CompTIA

SECURITY+

EXAM SY0-701

PRACTICE TESTS

www.bootcampinsight.com

CompTIA Security+ sy0-701 exam questions for Practice

01. Question: What type of access control model uses policies that evaluate attributes (user, resource, and environment) to make access decisions?
(A) Mandatory Access Control (MAC)
(B) Discretionary Access Control (DAC)
(C) Role-Based Access Control (RBAC)
(D) Attribute-Based Access Control (ABAC)

02. Question: Which principle ensures that critical decisions are not dependent on a single individual?
(A) Dual Control
(B) Need to Know
(C) Separation of Duties
(D) Least Privilege

03. Question: What security concept involves disguising data to hide its true content?
(A) Encryption
(B) Obfuscation
(C) Tokenization
(D) Anonymization

04. Question: Which of the following best defines the concept of 'availability' in the context of information security?
(A) Ensuring timely and reliable access to and use of information
(B) Preventing unauthorized access to information
(C) Ensuring the accuracy and completeness of information
(D) Guaranteeing the confidentiality of information

05. Question: Which type of security control attempts to discourage security violations before they occur?
(A) Preventive
(B) Detective
(C) Corrective
(D) Deterrent

06. Question: What term is used to describe the unauthorized tracking of RFID tags?
(A) Eavesdropping
(B) Phishing
(C) Skimming
(D) Spoofing

07. Question: Which security model is specifically designed to prevent conflict of interest when accessing data?
(A) Bell-LaPadula Model
(B) Biba Model
(C) Clark-Wilson Model
(D) Brewer and Nash Model

08. Question: Which of the following best describes a 'man-in-the-middle' (MITM) attack?
(A) An attack where the perpetrator secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.
(B) An attack that involves flooding a targeted machine or resource with excessive requests to overload systems and prevent some or all legitimate requests from being fulfilled.
(C) A form of cyber attack that uses disguised email as a weapon. The goal is to Ethan the email recipient into believing that the message is something they want or need.
(D) An attack where the attacker secretly intercepts and logs all the victim's outgoing messages.

09. Question: What is the primary security concern with 'shadow IT'?
(A) Increased costs due to unapproved software purchases
(B) Legal issues arising from unlicensed software use
(C) Security risks due to lack of oversight and management
(D) Decreased productivity due to non-standard software solutions

10. Question: What does a 'blacklist' access control strategy involve?
(A) Allowing access to all resources, except those specifically denied.
(B) Denying access to all resources, except those specifically allowed.
(C) Granting access based on the user's role within the organization.
(D) Allowing access based on the sensitivity of the information.

11. Question: A security team is concerned about the potential for data leaks through cloud storage services used by employees. Which of the following strategies would MOST effectively mitigate this risk?
(A) Blocking access to all cloud storage services
(B) Encrypting all data stored in the cloud
(C) Implementing a Cloud Access Security Broker (CASB)
(D) Training employees on the proper use of cloud storage

12. Question: Sara, while investigating a security incident, checks the **/var/log** directory on a Linux system and discovers the **audit.log** file to be empty, despite the system having been up for over a month. What scenario has she most likely stumbled upon?
(A) Log files have been wiped
(B) The system was recently rebooted
(C) There was a system error
(D) She lacks the correct permissions to view the log

13. Question: When evaluating concerns related to the hardware supply chain, which of the following is LEAST likely to be a prevalent issue?
(A) Pre-installed malware on hardware
(B) Shortages in hardware availability
(C) Unauthorized modifications by third parties
(D) Malicious alterations to firmware

14. Question: Evan is evaluating the motivations behind potential internal threat actors within his organization. Which motivation is MOST likely to drive such an individual?

(A) Engaging in espionage
(B) Acting out of blackmail
(C) Participating in warfare
(D) Holding strong political convictions

15. Question: Sophia notices an anomaly in login activities: an employee appears to have logged in from China and then from the United Kingdom within a single hour. How should this be categorized in terms of security concerns?

(A) Misuse of concurrent sessions
(B) Resource access issues
(C) Impossible travel activity
(D) Network segmentation breach

16. Question : James is required to enter a 6-digit PIN in addition to using his RFID badge at his workplace. What security threat is this additional measure aiming to mitigate?

(A) Tailgating
(B) Man-in-the-path attacks
(C) Simultaneous access breaches
(D) Cloning of RFID badges

17. Question: Ethan discovers that traffic from one of their domains is being redirected to a competitor's site, with administrative details altered. Assuming the domain hasn't expired, what likely happened?

(A) DNS hijacking
(B) Man-in-the-path attack
(C) Domain hijacking
(D) Exploitation of an unknown vulnerability (zero-day attack)

18. Question: An organization finds that certain outbound traffic is being redirected through an unauthorized IP address. What type of security breach is this indicative of?

- (A) DNS Spoofing

- (B) Service Denial
- (C) Insider Threat
- (D) Physical Security Breach

19. Question: During a routine audit, an admin discovers several user accounts with unusually high privileges not required for their job roles. What principle is being violated?

(A) Principle of Least Privilege
(B) Segregation of Duties
(C) Need to Know
(D) Continuous Monitoring

20. Question: An organization's IT department notices slow network performance and traces the issue to a large volume of outbound SMTP traffic. What kind of compromise does this suggest?

(A) Man-in-the-Middle Attack
(B) Distributed Denial of Service (DDoS) Attack
(C) Email Server Compromise
(D) Phishing Attack

21. Question: A security analyst notices an uptick in encrypted traffic bypassing the organization's secure web gateway. What might be occurring?

(A) SSL Stripping
(B) Encrypted Malware Transmission
(C) Certificate Authority Compromise
(D) Rogue VPN Usage

Question 22: Evelyn wants to deploy an encryption solution that will protect files in motion as they are copied between file shares, as well as at rest, and also needs it to support granular per-user security. What type of solution should she select?

A. Partition encryption
B. File encryption
C. Full-disk encryption
D. Record-level encryption

Question 23: Valerie wants to use a certificate to handle multiple subdomains for her website, including sales.example.com and support.example.com. What type of certificate should she use?
A. A self-signed certificate
B. A root of trust certificate
C. A CRL certificate
D. A wildcard certificate

Question 24: What information is analyzed during a gap analysis?
A. Control objectives and controls intended to meet the objectives
B. Physically separate networks and their potential connection points
C. Compensating controls and the controls they are replacing
D. Security procedures and the policies they are designed to support

Question 25: Casey's team has recommended an application restart for a production customer-facing application as part of an urgent patch due to a security update. What technical implication is the most common concern when conducting an application restart?
A. Application configuration changes caused by the restart
B. Whether the patch will properly apply
C. Lack of security controls during the restart
D. The downtime during the restart

Question 26: Using a tool like git is most frequently associated with what critical change management process?
A. Having a backout plan
B. Stakeholder analysis
C. Version control
D. Standard operating procedures (SOPs)
Question 27: Evelyn is concerned that the password used for one of his organization's services is weak, and he wants to make it harder to crack by making it harder to test possible keys during a brute-force attack. What is this technique called?
A. Master keying
B. Key stretching
C. Key rotation
D. Passphrase armoring

Question 28: Log monitoring is an example of what control category?
A. Technical
B. Managerial
C. Operational
D. Physical

Question 29: James wants to make offline brute-force attacks against his password file very difficult for attackers. Which of the following is NOT a common technique to make passwords harder to crack?
A. Use of a salt
B. Use of a pepper
C. Use of a purpose-built password hashing algorithm
D. Encrypting password plaintext using symmetric encryption

Question 30: Diffie-Hellman and RSA are both examples of what important encryption-related solution?
A. Rekeying
B. Certificate revocation protocols
C. Key exchange algorithms
D. Key generation algorithms

Question 31: Emma wants to ensure that her change management process includes a procedure for what to do if the change fails. What should she create to handle this possibility?
A. An impact analysis
B. A backout plan
C. A regression test
D. A maintenance window

Question 32: A rapidly growing e-commerce company has recently experienced an increase in cross-site scripting (XSS) and SQL injection attacks. To specifically combat these types of threats at the application layer, which firewall solution is most suitable?
(A) Stateful Packet Inspection Firewall
(B) Proxy Firewall
(C) Network Layer Firewall
(D) Web Application Firewall (WAF)

Question 33: SafeGaurdPlus, a cybersecurity firm, is tasked with deploying an Intrusion Detection System (IDS) for an enterprise client. Where should the IDS be positioned to optimally detect malicious activity?
(A) Before the perimeter firewall to capture all inbound traffic
(B) Between the perimeter firewall and the internal network to monitor filtered traffic
(C) Inside the DMZ to monitor only external service requests
(D) Adjacent to each workstation for personalized security

Question 34: ABC Corp's software development team has developed an application with unique and innovative algorithms. To prevent competitors from copying or replicating their application's functionality, what legal protection should the company seek?
(A) Copyright the user interface design
(B) Apply for a patent for the innovative algorithms
(C) Store the application code in an encrypted vault
(D) Ensure all users sign an acceptable use policy (AUP)

Question 35: When designing services in a microservices architecture, what principle ensures each service performs a specific task and interacts with others through well-defined interfaces?
(A) Principle of Least Privilege
(B) Single Responsibility Principle
(C) Open-Closed Principle
(D) Zero Trust Model

Question 36: A multinational organization with multiple branch offices seeks a technology to simplify their WAN connectivity, reduce costs, and ensure secure data transfers between offices. Which technology best fits their needs?
(A) VLAN
(B) MPLS
(C) SD-WAN
(D) DMZ

Question 37: A financial company aims to improve web browsing security by intercepting web traffic to prevent access to malicious sites and malware downloads. What solution acts as an intermediary for client resource requests?

(A) Network IDS
(B) VPN Concentrator
(C) Proxy server
(D) Jump server

Question 38: What is the primary purpose of conducting regular security audits within an organization?

(A) To monitor employee productivity levels
(B) To ensure compliance with security policies and regulations
(C) To evaluate the performance of IT infrastructure
(D) To manage employee access to social media

Question 39: In incident response, what is the FIRST step that should be taken after identifying a security breach?

(A) Eradication of the threat
(B) Containment of the breach
(C) Notification of stakeholders
(D) Recovery of affected systems

Question 40: Which tool is MOST effective for detecting unauthorized changes to software and system configurations?

(A) Antivirus software
(B) Intrusion Detection System (IDS)
(C) File Integrity Monitoring (FIM) tools
(D) Firewalls

Question 41: Which of the following best describes the role of a Security Operations Center (SOC)?

(A) Developing and enforcing the organization's security policies
(B) Designing the organization's network architecture
(C) Monitoring, detecting, analyzing, and responding to cybersecurity incidents
(D) Managing the organization's IT infrastructure

Question 42: What is the primary goal of implementing a Security Information and Event Management (SIEM) system?

(A) To encrypt sensitive data
(B) To provide real-time analysis of security alerts generated by applications and network hardware
(C) To manage network devices and configurations
(D) To conduct vulnerability scans on the network

Question 43: In the context of digital forensics, what is the primary importance of maintaining a chain of custody for evidence?
(A) To ensure the evidence can be safely stored for long periods
(B) To document the evidence’s control, transfer, analysis, and disposition
(C) To increase the efficiency of the forensic analysis
(D) To ensure the privacy of individuals involved in the investigation

Question 44: Which strategy is MOST effective in ensuring data recovery in the event of a catastrophic failure?
(A) Regular penetration testing
(B) Implementing strong encryption algorithms
(C) Offsite backup storage
(D) Deploying antivirus solutions

Question 45: What is the primary function of an intrusion prevention system (IPS)?
(A) To analyze and log traffic for future review
(B) To detect and prevent known threats in real time by analyzing traffic flows
(C) To encrypt traffic between the client and the server
(D) To provide a secure tunnel for data transmission over the internet

Question 46: Which phase of the incident response process involves actions taken to repair and restore systems or data affected by a cybersecurity incident?
(A) Identification
(B) Containment
(C) Eradication
(D) Recovery

Question 47: In cybersecurity, what is the primary purpose of a vulnerability assessment?

(A) To physically secure the organization’s premises
(B) To identify, quantify, and prioritize vulnerabilities in a system
(C) To monitor network traffic for malicious activity
(D) To test the effectiveness of organizational security policies

Question 48: Before deploying a new application, a large e-commerce company aims to identify and fix any code vulnerabilities. Which method should they use?

(A) Runtime application self-protection (RASP)
(B) Live application penetration testing
(C) Static code analysis
(D) User acceptance testing (UAT)

Question 49: Jenny wants to ensure each asset in her organization has a defined owner. What's the most effective strategy?

(A) Utilize an automated discovery tool and assign assets by location
(B) Assign department heads as default asset owners
(C) Require manual asset claims in audits
(D) Implement an Asset Management System with defined ownership

Question 50: Following an audit, a company needs to harden its network switches against unauthorized access. What's the BEST approach?

(A) Set up port mirroring
(B) Disable unused ports
(C) Implement load balancing
(D) Increase MAC address table size

Question 51: XenonTech's security team is tasked with monitoring a new web application for vulnerabilities during runtime. Which technique is most appropriate?

(A) Static Analysis
(B) Fuzz Testing
(C) Whitebox Testing
(D) Dynamic Analysis

Question 52: XenonTech seeks real-time updates on emerging threats. What's the BEST source for this information?

(A) Internal vulnerability scanners
(B) Manual penetration tests
(C) OSINT threat feeds
(D) Firewall logs

Question 53: Prior to finalizing a purchase, a medium-sized enterprise evaluates devices from a cost-effective vendor. What should be their main concern?

(A) Warranty length
(B) Device aesthetics
(C) Compliance with security standards
(D) IT staff training needs

Question 54: To understand CyberTech Inc.'s network layout, what activity will enumerate the active devices and their roles?

(A) Vulnerability Scanning
(B) Intrusion Detection
(C) Network Enumeration
(D) Penetration Testing

Question 55: For secure initial configuration of new routers, what step is paramount?

(A) Enabling DHCP for dynamic IP management
(B) Changing default admin credentials
(C) Updating to the latest firmware for new features
(D) Customizing LED indicators for identification

Question 56: What is the primary objective of implementing a Data Loss Prevention (DLP) system in an organization?

(A) To monitor and protect sensitive data from unauthorized access
(B) To enhance the speed of data transmission within the network
(C) To provide a backup solution for critical data
(D) To detect and mitigate network performance issues

Question 57: What is the primary purpose of conducting a risk assessment in an organization's security program management?

(A) To fulfill insurance requirements
(B) To identify and quantify risks to the organization’s assets and determine appropriate ways to mitigate them
(C) To ensure compliance with all software licenses
(D) To prepare for annual financial audits

Question 58: What role does a Security Policy play in an organization's security program?

(A) It provides detailed technical instructions for configuring network equipment.
(B) It outlines acceptable use of organization’s resources and expected behaviors from employees.
(C) It serves as a legal contract between the organization and its customers.
(D) It is a formal document that specifies who has administrative rights on the network.

Question 59: Why is it important for an organization to have a Business Continuity Plan (BCP)?

(A) To ensure all employees know their daily tasks
(B) To facilitate rapid recovery and continuation of operations after a significant disruption
(C) To monitor employee activities
(D) To comply with external marketing standards

Question 60: How does implementing an Incident Response Plan (IRP) benefit an organization?

(A) It eliminates the need for cybersecurity insurance.
(B) It ensures that no security incidents will occur.
(C) It provides a predefined set of procedures to follow in the event of a security incident.
(D) It automatically mitigates all vulnerabilities in the organization’s network.

Question 61: What is the significance of Security Awareness Training within an organization?

(A) It is only necessary for IT staff and security personnel.

(B) It educates employees about the organization’s security policy and their role in maintaining security.

(C) It qualifies employees to perform security audits.

(D) It is a one-time requirement during employee onboarding.

Question 62: What is the primary goal of a Third-Party Risk Management (TPRM) program?

(A) To ensure third parties have faster access to the organization’s data

(B) To manage risks associated with outsourcing services and products from third-party vendors

(C) To reduce costs associated with third-party services

(D) To transfer all security risks to third-party vendors

Question 63: Why is it crucial for an organization to conduct regular security audits?

(A) To check the efficiency of the IT department

(B) To evaluate the organization’s compliance with its security policies and relevant regulations

(C) To allocate budget for social events

(D) To assess the performance of individual employees

Question 64: What is the purpose of a Security Operations Center (SOC) in an organization?

(A) To serve as a call center for customer service inquiries

(B) To manage the organization's social media accounts

(C) To provide continuous monitoring and analysis of security alerts and incidents

(D) To handle the organization’s financial transactions

Question 65: In security program management, what is the role of a Change Management process?

(A) To document daily activities of the security team
(B) To ensure that changes to the IT infrastructure are performed in a controlled and secure manner
(C) To change the organization's security policies annually
(D) To manage changes in employee roles and responsibilities

Question 66: How does a vulnerability management program benefit an organization’s security posture?

(A) By ensuring all software is proprietary
(B) By facilitating the rapid development of new applications
(C) By systematically identifying, assessing, and mitigating vulnerabilities
(D) By eliminating the need for security policies

Question 67: XenonTech and InfoTechSolutions are formalizing their partnership with a set of terms for future transactions. What type of agreement best suits their need to establish foundational business terms?

(A) Memorandum of Understanding (MOU)
(B) Non-Disclosure Agreement (NDA)
(C) Licensing Agreement
(D) Master Service Agreement (MSA)

Question 68: InfoTechSolutions's security team is categorizing risks by potential impact levels as part of their new cloud-based project analysis. What type of risk analysis are they conducting?

(A) Quantitative
(B) Statistical
(C) Qualitative
(D) Financial

Question 69: MegaTech Inc. aims to ensure critical applications are restored within 4 hours after any disaster, with a maximum data loss window of 1 hour. Which policy specifically supports this goal?

(A) Data Retention Policy
(B) Incident Response Policy
(C) Disaster Recovery Policy
(D) Password Policy

Question 70: In the aftermath of a DDoS attack, the CISO of an e-commerce company stresses the need for a plan encompassing identification to lessons learned. Which policy outlines these stages for managing security incidents?

(A) Change Management Policy
(B) Incident Response Policy
(C) Disaster Recovery Policy
(D) Remote Access Policy