Self-Assessment-Network Security

OSI Layers

1. Which layer of the OSI model is responsible for logical addressing and routing?
    a) Physical Layer
    b) Data Link Layer
    c) Network Layer
    d) Transport Layer

2. What is the primary function of the Data Link Layer?
    a) Error detection and correction
    b) Framing and addressing
    c) Flow control and segmentation
    d) Encryption and decryption

3. Which layer of the OSI model is responsible for providing a common representation of data?
    a) Physical Layer
    b) Presentation Layer
    c) Session Layer
    d) Application Layer

4. The Transport Layer ensures:
    a) Reliable and ordered delivery of data
    b) Physical transmission of data
    c) Error detection and correction
    d) Framing and addressing

5. The Application Layer is responsible for:
    a) Establishing and terminating communication sessions
    b) Providing encryption and decryption of data
    c) Handling routing and logical addressing
    d) Providing services for user applications
6. Which layer of the OSI model provides synchronization and checkpointing of communication sessions?
    a) Transport Layer
    b) Session Layer
    c) Presentation Layer
    d) Application Layer

7. The role of the Data Link Layer includes:
    a) Logical addressing
    b) Reliable delivery of data

c) Physical transmission of data
d) Providing encryption and decryption of data

8. Which layer of the OSI model is responsible for data formatting and encryption/decryption?
    a) Physical Layer
    b) Presentation Layer
    c) Session Layer
    d) Application Layer

9. The Network Layer handles:
    a) Error detection and correction
    b) Flow control and segmentation
    c) Routing and logical addressing
    d) Framing and addressing

10. Which layer of the OSI model is closest to the end user?
    a) Physical Layer
    b) Data Link Layer
    c) Presentation Layer
    d) Application Layer

Answers :

1. c) Network Layer
2. b) Framing and addressing
3. b) Presentation Layer
4. Reliable and ordered delivery of data
5. Providing services for user applications
6. b) Session Layer
7. c) Physical transmission of data
8. b) Presentation Layer
9. c) Routing and logical addressing
10. d) Application Layer

TCP and UDP:

1. Which protocol provides a connection-oriented and reliable communication between applications?
    a) TCP
    b) UDP
    c) IP
    d) HTTP

2. What is the primary advantage of TCP over UDP?
    a) Lower latency
    b) Smaller packet size
    c) Reliable data delivery
    d) Simpler protocol design

3. Which protocol is suitable for real-time applications and video streaming?
    a) TCP
    b) UDP
    c) FTP
    d) HTTP

4. Which protocol includes features like congestion control and flow control?
    a) TCP
    b) UDP
    c) IP
    d) ICMP

5. Which protocol is considered connectionless and does not guarantee reliable data delivery?
    a) TCP
    b) UDP
    c) IP
    d) SMTP

Answers:

1) a) TCP

2) c) Reliable data delivery

3) b) UDP

4) a) TCP

5) b) UDP

DNS,DHCP and SMTP

1. DNS is primarily used for:
    a) Dynamic IP address assignment
    b) Resolving domain names to IP addresses
    c) Secure email communication
    d) Network routing

2. DHCP is responsible for:
    a) Transferring files between clients and servers
    b) Resolving domain names to IP addresses
    c) Assigning IP addresses to devices on a network
    d) Routing email messages

3. SMTP is used for:
    a) Resolving domain names to IP addresses
    b) Assigning IP addresses to devices on a network
    c) Transferring email messages between mail servers
    d) Performing network diagnostics

4. Which protocol is used to retrieve email messages from a mail server?
    a) SMTP
    b) POP3
    c) IMAP
    d) HTTP

5. DNS operates primarily at which layer of the OSI model?
    a) Physical Layer
    b) Data Link Layer
    c) Network Layer
    d) Application Layer

6. DHCP uses which port number for communication?
    a) 53
    b) 67
    c) 80
    d) 110

7. Which protocol is responsible for translating domain names into IP addresses?
    a) DNS
    b) DHCP
    c) SMTP

d) HTTP

8. SMTP typically uses which port number for communication?
    a) 25
    b) 53
    c) 67
    d) 80

9. DHCP allows for the automatic configuration of which network settings?
    a) IP address, subnet mask, and default gateway
    b) DNS server addresses
    c) MAC addresses of devices
    d) FTP server settings

10. Which protocol is commonly used to send email messages between mail servers?
    a) DNS
    b) DHCP
    c) SMTP
    d) HTTP

Answers:

1) b) Resolving domain names to IP addresses

2) c) Assigning IP addresses to devices on a network

3) c) Transferring email messages between mail servers

4) b) POP3

5) c) Network Layer

6) b) 67

7) a) DNS

8 a) 25

9) a) IP address, subnet mask, and default gateway

10 c) SMTP

Firewall:

1. What is the primary purpose of a firewall?
    a) Encryption of network traffic
    b) Prevent unauthorized access to a network
    c) Load balancing of network traffic
    d) Domain name resolution

2. Which layer of the OSI model does a firewall operate at?
    a) Physical Layer
    b) Data Link Layer
    c) Network Layer
    d) Transport Layer

3. Which type of firewall operates at the network layer (Layer 3) of the OSI model?
    a) Stateful Firewall
    b) Application Firewall
    c) Proxy Firewall
    d) Next-Generation Firewall

4. A stateful firewall can inspect:
    a) Only the header information of network packets
    b) Only the payload of network packets
    c) Both the header and payload of network packets
    d) None of the above

5. What is the purpose of a DMZ (Demilitarized Zone) in a firewall configuration?
    a) To provide a secure connection between internal and external networks
    b) To block all network traffic from reaching the internal network
    c) To filter incoming and outgoing traffic based on specific rules
    d) To provide a separate zone for publicly accessible servers

IPS/IDS:

6. What does IPS stand for?
    a) Internet Protocol Security
    b) Intrusion Prevention System
    c) Internet Protocol Suite
    d) Intrusion Detection System

7. An IDS (Intrusion Detection System) primarily focuses on:
    a) Preventing network attacks
    b) Detecting and alerting about network attacks
    c) Blocking malicious traffic from entering the network
    d) Encrypting network traffic

8. What is the primary difference between an IPS and an IDS?
    a) An IPS is hardware-based, while an IDS is software-based.
    b) An IPS can actively block or prevent attacks, while an IDS only detects and alerts.
    c) An IPS operates at the application layer, while an IDS operates at the network layer.
    d) An IPS is used for network monitoring, while an IDS is used for host monitoring.

9. Which type of IDS/IPS detection method compares network traffic against known patterns or signatures?
    a) Behavior-based detection
    b) Anomaly-based detection
    c) Signature-based detection
    d) Heuristic-based detection

10. Which component is responsible for analyzing and correlating events in an IDS/IPS system?
    a) Sensor
    b) Management console
    c) Signature database
    d) Event correlation engine

Proxy:

11. What is the primary purpose of a proxy server?
    a) To encrypt network traffic
    b) To cache web content and improve performance
    c) To authenticate users in a network
    d) To route network traffic between different networks

12. Which type of proxy server allows clients to access resources on the internet indirectly?
    a) Reverse proxy
    b) Forward proxy
    c) Transparent proxy
    d) Load balancing proxy

13. What is the function of a transparent proxy?
    a) To intercept and modify network traffic
    b) To authenticate users before allowing access to web resources
    c) To encrypt network traffic
    d) To block specific websites or content

14. Which layer of the OSI model does a proxy server operate at?
    a) Physical Layer
    b) Data Link Layer
    c) Network Layer
    d) Application Layer

15. Which protocol is commonly used by web proxies to communicate with clients?
    a) TCP
    b) UDP
    c) HTTP
    d) SMTP

WAF (Web Application Firewall):

16. What is the primary purpose of a WAF?
    a) To prevent distributed denial-of-service (DDoS) attacks
    b) To secure network devices from unauthorized access
    c) To protect web applications from common web-based attacks
    d) To encrypt sensitive data transmitted over the internet

17. Which type of security mechanism does a WAF primarily focus on?
    a) Network security
    b) Host security
    c) Application security
    d) Data security

18. Which layer of the OSI model does a WAF typically operate at?
    a) Physical Layer
    b) Data Link Layer
    c) Network Layer
    d) Application Layer

19. What is the function of a WAF rule set?

a) To define access control policies for network devices
b) To identify and block malicious network traffic
c) To filter and analyze web application traffic for vulnerabilities
d) To encrypt sensitive data transmitted over the internet

20. Which type of attack can a WAF help protect against?
    a) DNS poisoning
    b) SQL injection
    c) ARP spoofing
    d) Port scanning

21. A WAF can inspect and filter traffic based on:
    a) IP addresses
    b) MAC addresses
    c) URL patterns
    d) Domain names

22. Which protocol is commonly used by WAFs to communicate with web servers?
    a) FTP
    b) HTTPS
    c) SMTP
    d) SSH

23. What is the purpose of whitelisting and blacklisting in a WAF?
    a) To define allowed and blocked IP addresses
    b) To encrypt network traffic
    c) To detect and block malicious payloads in web requests
    d) To analyze network traffic patterns for anomalies

24. Which component is responsible for analyzing and filtering web traffic in a WAF?
    a) Sensor
    b) Management console
    c) Signature database
    d) Web application firewall engine

25. A WAF can help protect web applications from attacks such as:
    a) Brute-force attacks
    b) Cross-site scripting (XSS)
    c) Man-in-the-middle attacks
    d) Network sniffing

Answers:

1) b) Prevent unauthorized access to a network

2) c) Network Layer

3) a) Stateful Firewall

4) c) Both the header and payload of network packets

5) d) To provide a separate zone for publicly accessible servers

6) b) Intrusion Prevention System

7) b) Detecting and alerting about network attacks

8) b) An IPS can actively block or prevent attacks, while an IDS only detects and alerts.

9) c) Signature-based detection

10) d) Event correlation engine

11) b) To cache web content and improve performance

12) b) Forward proxy

13) a) To intercept and modify network traffic

14) d) Application Layer

15) c) HTTP

16) c) To protect web applications from common web-based attacks

17) c) Application security

18) d) Application Layer

19) c) To filter and analyze web application traffic for vulnerabilities

20) b) SQL injection

21) c) URL patterns

22) b) HTTPS

23) a) To define allowed and blocked IP addresses

24) d) Web application firewall engine

25) b) Cross-site scripting (XSS)