## **Practice Q&A (Tutorial-Based)**

### **📝 Short Answer:**

1. **Why is WPA more secure than WEP?** ➤ Uses stronger encryption (TKIP), longer IV, MIC for integrity, and 802.1X for authentication.
2. **Why doesn't EAPOL define a fixed authentication method?** ➤ It supports many (TLS, PEAP, EAP-MD5), allowing flexibility.
3. **What’s the role of 802.11i?** ➤ It’s the full wireless security standard; WPA is a subset.
4. **Does 802.11 require Mobile IP?** ➤ No, 802.11 handles local wireless, not global IP mobility.
5. **Can a connection be wireless and mobile?** ➤ Yes. Wireless = no wires; Mobile = roaming between locations.

## **✅ 4. Active Recall Exercises**

### **❓ MCQs**

1. What does a stateless firewall lack?  
   * a) Port filtering
   * b) IP filtering
   * c) Session awareness ✅
   * d) Logging
2. What attack does ICMP flooding target?  
   * a) Integrity
   * b) Availability ✅
   * c) Confidentiality
   * d) Authenticity
3. Which of the following is NOT a type of malware?  
   * a) Worm
   * b) Botnet
   * c) Trojan
   * d) DHCP ✅

### **✍️ Fill in the Blanks**

1. Intrusion detection systems can be **misuse-based** or **anomaly-based**.
2. A **DMZ** separates the external network from the internal protected network.
3. **UDP amplification** is an attack that exploits stateless servers like DNS or NTP.

### **💡 Short Answers**

1. **What makes anomaly detection valuable in IDS/IPS?** ➤ Detects new, unknown attacks not seen in signature databases.
2. **How does an IPS block an SQL Injection?** ➤ Detects and blocks known malicious query patterns in real-time.
3. **Why should firewalls limit UDP traffic?** ➤ To prevent amplification attacks which flood the victim with forged replies.