Tutorial Questions

1. A firewall is primarily used to:

A. Encrypt data
B. Monitor employee productivity
C. Control incoming and outgoing network traffic
D. Store backup files

2. What is the main purpose of an Intrusion Detection System (IDS)?

A. Encrypt network data
B. Detect unauthorized access or attacks
C. Block all incoming traffic
D. Assign IP addresses

3. Which of the following is an example of multi-factor authentication?

A. Password only
B. PIN only
C. Password and fingerprint
D. Username only

4. Which tool monitors and logs network traffic for analysis?

A. Antivirus
B. Packet sniffer
C. Compiler
D. Load balancer

5 What is the primary objective of an Information Security Risk Management Framework?

A. Eliminate all security risks
B. Reduce risks to an acceptable level
C. Increase system performance
D. Remove all vulnerabilities

6 Risk in information security is typically calculated as:

A. Threat × Vulnerability × Impact
B. Asset ÷ Threat
C. Control × Exposure
D. Vulnerability ÷ Impact

7 In the National Institute of Standards and Technology Risk Management Framework (RMF), which step comes first?

A. Implement Controls
B. Monitor Controls
C. Categorize Information Systems
D. Authorize System

8 Who is responsible for formally accepting system risk in RMF?

A. Security Analyst
B. System Administrator
C. Authorizing Official
D. End User

9 What is the first step in the risk management process?

A. Risk Mitigation
B. Risk Monitoring
C. Risk Identification
D. Risk Acceptance

10 Which step involves determining the potential consequences and likelihood of identified risks?

A. Risk Identification
B. Risk Assessment (Risk Analysis)
C. Risk Transfer
D. Risk Avoidance

Scenario-Based MCQs for Firewalls

1 Unauthorised Access Attempt

A company notices repeated login attempts to its internal HR server from unknown external IP addresses. The security team wants to automatically block such suspicious traffic.

Which firewall feature should be configured?

A. NAT
B. Access Control Lists (ACLs)
C. DHCP Relay
D. Port Forwarding

2 Public Web Server Deployment

An organization hosts a public web server but wants to prevent direct access to its internal network.

Which firewall architecture should be implemented?

A. Flat Network
B. DMZ (Demilitarized Zone)
C. Peer-to-Peer Network
D. VLAN Only

3 Application-Level Filtering

A company wants to block access to social media websites during working hours without blocking general internet access.

Which firewall type is most suitable?

A. Packet-Filtering Firewall
B. Stateful Inspection Firewall
C. Proxy Firewall (Application-Level Gateway)
D. Hub-Based Filtering

4 Secure Remote Access

Employees need secure access to the corporate network from home.

Which firewall feature supports this requirement?

A. VPN Termination
B. ARP Broadcasting
C. MAC Flooding
D. DNS Forwarding

5 Limiting Outbound Traffic

A company wants to prevent employees from using unauthorized FTP services to transfer company data externally.

What should the firewall administrator configure?

A. Block outbound FTP port (21)
B. Increase bandwidth
C. Enable DHCP
D. Disable NAT

6 Role Change in Organization

Sarah is promoted from Sales Executive to Sales Manager. She should now access team reports but no longer needs access to customer billing systems.

Which access control principle should be applied?

A. Separation of Duties
B. Least Privilege
C. Implicit Deny
D. Account Disablement

7 Biometric Door Access

An organization installs fingerprint scanners at the data center entrance.

This is an example of:

A. Logical Access Control
B. Physical Access Control
C. Administrative Control
D. Technical Audit Control

8 Temporary Project Access

A contractor needs system access for two weeks and must automatically lose access afterward.

What should be implemented?

A. Permanent Role Assignment
B. Time-Based Access Control
C. Open Permissions
D. Shared Accounts