IPSec Practice Questions - MCQs, SAQs, and Evaluation Questions

Section A: Multiple Choice Questions (MCQs)

A1. Internet Protocol Fundamentals

1. What is the minimum header length for an IPv4 packet? a) 16 bytes b) 20 bytes c) 24 bytes d) 32 bytes

Answer: b) 20 bytes *Explanation: Header Length field minimum value is 5, representing 5 × 32-bit words = 20 bytes*

2. Which field in the IPv4 header prevents infinite packet loops? a) Fragment Offset b) Time to Live (TTL) c) Header Checksum d) Protocol

Answer: b) Time to Live (TTL) *Explanation: TTL decrements at each hop; packet discarded when TTL reaches zero*

3. What is the maximum value for IPv4 Total Length field? a) 1,500 bytes b) 32,767 bytes c) 65,535 bytes d) 4,294,967,295 bytes

Answer: c) 65,535 bytes *Explanation: Total Length is 16 bits, so maximum value is 2^16 - 1 = 65,535*

4. IPv6 addresses are how many bits long? a) 32 bits b) 64 bits c) 96 bits d) 128 bits

Answer: d) 128 bits *Explanation: IPv6 uses 128-bit addresses to provide vastly expanded address space*

5. Which protocol value in IPv4 header indicates TCP? a) 1 b) 6 c) 17 d) 89

Answer: b) 6 *Explanation: TCP protocol number is 6, UDP is 17, ICMP is 1*

A2. Supporting Protocols

6. In DHCP, what is the correct order of message exchange? a) Offer → Discover → Request → Acknowledgment b) Discover → Offer → Request → Acknowledgment c) Request → Discover → Offer → Acknowledgment d) Discover → Request → Offer → Acknowledgment

Answer: b) Discover → Offer → Request → Acknowledgment *Explanation: DORA sequence - Discover, Offer, Request, Acknowledgment*

7. What does an ICMP Echo Request message implement? a) Traceroute b) Ping c) DNS lookup d) ARP resolution

Answer: b) Ping *Explanation: Ping uses ICMP Echo Request/Reply messages to test reachability*

8. What hop count value indicates an unreachable route in RIP? a) 0 b) 15 c) 16 d) 255

Answer: c) 16 *Explanation: RIP uses hop count 16 to indicate unreachable/infinite distance*

9. Which protocol is used for inter-domain routing between Autonomous Systems? a) RIP b) OSPF c) BGP d) EIGRP

Answer: c) BGP *Explanation: BGP (Border Gateway Protocol) handles routing between different ASes*

10. DHCP spoofing primarily enables which type of attack? a) Buffer overflow b) SQL injection c) Man-in-the-middle d) Cross-site scripting

Answer: c) Man-in-the-middle *Explanation: Rogue DHCP server can redirect traffic through attacker's gateway*

A3. IPSec Protocol Suite

11. IPSec operates at which layer of the OSI model? a) Physical Layer b) Data Link Layer c) Network Layer d) Transport Layer

Answer: c) Network Layer *Explanation: IPSec provides security at the IP/network layer*

12. Which IPSec mode encrypts only the payload? a) Transport Mode b) Tunnel Mode c) Bridge Mode d) Gateway Mode

Answer: a) Transport Mode *Explanation: Transport mode encrypts only payload, leaves original IP header unchanged*

13. What does ESP provide that AH does not? a) Authentication b) Integrity c) Confidentiality d) Replay protection

Answer: c) Confidentiality *Explanation: ESP provides encryption for confidentiality; AH only provides integrity/authentication*

14. How many bits is the SPI field in IPSec headers? a) 16 bits b) 24 bits c) 32 bits d) 64 bits

Answer: c) 32 bits *Explanation: Security Parameters Index is 32 bits in both AH and ESP headers*

15. What is the primary purpose of the sequence number in IPSec? a) Packet ordering b) Replay protection c) Error detection d) Flow control

Answer: b) Replay protection *Explanation: Sequence numbers prevent attackers from replaying old packets*

A4. IKE and Security Associations

16. How many phases does IKE have? a) 1 b) 2 c) 3 d) 4

Answer: b) 2 *Explanation: IKE has Phase 1 (secure channel) and Phase 2 (IPSec SA negotiation)*

17. Which IKE mode uses only 3 messages? a) Main Mode b) Aggressive Mode c) Quick Mode d) Base Mode

Answer: b) Aggressive Mode *Explanation: Aggressive mode uses 3 messages vs Main mode's 6 messages*

18. What advantage does Main Mode have over Aggressive Mode? a) Faster negotiation b) Identity protection c) Smaller packet size d) Better encryption

Answer: b) Identity protection *Explanation: Main mode protects endpoint identities from eavesdroppers*

19. Security Associations in IPSec are: a) Bidirectional b) Unidirectional c) Omnidirectional d) Multidirectional

Answer: b) Unidirectional *Explanation: Separate SAs needed for each direction of communication*

20. What does Perfect Forward Secrecy in IKE Phase 2 provide? a) Faster key generation b) Smaller key sizes c) Protection if long-term keys compromised d) Automatic key renewal

Answer: c) Protection if long-term keys compromised *Explanation: PFS ensures session keys remain secure even if long-term keys are compromised*

Section B: Short Answer Questions (SAQs)

B1. Protocol Analysis

1. Explain the difference between "mutable" and "mutable but predictable" fields in the context of IPSec AH.

Answer:

- **Mutable fields**: Change during packet transmission (e.g., TTL, header checksum)
- **Mutable but predictable fields**: Change during transmission but final values can be predicted by sender (e.g., TTL decrements predictably at each hop)
- **AH significance**: Mutable but predictable fields can be included in authentication calculations because the sender can determine what the receiver will see

2. Describe the three-step process of IP spoofing attack leading to DoS.

Answer:

1. **Crafting Attack**: Attacker creates packets with forged source IP addresses from legitimate users/services
2. **Flooding Target**: Target server receives flood of packets and attempts to respond to forged addresses
3. **Overloading Server**: Server resources (bandwidth, CPU, memory) exhausted handling requests and responses, denying service to legitimate users

3. Explain why IPv6 adoption has been slow despite its technical advantages.

Answer:

- **Compatibility issues**: IPv4 and IPv6 not directly compatible, requiring transition mechanisms
- **Infrastructure costs**: Significant investment needed for compatible hardware/software
- **Limited immediate incentive**: IPv4 workarounds (NAT) reduce urgency for upgrade
- **Training requirements**: Network administrators need education on new protocols

B2. IPSec Mechanisms

4. Compare Transport Mode and Tunnel Mode in IPSec.

Answer: Transport Mode:

- Encrypts only payload
- Original IP header unchanged
- Used for end-to-end host communication
- More efficient (less overhead)

Tunnel Mode:

- Encrypts entire original packet
- New IP header added
- Used for VPN and site-to-site connections
- More secure but higher overhead

5. Explain how the sliding window mechanism addresses the connectionless nature of IP in IPSec.

Answer:

- **Problem**: IP is connectionless, so packets may arrive out of order
- **Challenge**: Sequence numbers for replay protection might reject legitimate late packets

- **Solution**: Sliding window accepts packets within a range around expected sequence number
- **Benefit**: Allows legitimate out-of-order packets while still preventing replay attacks

6. Describe the components of a Security Association (SA).

Answer:

- **SPI (Security Parameters Index)**: Unique identifier for the SA
- **Cryptographic Algorithms**: Encryption (AES, 3DES) and authentication (HMAC-SHA1, HMAC-MD5) methods
- **Keys**: Encryption and authentication keys generated through IKE
- **Lifetime**: Duration SA remains valid before rekeying required
- **Security Protocol**: Whether using AH or ESP

B3. Attack Scenarios

7. Explain how a reflection attack works against symmetric key authentication.

Answer: Setup: Alice and Bob share key K_AB **Phase 1**:

- Eve → Bob: "I'm Alice", R2
- Bob → Eve: R1, f(K_AB, R2)
- Eve stuck (can't compute f(K_AB, R1))

Phase 2 (Reflection):

- Eve → Bob: "I'm Alice", R1 (using R1 as challenge)
- Bob → Eve: R3, f(K_AB, R1) (Bob provides needed response)
- Eve uses f(K_AB, R1) to complete Phase 1

8. Describe three methods of IP hijacking.

Answer:

1. **Hijack Unused Address**: Take over dormant IP address; use DoS to shut down legitimate device
2. **Redirect Hijacking**: Use ICMP redirect messages to redirect connections to alternate hosts
3. **Promiscuous Hijacking**: Position on network path between source and destination to act as man-in-the-middle

---

Section C: Evaluation Questions

C1. Security Analysis

1. Evaluate the security implications of IPSec providing protection at the network layer versus application layer security.

Answer: Advantages of Network Layer (IPSec):

- Transparent to applications - no modification needed
- Comprehensive protection for all traffic between endpoints
- Single configuration protects multiple applications
- Can secure legacy applications that lack built-in security

Limitations:

- Not universally deployed - creates security gaps
- Cannot provide user-level authentication
- May not meet specific application security requirements
- Coarser granularity than application-specific controls

Evaluation: Network layer security provides broad protection but cannot replace application-layer security entirely. Best practice is layered security approach.

2. Analyze the trade-offs between IKE Main Mode and Aggressive Mode.

Answer: Main Mode Analysis:

- **Pros**: Identity protection, more secure against eavesdropping
- **Cons**: Higher overhead (6 messages vs 3), slower establishment

Aggressive Mode Analysis:

- **Pros**: Faster negotiation, lower bandwidth usage
- **Cons**: Exposes endpoint identities, vulnerable to identity-based attacks

Evaluation: Main Mode preferred for security-critical environments; Aggressive Mode suitable for performance-critical scenarios with acceptable identity exposure risk.

3. Evaluate the effectiveness of sequence numbers for replay protection in IPSec.

Answer: Strengths:

- Prevents exact replay of captured packets
- Sliding window accommodates out-of-order delivery

- Automatic increment prevents manual manipulation

Weaknesses:

- Vulnerable to sequence number prediction attacks
- Window size affects both security and performance
- Doesn't prevent attacks that modify packet content while maintaining sequence

Evaluation: Effective against basic replay attacks but should be combined with other mechanisms for comprehensive protection.

C2. Protocol Comparison

4. Compare the vulnerabilities of RIP and BGP routing protocols.

Answer: RIP Vulnerabilities:

- **Route Injection**: Easy to inject false routes due to simple hop-count metric
- **Route Poisoning**: Marking legitimate routes as unreachable (hop count 16)
- **Limited Authentication**: Basic or no authentication mechanisms
- **Broadcast Nature**: Updates sent to all neighbors, easier to intercept

BGP Vulnerabilities:

- **Route Hijacking**: More complex but higher impact due to internet-wide scope
- **Session Hijacking**: Can redirect traffic across different networks
- **Trust-Based Model**: Accepts updates without strict verification
- **Longer Propagation**: Takes time to detect and correct false routes

Evaluation: RIP attacks are easier but limited scope; BGP attacks are harder but can affect global connectivity.

5. Evaluate IPv6 security improvements over IPv4.

Answer: IPv6 Security Enhancements:

- **Built-in IPSec**: Mandatory IPSec support (though implementation varies)
- **Improved Address Architecture**: Better support for hierarchical addressing
- **Reduced Header Complexity**: Fewer fields reduce attack surface
- **Enhanced Authentication**: Better support for authentication mechanisms

Persistent Issues:

- **Configuration Complexity**: More complex setup can lead to security errors
- **Transition Vulnerabilities**: Dual-stack implementations create new attack vectors
- **Limited Deployment**: Slow adoption limits security benefits

Evaluation: IPv6 provides better security foundation but practical deployment challenges limit immediate benefits.

Section D: Comparison Questions

D1. Protocol Mechanisms

1. Compare Authentication Header (AH) and Encapsulating Security Payload (ESP) in IPSec.

Answer:

Aspect	AH	ESP
Primary Function	Integrity & Authentication	Confidentiality + Optional Integrity
Encryption	None	Yes (payload encryption)
Authentication	Yes (entire packet)	Optional (configurable)
Header Coverage	Includes IP header	Excludes new IP header
Overhead	Lower	Higher (due to encryption)
Use Cases	Integrity-only requirements	Confidential communications
Performance	Faster processing	Slower (encryption overhead)

2. Compare IPv4 and IPv6 header structures.

Answer:

Feature	IPv4	IPv6
Header Size	Variable (20-60 bytes)	Fixed (40 bytes)
Address Length	32 bits	128 bits
Header Fields	14 fields	8 fields
Fragmentation	In header	Extension header only
Checksum	Present	None (handled by upper layers)
Options	Variable in header	Extension headers
Processing Speed	Slower (more fields)	Faster (simplified header)

D2. Attack Vectors

3. Compare DoS attacks: SYN Flooding vs ICMP Flooding.

Answer:

Aspect	SYN Flooding	ICMP Flooding
Target Layer	Transport (TCP)	Network (ICMP)
Resource Exhaustion	Connection state tables	Bandwidth & processing
Attack Packets	TCP SYN packets	ICMP Echo Requests
Reconnaissance Value	Port scanning capability	Basic reachability only
Defense Difficulty	Moderate (SYN cookies)	Easier (rate limiting)
Amplification Potential	High (half-open connections)	Low (1:1 response ratio)

Section E: Recommendation Questions

E1. Security Implementation

1. An organization is implementing IPSec for secure remote access. Recommend the appropriate IPSec configuration and justify your choices.

Answer: Recommended Configuration:

- **Mode**: Tunnel Mode
- **Protocol**: ESP with authentication
- **Key Management**: IKE with Main Mode
- **Encryption**: AES-256
- **Authentication**: HMAC-SHA-256
- **Perfect Forward Secrecy**: Enabled

Justifications:

- **Tunnel Mode**: Required for VPN scenarios to encapsulate entire packets
- **ESP with Auth**: Provides confidentiality and integrity for sensitive data
- **Main Mode**: Identity protection important for remote access
- **AES-256**: Strong encryption standard, widely supported
- **HMAC-SHA-256**: Robust authentication, better than SHA-1
- **PFS**: Protects past communications if keys compromised

2. A company experiences frequent DHCP spoofing attacks. Recommend countermeasures and implementation strategy.

Answer: Immediate Countermeasures:

- **DHCP Snooping**: Enable on network switches to filter untrusted DHCP messages
- **Port Security**: Limit MAC addresses per switch port
- **VLAN Segregation**: Separate network segments to limit attack scope

Long-term Solutions:

- **802.1X Authentication**: Authenticate devices before network access
- **DHCP Reservations**: Static assignments for critical systems
- **Network Monitoring**: Deploy tools to detect rogue DHCP servers

Implementation Strategy:

1. **Phase 1**: Enable DHCP snooping on core switches
2. **Phase 2**: Implement port security and monitoring
3. **Phase 3**: Deploy 802.1X for comprehensive access control

3. An ISP is considering IPv6 deployment. Recommend a transition strategy addressing security concerns.

Answer: Transition Strategy:

- **Dual-Stack Deployment**: Run IPv4 and IPv6 simultaneously
- **Staged Rollout**: Start with internal networks, then customer-facing services
- **Training Program**: Educate network administrators on IPv6 security

Security Recommendations:

- **Firewall Updates**: Ensure IPv6 support in security appliances
- **Monitoring Enhancement**: Extend security monitoring to IPv6 traffic
- **Policy Alignment**: Synchronize IPv4 and IPv6 security policies

Risk Mitigation:

- **Tunnel Security**: Secure IPv6-in-IPv4 tunnels during transition
- **Access Controls**: Implement IPv6-aware access control lists
- **Incident Response**: Update procedures for IPv6 security events

Timeline:

- **Months 1-3**: Internal infrastructure upgrade
- **Months 4-6**: Pilot deployment with select customers
- **Months 7-12**: Full customer deployment with monitoring

Answer Key Summary

MCQ Answer Key:

1. b 2. b 3. c 4. d 5. b 6. b 7. b 8. c 9. c 10. c
2. c 12. a 13. c 14. c 15. b 16. b 17. b 18. b 19. b 20. c

Key Study Points:

- Focus on IPSec modes, protocols, and header structures
- Understand attack mechanisms and countermeasures
- Know IKE phases and their purposes
- Master protocol field sizes and functions
- Practice comparing different security approaches