

20. What are the roles of SSL/TLS in network security?

- are cryptographic protocols that provide three key security services for network communications.
- protects data in transit from interception and eavesdropping
- verifies the identity of servers to prevent impersonation
- prevents data tampering during transmission by using MAC.

21. What is OS hardening? Name a few techniques.

- process of securing a system by reducing its surface.
- disabling unnecessary services.
- configuring a host-based firewall.
- Implementing access controls.

22. How do you secure Linux server?

- Regularly apply security patches
- Detects potential security issues.

23. What is the Windows Security event log and what are the key events to monitor?

- login attempts and file access, based on system's audit policies.
- Event ID 4728, 4732, 4625, 4756.

24. What is sandboxing in cybersecurity?

- security mechanism that isolates application or system from the rest of the network, preventing potential malware.

25. How would you protect an application from SQL injection?

- parameterized queries.

35. What is a buffer overflow attack?

→ When a program attempts to write more data into a memory block than it can hold.

41. What are the top OWASP vulnerabilities?

→ SQL injection, broken authentication, XSS.

50. What's the purpose of an incident response plan?

→ outlines procedures for responding to security incidents; aims to ensure that all legal and compliance requirements are met following a breach.