Security Fundamentals - Interview Preparation Canvas

---

1. Firewalls, IDS/IPS

Concept Explanation: - Firewall: Controls inbound/outbound traffic based on rules - Stateful: tracks connection state - Stateless: filters based only on IP/port - IDS (Intrusion Detection System): Monitors and alerts on suspicious activity - IPS (Intrusion Prevention System): Detects and blocks malicious activity

Interview Answer: "Firewalls enforce network traffic rules; IDS monitors and alerts on threats, while IPS can actively block threats. Stateful firewalls track connection state, whereas stateless do not."

Delivery Example: "I would say: 'Firewalls control network traffic; stateful firewalls track the connection state for security, while stateless firewalls filter packets without context. IDS alerts me of suspicious activity, and IPS can block attacks in real-time.'"

---

2. VPN Types: SSL, IPSec, L2TP

Concept Explanation: - SSL VPN: Secure remote access via browser or client - IPSec VPN: Secure site-to-site or client-to-site connection - L2TP: Tunnels Layer 2 traffic, often combined with IPSec

Interview Answer: "VPNs provide secure communication. SSL is client/browser based, IPSec is for encrypted site-to-site connections, and L2TP tunnels Layer 2 traffic securely."

Delivery Example: "I would explain: 'SSL VPN allows secure remote access from a browser, IPSec VPN is used to securely connect different sites, and L2TP tunnels data securely over the network, often with IPSec encryption.'"

---

3. User Authentication: MFA, SSO

Concept Explanation: - MFA: Multi-factor authentication, combines password + token/device/biometrics - SSO: Single Sign-On, one login grants access to multiple systems

Interview Answer: "MFA strengthens security by requiring multiple forms of verification, while SSO improves user convenience by allowing one login for multiple services."

Delivery Example: "I would say: 'MFA adds layers of verification like password plus OTP, making accounts more secure. SSO allows users to access multiple applications with a single login, improving usability.'"

---

4. Patching and Updates

Concept Explanation: - Regular updates to OS and software to fix vulnerabilities - Reduces risk of exploits and malware

Interview Answer: "Patching and updates are crucial for maintaining system security by fixing vulnerabilities and reducing the risk of attacks."

Delivery Example: "I would explain: 'I regularly apply security patches to OS and applications to prevent vulnerabilities from being exploited by attackers.'"

---

5. Antivirus & Endpoint Security

Concept Explanation: - Protects devices from malware, ransomware, and other threats - Endpoint security includes antivirus, firewalls, and EDR

Interview Answer: "Antivirus and endpoint security protect systems from malware, monitor endpoints, and help in detecting and responding to threats."

Delivery Example: "I would say: 'I deploy antivirus and endpoint security solutions to protect devices from malware, monitor for suspicious activity, and respond to threats proactively.'"

---

6. Basic Threat Awareness

Concept Explanation: - Understanding malware, phishing, social engineering, ransomware - Recognizing suspicious activities and behaviors

Interview Answer: "Basic threat awareness involves knowing different types of attacks and being able to identify and mitigate them."

Delivery Example: "I would explain: 'I stay aware of common threats like phishing and ransomware, recognize suspicious patterns, and follow security best practices to mitigate risks.'"

Example Questions & Scenario Responses:

Q1: Difference between stateful and stateless firewall? - Stateful: tracks connection state, makes context-aware decisions - Stateless: no context, filters per packet - Delivery: 'Stateful firewalls maintain the state of active connections and allow return traffic, while stateless firewalls filter each packet individually without context.'

Q2: MFA importance? - Provides extra security beyond passwords - Delivery: 'MFA ensures that even if a password is compromised, attackers cannot access accounts without the second factor, enhancing security.'

Q3: VPN types and use cases? - SSL: remote user access - IPSec: site-to-site secure connection - L2TP/IPSec: secure tunneling - Delivery: 'SSL VPNs allow remote users to connect via browser, IPSec secures communication between sites, and L2TP with IPSec provides Layer 2 tunneling securely.'

Scenario 1: Unauthorized access detected - Steps: Check logs, identify source, isolate system, reset credentials, monitor for further access - Delivery: 'I would review server logs to identify the source, isolate affected accounts or systems, reset credentials, and monitor for additional unauthorized attempts.'

Scenario 2: Ransomware detected - Steps: Isolate workstation, stop spreading, backup, scan, restore, investigate - Delivery: 'I would immediately disconnect the workstation from the network, prevent further spread, backup critical data, scan for malware, restore systems from clean backups, and investigate the source.'

Scenario 3: Configure firewall rules - Allow HTTP (port 80), block FTP (port 21) - Delivery: 'I would create a rule allowing TCP port 80 for HTTP traffic and another rule to block TCP port 21 for FTP, ensuring proper firewall rule order and testing connectivity.'