

Network Fundamentals Practice Quiz

Test Your Security+ Readiness!

Section 1: OSI Model & Layers (15 questions)

1. **At which OSI layer do IP addresses operate?**

- A) Layer 2
- B) Layer 3
- C) Layer 4
- D) Layer 7

2. **MAC addresses operate at which layer?**

- A) Layer 1
- B) Layer 2
- C) Layer 3
- D) Layer 4

3. **Port numbers are associated with which layer?**

- A) Layer 2
- B) Layer 3
- C) Layer 4
- D) Layer 7

4. **Which layer is where users interact with applications?**

- A) Layer 5
- B) Layer 6
- C) Layer 7
- D) Layer 4

5. **TCP and UDP operate at which layer?**

- A) Layer 2
- B) Layer 3
- C) Layer 4

- D) Layer 7

6. **A router operates primarily at which layer?**

- A) Layer 2
- B) Layer 3
- C) Layer 4
- D) Layer 7

7. **A switch operates primarily at which layer?**

- A) Layer 1
- B) Layer 2
- C) Layer 3
- D) Layer 4

8. **Which protocol provides reliable, connection-oriented transport?**

- A) UDP
- B) IP
- C) TCP
- D) ICMP

9. **Which is faster but unreliable?**

- A) TCP
- B) UDP
- C) FTP
- D) HTTP

10. **SQL injection attacks target which layer?**

- A) Layer 2
- B) Layer 4
- C) Layer 6
- D) Layer 7

11. **SSL/TLS encryption occurs at which layer?**

- A) Layer 4
- B) Layer 5
- C) Layer 6
- D) Layer 7

12. **ARP spoofing occurs at which layer?**

- A) Layer 2

- B) Layer 3
- C) Layer 4
- D) Layer 7

13. Which best describes TCP?

- A) Connectionless and fast
- B) Connection-oriented and reliable
- C) Used for streaming only
- D) Operates at Layer 2

14. Streaming video typically uses which protocol?

- A) TCP
- B) UDP
- C) FTP
- D) SMTP

15. A Web Application Firewall (WAF) operates at which layer?

- A) Layer 2
 - B) Layer 3
 - C) Layer 4
 - D) Layer 7
-

Section 2: Ports & Protocols (20 questions)

16. What port does HTTPS use?

- A) 80
- B) 443
- C) 8080
- D) 8443

17. What port does SSH use?

- A) 21
- B) 22
- C) 23
- D) 25

18. What port does Telnet use?

- A) 20

- B) 21
- C) 22
- D) 23

19. What port does HTTP use?

- A) 53
- B) 80
- C) 443
- D) 8080

20. What port does DNS use?

- A) 25
- B) 53
- C) 110
- D) 143

21. Which protocol is encrypted?

- A) HTTP
- B) FTP
- C) Telnet
- D) SSH

22. Which protocol is NOT encrypted by default?

- A) HTTPS
- B) SFTP
- C) HTTP
- D) LDAPS

23. SFTP uses which port?

- A) 20
- B) 21
- C) 22
- D) 23

24. RDP uses which port?

- A) 445
- B) 3389
- C) 1433
- D) 8080

25. Which port is associated with Windows file sharing and ransomware?

- A) 80
- B) 443
- C) 445
- D) 3389

26. POP3 uses which port?

- A) 25
- B) 110
- C) 143
- D) 993

27. IMAP uses which port?

- A) 25
- B) 110
- C) 143
- D) 993

28. SMTP is used to:

- A) Receive email
- B) Send email
- C) Browse websites
- D) Transfer files

29. Which is the secure version of FTP?

- A) FTPS or SFTP
- B) HTTP
- C) Telnet
- D) SMTP

30. LDAPS uses which port?

- A) 389
- B) 636
- C) 443
- D) 993

31. DHCP uses which ports?

- A) 20/21
- B) 53

- C) 67/68
- D) 80/443

32. Which protocol should NEVER be used due to sending credentials in plaintext?

- A) SSH
- B) HTTPS
- C) Telnet
- D) SFTP

33. What does DNS do?

- A) Sends email
- B) Assigns IP addresses
- C) Translates domain names to IP addresses
- D) Encrypts web traffic

34. What does DHCP do?

- A) Translates domain names
- B) Automatically assigns IP addresses
- C) Sends email
- D) Encrypts connections

35. Port 25 is used by:

- A) HTTP
- B) SMTP
- C) FTP
- D) SSH

Section 3: IP Addressing (10 questions)

36. Which is a private IP range?

- A) 8.8.8.8
- B) 192.168.1.1
- C) 142.250.80.46
- D) 24.5.67.89

37. Which is a public IP address?

- A) 10.0.0.1
- B) 172.16.1.1

- C) 192.168.1.1
- D) 8.8.8.8

38. What does NAT do?

- A) Translates domain names to IPs
- B) Translates private IPs to public IPs
- C) Encrypts network traffic
- D) Assigns IP addresses

39. Is 172.20.1.50 a private or public IP?

- A) Private
- B) Public
- C) Loopback
- D) APIPA

40. What does /24 mean in CIDR notation?

- A) 24 total addresses
- B) Subnet mask 255.255.255.0
- C) 24 networks
- D) Class A network

41. What is 127.0.0.1?

- A) Default gateway
- B) Loopback address
- C) Broadcast address
- D) Private IP

42. An IP address of 169.254.x.x indicates:

- A) Private network
- B) DHCP failure (APIPA)
- C) Loopback address
- D) Public IP

43. IPv6 addresses are how many bits?

- A) 32
- B) 64
- C) 128
- D) 256

44. Which is an IPv6 address?

- A) 192.168.1.1
- B) 255.255.255.0
- C) 2001:0db8::1
- D) 10.0.0.1

45. **Is NAT a firewall?**

- A) Yes
 - B) No, but it provides some security benefits
 - C) Yes, it blocks all attacks
 - D) No, it has no security benefits
-

Section 4: Network Devices & Security (15 questions)

46. **What is the PRIMARY difference between IDS and IPS?**

- A) IDS encrypts, IPS doesn't
- B) IDS detects only, IPS detects and blocks
- C) IDS is faster than IPS
- D) IDS works at Layer 2, IPS at Layer 3

47. **An IDS is positioned:**

- A) In-line with traffic
- B) Out-of-band (monitoring)
- C) At Layer 2 only
- D) On the internet

48. **An IPS is positioned:**

- A) In-line with traffic
- B) Out-of-band (monitoring)
- C) Outside the firewall
- D) At Layer 7 only

49. **You need to detect attacks but can't risk blocking legitimate traffic. Which do you use?**

- A) IPS
- B) IDS
- C) Firewall
- D) Router

50. **A switch uses which type of address to forward traffic?**

- A) IP address
- B) MAC address
- C) Port number
- D) Domain name

51. A router uses which type of address?

- A) IP address
- B) MAC address
- C) Port number
- D) Email address

52. What does a WAF protect?

- A) The entire network
- B) Web applications specifically
- C) Email servers
- D) DNS servers

53. What is a VLAN used for?

- A) Increasing speed
- B) Network segmentation
- C) Encrypting traffic
- D) Replacing routers

54. VLANs provide security through:

- A) Encryption
- B) Segmentation/isolation
- C) Authentication
- D) Port blocking

55. What is a DMZ?

- A) A type of firewall
- B) A buffer network between internet and internal network
- C) A denial of service attack
- D) A type of encryption

56. What belongs in a DMZ?

- A) Internal file servers
- B) Employee workstations
- C) Public-facing web servers
- D) Domain controllers

57. A firewall that tracks connection state is called:

- A) Packet-filtering firewall
- B) Stateful firewall
- C) Stateless firewall
- D) Application firewall

58. Which attack targets port 445?

- A) Web attacks
- B) Email attacks
- C) Ransomware (WannaCry)
- D) DNS attacks

59. A load balancer provides:

- A) Encryption
- B) High availability and DDoS mitigation
- C) Antivirus protection
- D) Password management

60. A proxy server can:

- A) Only slow down traffic
- B) Filter content and hide internal IPs
- C) Replace a firewall completely
- D) Eliminate all security risks

ANSWER KEY

Section 1 (OSI Model)

1. B (Layer 3)
2. B (Layer 2)
3. C (Layer 4)
4. C (Layer 7)
5. C (Layer 4)
6. B (Layer 3)
7. B (Layer 2)
8. C (TCP)
9. B (UDP)
10. D (Layer 7)

- 11. C (Layer 6)
- 12. A (Layer 2)
- 13. B (Connection-oriented and reliable)
- 14. B (UDP)
- 15. D (Layer 7)

Section 2 (Ports & Protocols)

- 16. B (443)
- 17. B (22)
- 18. D (23)
- 19. B (80)
- 20. B (53)
- 21. D (SSH)
- 22. C (HTTP)
- 23. C (22)
- 24. B (3389)
- 25. C (445)
- 26. B (110)
- 27. C (143)
- 28. B (Send email)
- 29. A (FTPS or SFTP)
- 30. B (636)
- 31. C (67/68)
- 32. C (Telnet)
- 33. C (Translates domain names)
- 34. B (Assigns IP addresses)
- 35. B (SMTP)

Section 3 (IP Addressing)

- 36. B (192.168.1.1)
- 37. D (8.8.8.8)
- 38. B (Translates private to public IPs)
- 39. A (Private)
- 40. B (255.255.255.0)
- 41. B (Loopback)
- 42. B (DHCP failure/APIPA)
- 43. C (128 bits)
- 44. C (2001:0db8::1)
- 45. B (No, but security benefits)

Section 4 (Devices & Security)

- 46. B (IDS detects only, IPS blocks)
 - 47. B (Out-of-band)
 - 48. A (In-line)
 - 49. B (IDS)
 - 50. B (MAC address)
 - 51. A (IP address)
 - 52. B (Web applications)
 - 53. B (Network segmentation)
 - 54. B (Segmentation/isolation)
 - 55. B (Buffer network)
 - 56. C (Public-facing servers)
 - 57. B (Stateful firewall)
 - 58. C (Ransomware)
 - 59. B (High availability/DDoS mitigation)
 - 60. B (Filter content/hide IPs)
-

Scoring Guide

- **54-60 correct:** Excellent! You're ready for Security+
- **48-53 correct:** Good! Review areas you missed
- **42-47 correct:** Fair. More study needed, focus on weak areas
- **Below 42:** Keep studying! Focus on ports and OSI model first

Study Priorities Based on Results

If you missed many in Section 1: Review OSI model layers and what operates at each

If you missed many in Section 2: MEMORIZE port numbers - make flashcards!

If you missed many in Section 3: Review private IP ranges and NAT

If you missed many in Section 4: Focus on IDS vs IPS and device functions