CYBERSECURITY INTERVIEW QUESTIONS BASED ON NETWORKING

VAISHALI SHISHODIA

NETWORKING BASED INTERVIEW QUESTIONS ANSWERS FOR CYBERSECURITY

---

1. What is the OSI model, and why is it important in networking and cybersecurity?

Answer: The OSI (Open Systems Interconnection) model is a conceptual framework used to understand and describe network communications in seven layers:

1. **Physical**: Deals with hardware and physical transmission media.
2. **Data Link**: Ensures error-free transmission over the physical layer.
3. **Network**: Manages data routing, switching, and addressing (e.g., IP addresses).
4. **Transport**: Ensures reliable data transfer (e.g., TCP, UDP).
5. **Session**: Manages sessions between applications.
6. **Presentation**: Deals with data translation and encryption.
7. **Application**: Provides network services to end-user applications.

It's important for cybersecurity because it helps professionals understand where vulnerabilities can exist and where to apply security measures.

---

2. What is an IP address and what role does it play in networking?

Answer: An IP (Internet Protocol) address is a unique numerical identifier assigned to each device on a network. It serves two main purposes:

- Identifying the host or network interface.
- Providing the location of the device in the network, facilitating communication between devices.

In cybersecurity, IP addresses are vital for traffic monitoring, access control, and blocking malicious actors.

---

3. What is DNS, and how does it work in networking?

Answer: DNS (Domain Name System) translates human-readable domain names (like www.example.com) into IP addresses. When you type a website address, your computer queries a DNS server to resolve the domain into an IP address, allowing your device to access the website.

In cybersecurity, attackers can exploit DNS vulnerabilities (e.g., DNS poisoning), so securing DNS is crucial.

---

4. What is DHCP, and what does it do?

Answer: DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses to devices on a network. It eliminates the need for manual configuration by dynamically distributing IP addresses within a specified range.

In cybersecurity, improper DHCP configuration can lead to issues like IP spoofing or unauthorized network access.

---

5. What is a VPN, and how does it enhance network security?

Answer: A VPN (Virtual Private Network) creates an encrypted connection between a user's device and a network, ensuring secure data transmission over potentially untrusted networks (e.g., the internet). It helps maintain confidentiality and integrity by masking the user's real IP address.

VPNs are used for securing remote work, bypassing georestrictions, and protecting sensitive data from man-in-the-middle attacks.

---

6. What is ARP, and how is it used in networking?

Answer: ARP (Address Resolution Protocol) maps a device's IP address to its MAC (Media Access Control) address on a local network. ARP helps devices identify the physical address of other devices in the same local network.

ARP spoofing or poisoning is a common attack where attackers send falsified ARP messages to redirect network traffic.

---

7. What is port scanning, and why is it important in cybersecurity?

Answer: Port scanning involves probing a device or network to identify open ports and services. It's a technique used by attackers to find vulnerabilities (e.g., services that can be exploited). However, it's also used by security professionals to identify weaknesses in their systems.

---

8. What is the difference between TCP and UDP?

Answer: TCP (Transmission Control Protocol) is a connection-oriented protocol that ensures reliable delivery of data by establishing a connection before transmission and checking for errors. UDP (User Datagram Protocol) is connectionless, faster, but less reliable because it doesn't guarantee delivery or check for errors.

In cybersecurity, TCP is used when data integrity is crucial (e.g., file transfers), and UDP is used for faster applications where speed is a priority (e.g., live streaming).

---

9. What is a firewall, and how does it work?

Answer: A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It can block malicious traffic, prevent unauthorized access, and protect against cyberattacks.

---

10. What is the difference between a switch and a router?

Answer:

- **Switch**: A device that connects multiple devices within the same network and uses MAC addresses to forward data.
- **Router**: A device that connects different networks and forwards data between them using IP addresses.

Routers are used for routing traffic between networks, while switches operate within a network to direct traffic.

---

11. What is encryption, and why is it important?

Answer: Encryption is the process of converting data into an unreadable format to prevent unauthorized access. It ensures that sensitive data (e.g., passwords, credit card numbers) is secure during transmission or storage.

Encryption is vital in cybersecurity to maintain confidentiality and protect data from being intercepted.

---

12. What is subnetting, and why is it useful in networking?

Answer: Subnetting divides a large network into smaller, more manageable sub-networks (subnets). It helps in organizing networks efficiently, improving performance, and enhancing security by segmenting traffic.

Subnetting reduces congestion, controls traffic flow, and can limit the impact of attacks to a smaller part of the network.

---

13. What are the different types of networks (LAN, WAN, etc.)?

Answer:

- **LAN (Local Area Network)**: A network covering a small geographical area (e.g., a home or office).
- **WAN (Wide Area Network)**: A network covering a large geographical area, often connecting multiple LANs (e.g., the internet).
- **MAN (Metropolitan Area Network)**: A network that covers a city or large campus.
- **PAN (Personal Area Network)**: A network for personal devices within a short range.

---

14. What are ACLs (Access Control Lists), and how do they work?

Answer: ACLs are used to filter network traffic by defining rules that allow or deny traffic based on parameters such as IP address, protocol type, or port number. They are used in routers and firewalls to control access to resources.

---

15. What is a WAF (Web Application Firewall)?

Answer: A WAF protects web applications by filtering and monitoring HTTP traffic between the web server and the internet. It can defend against attacks such as SQL injection, cross-site scripting (XSS), and other web-based threats.

---

16. What is a proxy server, and how does it improve security?

Answer: A proxy server acts as an intermediary between a user's device and the internet. It can hide the user's IP address, cache data for faster access, and filter harmful content or malicious requests, providing an extra layer of security.

---

17. What is the CIA triad in cybersecurity?

Answer: The CIA triad stands for **Confidentiality**, **Integrity**, and **Availability**. These are the three core principles of cybersecurity:

- **Confidentiality** ensures that sensitive information is kept private.
- **Integrity** ensures that data is accurate and not tampered with.
- **Availability** ensures that authorized users can access data and resources when needed.

---

18. How does antivirus software help protect a network?

Answer: Antivirus software detects, prevents, and removes malware (viruses, worms, Trojans) from a device. It helps protect against malicious software that can compromise data integrity and system functionality.

---

19. What does AAA stand for in networking, and how does it function?

Answer: AAA stands for **Authentication**, **Authorization**, and **Accounting**. It's a framework for managing access control:

- **Authentication** verifies the identity of users or devices.
- **Authorization** defines what resources users can access.
- **Accounting** tracks user activity and resource usage.

AAA is often used in VPNs, routers, and network devices to secure access and monitor usage.

---

20. What is the difference between encoding and hashing?

Answer:

- **Encoding** is the process of converting data into a different format to ensure it can be properly transmitted or stored. It's reversible (e.g., Base64).
- **Hashing** is a one-way transformation of data into a fixed-length value. It's used to ensure data integrity (e.g., passwords stored as hashes). Hashing cannot be reversed.
