Module 3: Operating Systems Security - MCQs

Q1: What is the main goal of security in operating systems?

A. To enhance speed

B. To improve UI

C. To prevent unauthorized access

D. To increase memory

Answer: C

Q2: Which of the following is a principle of secure OS design?

A. Simplified Design

B. Complex Interfaces

C. User-Driven Execution

D. Randomized Layout

Answer: A

Q3: What is a Layered Design in OS security?

A. A design based on GUI

B. One layer for all functions

C. Security through multiple independent layers

D. Design based on user roles

Answer: C

Q4: What is the function of a Kernel in OS security?

A. Manages hardware only

B. Provides access to apps

C. Manages system calls and enforces security

D. Enhances graphics

Answer: C

Q5: What does the Reference Monitor concept ensure?

A. Free software updates

B. Unauthenticated access

C. Controlled and audited access

D. Layered GUI

Answer: C

Q6: Which term refers to systems designed to enforce a security policy?

A. User Systems

B. Trusted Systems

C. Admin Systems

D. Networked Systems

Answer: B

Q7: What are Trusted System Functions?

A. Regular app features

B. Critical functions ensuring security policy

C. Debugging tools

D. Design components

Answer: B

Q8: What is a Trusted Operating System?

A. One developed by open source

B. OS with advanced GUI

C. OS designed with security policies and enforcement mechanisms

D. Gaming OS

Answer: C

Q9: What type of attack modifies the OS to hide its presence?

A. Virus

B. Worm

C. Rootkit

D. Spyware

Answer: C

Q10: How can rootkit attacks be mitigated?

A. Ignore logs

B. Run unknown apps

C. Use secure boot and integrity checks

D. Disable antivirus

Answer: C

Q11: Which layer in a layered design usually includes hardware?

A. Top layer

B. Middle layer

C. Bottom layer

D. All layers

Answer: C

Q12: Which of the following is not a characteristic of Trusted Systems?

A. Audit

B. Discretionary Access Control

C. Randomized Execution

D. Mandatory Access Control

Answer: C

Q13: What is the kernel's role in a kernelized OS design?

A. Graphic enhancement

B. Internet routing

C. Core security enforcement and resource management

D. User communication

Answer: C

Q14: What does a secure reference monitor require?

A. Speed

B. Graphics

C. Tamper-proof and complete mediation

D. Accessibility

Answer: C

Q15: Trusted Computing Base (TCB) is part of which system?

A. User Applications

B. Trusted Systems

C. Social Media

D. Cloud Services

Answer: B

Q16: What defines a rootkit?

A. Data backup software

B. Hidden malware modifying system behavior

C. Email scanner

D. Text editor

Answer: B

Q17: Which OS design ensures layered separation of privileges?

A. Flat design

B. Layered design

C. User-centric design

D. Kernel bypass

Answer: B

Q18: Which feature is NOT part of a secure OS design?

A. Access control

B. Audit logs

C. Open debugging

D. Authentication

Answer: C

Q19: How can trusted systems help in enterprise environments?

A. Increase graphics

B. Ensure secure multi-user access

C. Simplify user roles

D. Enhance email features

Answer: B

Q20: Rootkit mitigation requires which of the following?

A. Installing games

B. Clearing cache

C. Trusted boot mechanisms

D. Turning off antivirus

Answer: C

Module 4: Security Countermeasures - MCQs

Q1: What is the main function of a firewall?

A. Data backup

B. Power regulation

C. Control network traffic

D. Run applications

Answer: C

Q2: Which firewall type filters packets based on rules?

A. Application firewall

B. Proxy firewall

C. Packet-filtering firewall

D. Database firewall

Answer: C

Q3: What is a personal firewall?

A. Firewall for routers

B. Firewall for home/individual devices

C. Firewall for websites

D. Firewall for data centers

Answer: B

Q4: How can firewalls be configured?

A. Static only

B. Manually and automatically

C. Only by developers

D. Only in Linux

Answer: B

Q5: What is the function of Network Address Translation (NAT)?

A. Encrypt files

B. Hide IP addresses by mapping private to public addresses

C. Control email traffic

D. Run protocols

Answer: B

Q6: What does DLP stand for in security?

A. Data Loss Prevention

B. Direct Line Protocol

C. Data Loop Protection

D. Device Load Panel

Answer: A

Q7: What does a DLP system protect against?

A. System crashes

B. Data leakage

C. Network throttling

D. Unauthorized encryption

Answer: B

Q8: What is an IDS?

A. Internet Delivery System

B. Intrusion Detection System

C. Internal Data Server

D. Information Drive Scanner

Answer: B

Q9: Which type of IDS analyzes network packets?

A. Host-based IDS

B. Network-based IDS

C. Signature-based IDS

D. Behavioral IDS

Answer: B

Q10: What is the role of IPS?

A. Prevent intrusions

B. Store passwords

C. Compress data

D. Manage users

Answer: A

Q11: Which IDS type uses known attack patterns?

A. Anomaly-based

B. Signature-based

C. Heuristic

D. Heuristic-based

Answer: B

Q12: What is an intrusion response mechanism?

A. Data visualization

B. Automated action against detected threats

C. Memory cleaning

D. RAM scheduling

Answer: B

Q13: Which is a limitation of IDS?

A. Cannot monitor

B. Slow response time

C. High false positives

D. Low cost

Answer: C

Q14: Which of the following is a goal of IDS?

A. Detect and alert on threats

B. Optimize screen display

C. Speed up RAM

D. Run apps faster

Answer: A

Q15: What is a strength of IDS systems?

A. Accurate power usage

B. Low network delay

C. High visibility into attacks

D. Fast internet browsing

Answer: C

Q16: Which IDS can identify previously unknown threats?

A. Signature-based

B. Anomaly-based

C. Rule-based

D. Block-based

Answer: B

Q17: Which firewall works at the application layer?

A. Packet-filtering

B. Stateful

C. Application firewall

D. NAT firewall

Answer: C

Q18: How does IPS differ from IDS?

A. IPS detects only

B. IPS responds actively to threats

C. IPS is slower

D. IPS needs no configuration

Answer: B

Q19: What does NAT enhance?

A. Graphics

B. Security by hiding internal IPs

C. Data mining

D. USB performance

Answer: B

Q20: Personal firewalls are most useful for?

A. Corporate servers

B. Individual devices

C. Public Wi-Fi

D. Gaming consoles

Answer: B