorization?**

    - **Authentication** is the process of verifying the identity of a user or device. It answers the question, "Who are you?" Common methods include passwords, biometrics, and security tokens.
    - **Authorization** is the process of determining what an authenticated user is allowed to do. It answers the question, "What can you do?" This involves setting permissions and access controls.

125. **What are some common authentication methods used in cybersecurity?**

    - **Passwords/PINs:** The most basic form of authentication.
    - **Biometric Authentication:** Fingerprints, facial recognition, retina scans.
    - **Two-Factor Authentication (2FA):** Combines something you know (password) with something you have (mobile phone).

- **Multi-Factor Authentication (MFA):** Uses two or more different factors to verify identity.
- **Smart Cards:** Physical cards embedded with chips that store authentication data.
- **Security Tokens:** Physical devices that generate authentication codes.

126. **What is Cryptography?**

- Cryptography is the practice and study of techniques for securing information and communication mainly to protect the data from third parties that the data is not intended for.

127. **What are the response codes that can be received from a Web Application?**

- 1xx : Informational responses
- 2xx : Success
- 3xx : Redirection
- 4xx : Client-side Error
- 5xx : Server-side Error

128. **What is traceroute? Why is it used?**

- Traceroute is a tool that shows the path of a packet. It lists all the points (mainly routers) that the packet passes through. This is used mostly when the packet is not reaching its destination. Traceroute is used to check where the connection stops or breaks to identify the point of failure.

129. **What is the difference between HIDS and NIDS?**

- HIDS(Host IDS) and NIDS(Network IDS) are both Intrusion Detection System and work for the same purpose i.e., to detect the intrusions. The only difference is that the HIDS is set up on a particular host/device. It monitors the traffic of a particular device and suspicious system activities. On the other hand, NIDS is set up on a network. It monitors traffic of all device of the network.

130. **What are the steps to set up a firewall?**

1. **Username/password:** modify the default password for a firewall device
2. **Remote administration:** Disable the feature of the remote administration
3. **Port fotwarding:** Configure appropriate port forwarding for certain applications to work properly, such as a web server or FTP server
4. **DHCP server:** Installing a firewall on a network with an existing DHCP server will cause conflict unless the firewall's DHCP is disabled
5. **Logging:** To troubleshoot firewall issues or potential attacks, ensure that logging is enabled and understand how to view logs
6. **Policies:** You should have solid security policies in place and make sure that the firewall is configured to enforce those policies.

131. **Explain SSL Encryption**

- SSL(Secure Sockets Layer) is the industry-standard security technology creating encrypted connections between Web Server and a Browser. This is used to maintain data privacy and to protect the information in online transactions. The steps for establishing an SSL connection is as follows:

1. A browser tries to connect to the webserver secured with SSL
2. The browser sends a copy of its SSL certificate to the browser
3. The browser checks if the SSL certificate is trustworthy or not. If it is trustworthy,then the browser sends a message to the web server requesting to establish an encrypted connection
4. The web server sends an acknowledgment to start an SSL encrypted connection
5. SSL encrypted communication takes place between the browser and the web server

132. **What steps will you take to secure a server?**

- Secure servers use the Secure Sockets Layer (SSL) protocol for data encryption and decryption to protect data from unauthorized interception.

  Step 1: Make sure you have a secure password for your root and administrator users

  Step 2: The next thing you need to do is make new users on your system. These will be the users you use to manage the system

  Step 3: Remove remote access from the default root/administrator accounts

  Step 4: The next step is to configure your firewall rules for remote access

133. **Explain Data Leakage/Loss**

- Data Leakage is an intentional or unintentional transmission of data from within the organization to an external unauthorized destination. It is the disclosure of confidential information to an unauthorized entity. Data Leakage can be divided into 3 categories based on how it happens:
  1. **Accidental Breach:** An entity unintentionally send data to an unauthorized person due to a fault or a blunder
  2. **Intentional Breach:** The authorized entity sends data to an unauthorized entity on purpose
  3. **System Hack:** Hacking techniques are used to cause data leakage

134. **What is a Brute Force Attack? How can you prevent it?**

- Brute Force is a way of finding out the right credentials by repetitively trying all the permutations and combinations of possible credentials. In most cases, brute force attacks are automated where the tool/software automatically tries to login with a list of credentials. There are various ways to prevent Brute Force attacks. Some of them are:
  - **Password Length:** You can set a minimum length for password. The lengthier the password, the harder it is to find.
  - **Password Complexity:** Including different formats of characters in the password makes brute force attacks harder. Using alpha-numeric passwords along with special characters, and upper and lower case characters increase the password complexity making it difficult to be cracked.
  - **Limiting Login Attempts:** Set a limit on login failures. For example, you can set the limit on login failures as 3. So, when there are 3 consecutive login failures, restrict the user from logging in for some time, or send an Email or OTP to use to log in the next time.

Because brute force is an automated process, limiting login attempts will break the brute force process.

135. **How would you reset a password-protected BIOS configuration?**

- Since BIOS is a pre-boot system it has its own storage mechanism for settings and preferences. A simple way to reset is by popping out the CMOS battery so that the memory storing the settings lose its power supply and as a result, it will lose its setting.

136. **What is port blocking within LAN?**

- Restricting the users from accessing a set of services within the local area network is called port blocking.
- Stopping the source to not to access the destination node via ports. As the application works on the ports, so ports are blocked to restricts the access filling up the security holes in the network infrastructure.

137. **What are salted hashes?**

- Salt is a random data. When a properly protected password system receives a new password, it creates a hash value of that password, a random salt value, and then combined value is stored in its database. This helps to defend against dictionary attacks and known hash attacks.
- **Example:** If someone uses the same password on two different systems and they are being used using the same hashing algorithm, the hash value would be same, however, if even one of the system uses salt with the hashes, the value will be different.

💖 Thank You 💖
