

100 CompTIA Security+ SY0-701 Practice Questions & Answers

Welcome to your complete **Security+ SY0-701 practice questions** collection. This set is designed not just for testing — but also **to teach, strengthen, and deepen** your real exam readiness.



Learning Objectives and Expectations

You'll get:

- Real-world style questions, modeled after CompTIA exam wording.
- Formatted by **10 questions then 10 answers** to quickly verify yourself.
- Short explanations clarifying correct answers and reinforcing key points.

Security+ SY0-701 Domains at a Glance

Each domain is weighted differently on the exam, with Security Operations being the largest:

- Domain 1: General Security Concepts (12%)
- Domain 2: Threats, Vulnerabilities, and Mitigations (22%)
- Domain 3: Security Architecture (18%)
- Domain 4: Security Operations (28%)
- Domain 5: Security Program Management and Oversight (20%)

Quick Reminder: How the Exam Works

- Number of Questions: Up to 90
- Format: Multiple choice + Performance-Based Questions (PBQs)
- Time Limit: 90 minutes
- Passing Score: 750/900 (about 83%)
- Test Provider: Pearson VUE (onsite or online)

Questions By Domain

Domain	Title	Questions Assigned	Question Numbers
Domain 1	General Security Concepts (12%)	12 Questions	Q1–4, Q24, Q31, Q44–45, Q53, Q78, Q91, Q93
Domain 2	Threats, Vulnerabilities, and Mitigations (22%)	22 Questions	Q2–3, Q8–9, Q11–13, Q19, Q28–29, Q36, Q40, Q46, Q49, Q54, Q58, Q61, Q68, Q69, Q76, Q79, Q96
Domain 3	Security Architecture (18%)	18 Questions	Q5–7, Q14–15, Q18, Q22, Q26–27, Q32, Q35, Q42, Q47–48, Q55, Q66, Q77, Q80
Domain 4	Security Operations (28%)	28 Questions	Q10, Q16–17, Q20–21, Q23, Q25, Q30, Q33–34, Q37–39, Q41, Q43, Q50, Q52, Q57, Q60, Q63–64, Q70, Q73, Q81–82, Q87, Q90
Domain 5	Security Program Management and Oversight (20%)	20 Questions	Q35, Q51, Q56, Q59, Q62, Q65, Q67, Q71–72, Q74–75, Q83, Q85–86, Q88–89, Q92, Q94–95, Q97, Q99–100

Remember — you don't need to be perfect to pass!

The Security+ passing score is about **83%**. That means you **can miss around 15–16 questions out of 90** and still pass!

Missing a few tricky questions won't ruin your chances — **stay calm**, trust your preparation, and keep moving forward.

Practice Questions 1–10

Q1.

Which of the following ensures that a sender cannot deny sending a message?

- A) Encryption
 - B) Hashing
 - C) Digital Signature
 - D) Symmetric Key Exchange
-

Q2. Which type of threat actor is MOST likely to have the greatest resources and patience for an extended attack?

- A) Insider
 - B) Nation-State
 - C) Script Kiddie
 - D) Hacktivist
-

Q3.

What type of attack involves inserting malicious code into a legitimate web application to steal information from users?

- A) Phishing
 - B) SQL Injection
 - C) Cross-Site Scripting (XSS)
 - D) DNS Spoofing
-

Q4.

A company needs to prevent unauthorized devices from connecting to its internal network. What technology should be used?

- A) Firewall
 - B) VPN
 - C) NAC (Network Access Control)
 - D) IDS
-

Q5.

Which backup type saves only the changes made since the last full backup?

- A) Incremental
 - B) Differential
 - C) Full
 - D) Snapshot
-

Q6.

What control type is a biometric fingerprint scanner?

- A) Technical
 - B) Administrative
 - C) Physical
 - D) Compensating
-

Q7.

Which wireless security protocol is the most secure for corporate environments?

- A) WEP
 - B) WPA
 - C) WPA2-PSK
 - D) WPA3-Enterprise
-

Q8.

Which of the following would BEST help mitigate risks associated with phishing attacks?

- A) IDS
 - B) Security Awareness Training
 - C) Firewall Rules
 - D) Password Complexity Requirements
-

Q9.

Which risk response involves buying cyber insurance?

- A) Accept
- B) Mitigate

- C) Transfer
 - D) Avoid
-

Q10.

Which concept is being applied when access to files is based on job roles such as HR, IT, or Accounting?

- A) MAC
 - B) DAC
 - C) RBAC
 - D) ABAC
-

Answers and Explanations 1–10

A1.

Answer: C) Digital Signature

Explanation:

Digital signatures ensure non-repudiation — proving who sent the data.

A2.

Answer: B) Nation-State

Explanation:

Nation-state actors have the highest resources, skills, and patience for prolonged attacks.

A3.

Answer: C) Cross-Site Scripting (XSS)

Explanation:

XSS injects malicious scripts into web apps to steal session cookies, data, etc.

A4.

Answer: C) NAC (Network Access Control)

Explanation:

NAC checks device health and enforces policies before allowing network access.

A5.

Answer: A) Incremental

Explanation:

Incremental backup captures only changes since the last full backup.

A6.

Answer: C) Physical

Explanation:

Biometric scanners are physical controls that authenticate users.

A7.

Answer: D) WPA3-Enterprise

Explanation:

WPA3-Enterprise is the most secure option for business wireless networks.

A8.

Answer: B) Security Awareness Training

Explanation:

Training users helps them recognize phishing attempts and avoid falling victim.

A9.

Answer: C) Transfer

Explanation:

Buying insurance transfers the financial risk to another party.

A10.

Answer: C) RBAC

Explanation:

Role-Based Access Control (RBAC) assigns permissions based on user job roles.

Practice Questions 11–20

Q11.

Which term describes an attack where an unauthorized device connects to a corporate wireless network?

- A) Rogue AP
 - B) Evil Twin
 - C) Bluejacking
 - D) MAC Spoofing
-

Q12.

What type of malware disguises itself as a legitimate program but delivers a malicious payload?

- A) Worm
 - B) Ransomware
 - C) Trojan
 - D) Rootkit
-

Q13.

Which process helps ensure that only needed ports and services are running on a server?

- A) Network segmentation
 - B) Baseline configuration
 - C) Change management
 - D) Hardening
-

Q14.

A database administrator is setting access so that users only have permission to view certain data. Which principle is being applied?

- A) Separation of Duties
 - B) Need-to-Know
 - C) Non-repudiation
 - D) Risk Transference
-

Q15.

Which option BEST describes a warm site in disaster recovery planning?

- A) Fully operational copy of the production environment
 - B) Facility with basic hardware but not real-time data
 - C) Empty building with power and Internet only
 - D) Vendor-provided cloud backup solution
-

Q16.

Which technology would a company use to detect unauthorized changes to critical system files?

- A) DLP
 - B) File Integrity Monitoring (FIM)
 - C) SIEM
 - D) HIDS
-

Q17.

A phishing attack led to a ransomware infection. Which two controls would have BEST prevented the incident? (Choose two.)

- A) Data Encryption
 - B) Email Filtering
 - C) Security Awareness Training
 - D) RAID 5
-

Q18.

Which type of access control is enforced by system policies rather than user discretion?

- A) DAC
 - B) RBAC
 - C) ABAC
 - D) MAC
-

Q19.

What is the primary purpose of a honeypot?

- A) Encrypt sensitive data
- B) Divert attackers away from real systems

- C) Patch vulnerabilities
 - D) Enforce firewall rules
-

Q20.

Which incident response phase involves learning lessons and updating the incident response plan after a security event?

- A) Detection
 - B) Containment
 - C) Recovery
 - D) Lessons Learned
-

Answers and Explanations 11–20

A11.

Answer: B) Evil Twin

Explanation:

An evil twin is a rogue Wi-Fi access point set up to mimic a legitimate network.

A12.

Answer: C) Trojan

Explanation:

A trojan appears legitimate but delivers malicious code once executed.

A13.

Answer: D) Hardening

Explanation:

Hardening reduces attack surface by disabling unnecessary services.

A14.

Answer: B) Need-to-Know

Explanation:

Need-to-know restricts data access to only necessary users.

A15.

Answer: B) Facility with basic hardware but not real-time data

Explanation:

Warm sites have equipment ready but need configuration and data loading.

A16.

Answer: B) File Integrity Monitoring (FIM)

Explanation:

FIM detects unauthorized changes to files.

A17.

Answer: B) Email Filtering and C) Security Awareness Training

Explanation:

Filtering blocks phishing emails; training teaches users to recognize them.

A18.

Answer: D) MAC

Explanation:

Mandatory Access Control (MAC) strictly enforces security policies.

A19.

Answer: B) Divert attackers away from real systems

Explanation:

Honeypots attract attackers to fake systems to study them.

A20.

Answer: D) Lessons Learned

Explanation:

Post-incident analysis improves future responses.

Practice Questions 21–30

Q21.

Which of the following BEST describes a risk mitigation strategy?

- A) Ignoring a low-probability event
 - B) Purchasing cyber insurance
 - C) Installing a firewall to block threats
 - D) Documenting a risk acceptance form
-

Q22.

An attacker is trying multiple passwords against many different user accounts. What is this called?

- A) Dictionary Attack
 - B) Brute Force Attack
 - C) Password Spraying
 - D) Rainbow Table Attack
-

Q23.

What is the purpose of a disaster recovery plan (DRP)?

- A) Prevent data breaches
 - B) Maintain operations during an attack
 - C) Restore critical business systems after disruption
 - D) Identify vulnerabilities before attacks occur
-

Q24.

Which concept ensures that sensitive data is only accessible to authorized individuals?

- A) Integrity
 - B) Confidentiality
 - C) Availability
 - D) Authentication
-

Q25.

Which of the following BEST describes a vulnerability scanner?

- A) Blocks malicious traffic at the network perimeter
 - B) Actively exploits vulnerabilities
 - C) Passively identifies potential weaknesses
 - D) Encrypts sensitive communications
-

Q26.

Which of the following technologies uses security groups and microsegmentation to enhance cloud security?

- A) VPNs
 - B) Infrastructure as Code
 - C) Cloud-native firewalls
 - D) Software-Defined Networking (SDN)
-

Q27.

A system administrator wants to monitor failed login attempts centrally. Which system should be deployed?

- A) SIEM
 - B) NAC
 - C) DLP
 - D) SOAR
-

Q28.

Which attack occurs when a malicious actor manipulates a DNS server to redirect traffic to fraudulent websites?

- A) DNS Poisoning
 - B) Domain Hijacking
 - C) IP Spoofing
 - D) ARP Poisoning
-

Q29.

A company requires users to authenticate once and then have access to multiple systems without re-entering credentials. Which solution BEST meets this requirement?

- A) Federation
- B) LDAP

- C) Multifactor Authentication
 - D) VPN
-

Q30.

Which backup strategy would provide the QUICKEST recovery time in case of a server failure?

- A) Full Backup
 - B) Differential Backup
 - C) Incremental Backup
 - D) Snapshot Backup
-

Answers and Explanations 21–30

A21.

Answer: C) Installing a firewall to block threats

Explanation:

Mitigation adds controls to reduce risk likelihood or impact.

A22.

Answer: C) Password Spraying

Explanation:

Password spraying tries common passwords across many accounts to avoid lockout.

A23.

Answer: C) Restore critical business systems after disruption

Explanation:

DRP focuses on system recovery after disaster events.

A24.

Answer: B) Confidentiality

Explanation:

Confidentiality ensures sensitive data isn't disclosed to unauthorized users.

A25.

Answer: C) Passively identifies potential weaknesses

Explanation:

Vulnerability scanners find weaknesses but don't exploit them.

A26.

Answer: D) Software-Defined Networking (SDN)

Explanation:

SDN uses segmentation and programmable security in cloud environments.

A27.

Answer: A) SIEM

Explanation:

SIEM collects and analyzes logs, including login failures.

A28.

Answer: A) DNS Poisoning

Explanation:

DNS poisoning manipulates DNS to redirect users to malicious sites.

A29.

Answer: A) Federation

Explanation:

Federation allows single authentication across multiple domains or systems.

A30.

Answer: D) Snapshot Backup

Explanation:

Snapshots allow rapid rollback to a known good system state.

Practice Questions 31–40

Q31.

Which principle ensures that users are granted only the access necessary to perform their job functions?

- A) Separation of Duties
 - B) Need-to-Know
 - C) Least Privilege
 - D) Role-Based Access Control
-

Q32.

An attacker captures data from a public Wi-Fi network without connecting to it. Which attack is being performed?

- A) Evil Twin
 - B) On-Path Attack (MITM)
 - C) Passive Eavesdropping
 - D) Session Hijacking
-

Q33.

What is the PRIMARY goal of a business impact analysis (BIA)?

- A) Identify and prioritize critical business functions
 - B) Analyze threats against network security
 - C) Determine security control effectiveness
 - D) Perform a penetration test
-

Q34.

What type of backup method would you use if you want to store only the changes made since the last full backup AND you want fast recovery?

- A) Incremental
- B) Full
- C) Differential
- D) Snapshot

Q35.

Which of the following technologies BEST protects against on-path (Man-in-the-Middle) attacks?

- A) VLAN
 - B) IPS
 - C) VPN
 - D) RAID
-

Q36.

During which incident response phase would you isolate a compromised server?

- A) Recovery
 - B) Containment
 - C) Lessons Learned
 - D) Identification
-

Q37.

What security principle is enforced when employees are required to use two different passwords for administrative and non-administrative accounts?

- A) Separation of Duties
 - B) Least Privilege
 - C) Defense in Depth
 - D) Dual Control
-

Q38.

Which cloud model allows the customer the MOST control over the operating system and applications?

- A) SaaS
 - B) PaaS
 - C) IaaS
 - D) FaaS
-

Q39.

What is a PRIMARY security concern with Infrastructure as Code (IaC)?

- A) Outdated server hardware
 - B) Rapid spread of misconfigurations
 - C) Vendor lock-in
 - D) Poor network performance
-

Q40.

An attacker sends unsolicited Bluetooth messages to nearby devices. What attack is this?

- A) Bluesnarfing
 - B) Bluebugging
 - C) Bluejacking
 - D) Bluespoofing
-

Answers and Explanations 31–40

A31.

Answer: C) Least Privilege

Explanation:

Least privilege gives users only necessary access rights to do their jobs.

A32.

Answer: C) Passive Eavesdropping

Explanation:

Passive eavesdropping listens to network traffic without active interception.

A33.

Answer: A) Identify and prioritize critical business functions

Explanation:

BIA identifies essential processes and their recovery priorities.

A34.

Answer: C) Differential

Explanation:

Differential backups capture changes since last full backup and restore faster than incremental.

A35.

Answer: C) VPN

Explanation:

VPNs encrypt traffic, preventing interception and tampering in on-path attacks.

A36.

Answer: B) Containment

Explanation:

Containment limits the spread of the incident, like isolating a server.

A37.

Answer: A) Separation of Duties

Explanation:

Separating credentials for admin and user accounts supports separation of duties.

A38.

Answer: C) IaaS

Explanation:

In Infrastructure as a Service (IaaS), the customer manages OS, apps, and configurations.

A39.

Answer: B) Rapid spread of misconfigurations

Explanation:

laC errors can quickly replicate insecure settings across environments.

A40.**Answer:** C) Bluejacking**Explanation:**

Bluejacking involves sending unsolicited Bluetooth messages to devices.

Practice Questions 41–50

Q41.

Which of the following BEST describes a cold site?

- A) Operational data center ready for immediate use
 - B) Empty facility with basic infrastructure like power and HVAC
 - C) Fully equipped center with real-time data replication
 - D) Offsite cloud backup provider
-

Q42.

Which access control method enforces strict policies based on security labels such as “Confidential” or “Top Secret”?

- A) DAC
 - B) RBAC
 - C) MAC
 - D) ABAC
-

Q43.

An employee plugs a personal USB drive into a company workstation without approval. What risk does this primarily represent?

- A) Insider Threat
 - B) Phishing Attack
 - C) Supply Chain Attack
 - D) Business Email Compromise
-

Q44.

Which protocol secures email communication by digitally signing and encrypting messages?

- A) TLS
- B) S/MIME
- C) SSH
- D) SSL

Q45.

Which type of control is implementing a security awareness training program?

- A) Physical
 - B) Technical
 - C) Preventive
 - D) Administrative
-

Q46.

What is the MOST appropriate tool to use when wanting to aggregate, correlate, and analyze logs from multiple systems?

- A) VPN
 - B) Firewall
 - C) SIEM
 - D) NAC
-

Q47.

Which of the following would MOST help prevent unauthorized physical access to a data center?

- A) IDS
 - B) Biometric Access Controls
 - C) VPN
 - D) Anti-Malware
-

Q48.

What security concept involves separating services and functions into isolated containers to minimize the attack surface?

- A) Microsegmentation
 - B) Defense in Depth
 - C) Least Privilege
 - D) Data Sovereignty
-

Q49.

An attacker successfully tricks a user into giving up login credentials via a fake login page. What attack technique was used?

- A) Spear Phishing
 - B) Vishing
 - C) Smishing
 - D) Pharming
-

Q50.

Which phase of the incident response process involves finding and removing malware from infected systems?

- A) Preparation
 - B) Containment
 - C) Eradication
 - D) Lessons Learned
-

Answers and Explanations 41–50

A41.

Answer: B) Empty facility with basic infrastructure like power and HVAC

Explanation:

A cold site is ready with essentials but needs equipment and data to become operational.

A42.

Answer: C) MAC

Explanation:

Mandatory Access Control uses labels like “Top Secret” to strictly control access.

A43.

Answer: A) Insider Threat

Explanation:

Unauthorized devices plugged into company systems pose insider risks.

A44.**Answer:** B) S/MIME**Explanation:**

S/MIME secures email with digital signatures and encryption.

A45.**Answer:** D) Administrative**Explanation:**

Security training programs are administrative controls (policy/procedure related).

A46.**Answer:** C) SIEM**Explanation:**

A SIEM collects and analyzes logs from across the enterprise.

A47.**Answer:** B) Biometric Access Controls**Explanation:**

Biometrics (like fingerprints) are effective physical security measures.

A48.**Answer:** A) Microsegmentation**Explanation:**

Microsegmentation isolates workloads to minimize lateral movement risk.

A49.**Answer:** A) Spear Phishing

Explanation:

Spear phishing targets individuals with highly customized fake login pages.

A50.

Answer: C) Eradication

Explanation:

Eradication is when you remove malware or vulnerabilities after containment.

Practice Questions 51–60

Q51.

Which security tool uses signatures and anomaly detection to identify malicious network traffic?

- A) Firewall
 - B) SIEM
 - C) IDS
 - D) DLP
-

Q52.

A company wants to ensure that employees can recover their files after a ransomware attack without paying the ransom. Which control BEST achieves this?

- A) IDS
 - B) Regular Offline Backups
 - C) VPN Access
 - D) Email Filtering
-

Q53.

Which of the following is MOST critical to maintain when preserving digital evidence?

- A) Full Disk Encryption
 - B) Legal Hold
 - C) Chain of Custody
 - D) Incident Triage
-

Q54.

A company configures a cloud storage bucket and mistakenly leaves it open to the public. What type of vulnerability is this?

- A) Zero-Day
- B) Misconfiguration
- C) Insider Threat
- D) Malware Infection

Q55.

Which layer of the OSI model does a firewall operate primarily at?

- A) Application
 - B) Transport
 - C) Network
 - D) Data Link
-

Q56.

What security concept is enforced when two employees are required to approve a wire transfer above a certain dollar amount?

- A) Dual Control
 - B) Least Privilege
 - C) Discretionary Access Control
 - D) Federation
-

Q57.

Which cryptographic concept is used to ensure message integrity?

- A) Symmetric Encryption
 - B) Asymmetric Encryption
 - C) Hashing
 - D) Key Exchange
-

Q58.

What is the purpose of tokenization in data security?

- A) Encrypt sensitive data
 - B) Replace sensitive data with non-sensitive placeholders
 - C) Hash sensitive data
 - D) Create a secure communication channel
-

Q59.

Which type of backup provides the FASTEST full system recovery after a catastrophic failure?

- A) Incremental
 - B) Full Backup
 - C) Differential
 - D) Cloud Backup
-

Q60.

A team uses a sandbox environment to open suspicious files. What type of control is this?

- A) Preventive
 - B) Detective
 - C) Corrective
 - D) Compensating
-

Answers and Explanations 51–60

A51.

Answer: C) IDS

Explanation:

An IDS detects threats by matching signatures or identifying anomalies.

A52.

Answer: B) Regular Offline Backups

Explanation:

Offline backups protect against ransomware by providing safe recovery data.

A53.

Answer: C) Chain of Custody

Explanation:

Chain of custody ensures evidence integrity for legal use.

A54.

Answer: B) Misconfiguration

Explanation:

Leaving a cloud bucket public is a classic misconfiguration vulnerability.

A55.

Answer: C) Network

Explanation:

Firewalls operate mainly at Layer 3 (Network layer) — managing IP addresses and traffic.

A56.

Answer: A) Dual Control

Explanation:

Dual control requires two people to authorize a sensitive action.

A57.

Answer: C) Hashing

Explanation:

Hashing ensures data integrity by generating a fixed fingerprint of data.

A58.

Answer: B) Replace sensitive data with non-sensitive placeholders

Explanation:

Tokenization replaces real data with fake tokens to protect sensitive information.

A59.

Answer: B) Full Backup

Explanation:

Full backups allow the quickest recovery without relying on incremental data restoration.

A60.

Answer: A) Preventive

Explanation:

Sandboxes are preventive, isolating suspicious files before damage can occur.

Practice Questions 61–70

Q61.

Which of the following is a PRIMARY characteristic of a rootkit?

- A) Encrypts files and demands ransom
 - B) Hides its existence by manipulating the OS
 - C) Replicates itself across the network
 - D) Sends unsolicited messages via Bluetooth
-

Q62.

An organization wants to minimize data loss during a disaster. Which metric defines the maximum amount of data loss acceptable?

- A) RTO
 - B) MTD
 - C) RPO
 - D) ALE
-

Q63.

Which wireless security protocol is considered obsolete and should NOT be used?

- A) WPA2
 - B) WPA
 - C) WPA3
 - D) WEP
-

Q64.

A system administrator is deploying security patches to all systems automatically after testing. This is an example of:

- A) Change Management
 - B) Patch Management
 - C) Hardening
 - D) Incident Response
-

Q65.

What type of malware restricts access to a system until payment is made?

- A) Trojan
 - B) Worm
 - C) Spyware
 - D) Ransomware
-

Q66.

Which term describes isolating different departments in a network to improve security?

- A) Subnetting
 - B) Virtualization
 - C) Network Segmentation
 - D) Packet Filtering
-

Q67.

What concept does the principle of "never trust, always verify" relate to?

- A) VPN
 - B) Zero Trust
 - C) Single Sign-On
 - D) Role-Based Access Control
-

Q68.

Which tool is specifically designed to discover vulnerabilities in a system but NOT exploit them?

- A) Penetration Test
 - B) Exploit Framework
 - C) Vulnerability Scanner
 - D) SIEM
-

Q69.

An employee receives a fake call pretending to be IT support asking for a password. What attack is this?

- A) Phishing
- B) Vishing

- C) Smishing
 - D) Spear Phishing
-

Q70.

A user logs into an internal website using a badge and PIN. What authentication factors are being used?

- A) Something you know and something you are
 - B) Something you know and something you have
 - C) Something you have and something you are
 - D) Two instances of something you know
-

Answers and Explanations 61–70

A61.

Answer: B) Hides its existence by manipulating the OS

Explanation:

Rootkits hide their presence by modifying OS functions to avoid detection.

A62.

Answer: C) RPO

Explanation:

Recovery Point Objective defines the maximum acceptable data loss.

A63.

Answer: D) WEP

Explanation:

WEP is outdated and insecure — easily cracked in minutes.

A64.

Answer: B) Patch Management

Explanation:

Patch management involves scheduling and deploying updates systematically.

A65.

Answer: D) Ransomware

Explanation:

Ransomware encrypts systems/files and demands payment for access.

A66.

Answer: C) Network Segmentation

Explanation:

Segmentation isolates different parts of the network for better control and security.

A67.

Answer: B) Zero Trust

Explanation:

Zero Trust always requires verification, regardless of network location.

A68.

Answer: C) Vulnerability Scanner

Explanation:

Vulnerability scanners detect weaknesses without active exploitation.

A69.

Answer: B) Vishing

Explanation:

Vishing is phishing conducted over the telephone.

A70.

Answer: B) Something you know and something you have

Explanation:

PIN = something you know; Badge = something you have.

Practice Questions 71–80

Q71.

Which technology allows secure remote access to a corporate network by encrypting all traffic?

- A) VLAN
 - B) IDS
 - C) VPN
 - D) Proxy Server
-

Q72.

An employee leaves a confidential document on a shared printer. What kind of risk is this?

- A) Insider Threat
 - B) Physical Security Risk
 - C) Supply Chain Risk
 - D) Malware Infection
-

Q73.

Which of the following would MOST effectively prevent malware from executing on endpoints?

- A) Application Allowlisting
 - B) IDS Deployment
 - C) SSL/TLS Encryption
 - D) Role-Based Access Control
-

Q74.

A company requires that users verify their identity using a username, password, and fingerprint scan. This is an example of:

- A) Multi-Factor Authentication
- B) Federation
- C) SSO
- D) Kerberos Authentication

Q75.

Which security principle ensures that critical functions are divided among multiple people to prevent fraud?

- A) Least Privilege
 - B) Separation of Duties
 - C) Job Rotation
 - D) Dual Control
-

Q76.

What technique is used by attackers to overload a server with requests, causing service disruption?

- A) SQL Injection
 - B) DNS Poisoning
 - C) DDoS Attack
 - D) ARP Spoofing
-

Q77.

Which of the following devices inspects and filters packets based on application-level data?

- A) Traditional Firewall
 - B) Proxy Server
 - C) Next-Generation Firewall (NGFW)
 - D) Router
-

Q78.

Which method ensures that a user cannot deny performing an action, such as sending an email?

- A) Non-Repudiation
 - B) Availability
 - C) Encryption
 - D) Role-Based Access Control
-

Q79.

An attacker exploits a race condition in a web application. What is this an example of?

- A) Improper Input Handling
 - B) Application Logic Flaw
 - C) Secure Coding Practice
 - D) Race Attack Vulnerability
-

Q80.

Which of the following is a benefit of implementing Infrastructure as Code (IaC) securely?

- A) Manual configuration of servers
 - B) Consistent and repeatable deployments
 - C) Physical separation of networks
 - D) Encrypted communication tunnels
-

Answers and Explanations 71–80

A71.

Answer: C) VPN

Explanation:

A VPN encrypts data between remote users and corporate networks.

A72.

Answer: B) Physical Security Risk

Explanation:

Leaving sensitive documents in shared spaces risks unauthorized access.

A73.

Answer: A) Application Allowlisting

Explanation:

Only approved apps can run, blocking unknown malware.

A74.

Answer: A) Multi-Factor Authentication

Explanation:

Using two or more different authentication types (password + fingerprint).

A75.

Answer: B) Separation of Duties

Explanation:

No one person controls all parts of a critical process, preventing fraud.

A76.

Answer: C) DDoS Attack

Explanation:

Distributed Denial of Service floods a server with traffic.

A77.

Answer: C) Next-Generation Firewall (NGFW)

Explanation:

NGFWs inspect packets deeply, including application-level data.

A78.

Answer: A) Non-Repudiation

Explanation:

Non-repudiation ensures proof of actions like sending emails.

A79.

Answer: D) Race Attack Vulnerability

Explanation:

Race conditions exploit timing issues in applications.

A80.

Answer: B) Consistent and repeatable deployments

Explanation:

IaC enables secure, automated, consistent infrastructure setup.

Practice Questions 81–90

Q81.

Which of the following BEST describes the primary benefit of implementing a SIEM system?

- A) Blocking unauthorized access attempts
 - B) Preventing malware infections
 - C) Aggregating and analyzing security logs centrally
 - D) Encrypting sensitive data at rest
-

Q82.

What is the MAIN purpose of a DLP (Data Loss Prevention) system?

- A) Detect malware signatures
 - B) Monitor unauthorized data transfers
 - C) Block phishing emails
 - D) Scan networks for vulnerabilities
-

Q83.

An attacker tricks a user into resetting their password by spoofing a legitimate password reset page. What kind of attack is this?

- A) Phishing
 - B) SQL Injection
 - C) Session Hijacking
 - D) Privilege Escalation
-

Q84.

Which backup method copies only the files that have changed since the last backup, no matter what type it was?

- A) Full
- B) Incremental
- C) Differential
- D) Snapshot

Q85.

What does the principle of Defense in Depth emphasize?

- A) Using multiple layers of security controls
 - B) Deploying only firewalls at the network perimeter
 - C) Using two-factor authentication for all logins
 - D) Relying primarily on SIEM alerts
-

Q86.

Which of the following is an example of an administrative control?

- A) Fire extinguisher in server room
 - B) Firewall rules
 - C) Security awareness policy
 - D) Encryption of data at rest
-

Q87.

A SOC analyst notices large outbound traffic to an unknown IP. What is the BEST immediate action?

- A) Shut down all network switches
 - B) Disconnect affected systems
 - C) Reboot affected systems
 - D) Call the ISP
-

Q88.

Which term describes unauthorized commands sent from a user's browser to a trusted website?

- A) Cross-Site Scripting (XSS)
 - B) SQL Injection
 - C) Command Injection
 - D) Cross-Site Request Forgery (CSRF)
-

Q89.

Which of the following technologies enables a single identity to access multiple

applications across different domains?

- A) Multifactor Authentication
 - B) Federation
 - C) VPN
 - D) Zero Trust
-

Q90.

What is the FIRST action to take when you detect an active ransomware infection?

- A) Pay the ransom
 - B) Disconnect infected systems from the network
 - C) Run antivirus scan
 - D) Contact cloud backup provider
-

Answers and Explanations 81–90

A81.

Answer: C) Aggregating and analyzing security logs centrally

Explanation:

SIEM systems collect logs from multiple sources for centralized analysis.

A82.

Answer: B) Monitor unauthorized data transfers

Explanation:

DLP systems prevent sensitive data from leaving the network.

A83.

Answer: A) Phishing

Explanation:

Spoofed password reset pages are classic phishing attacks.

A84.

Answer: B) Incremental

Explanation:

Incremental backups save changes since the last backup (full or incremental).

A85.

Answer: A) Using multiple layers of security controls

Explanation:

Defense in Depth means no single point of failure.

A86.

Answer: C) Security awareness policy

Explanation:

Administrative controls include policies and procedures.

A87.

Answer: B) Disconnect affected systems

Explanation:

Disconnect immediately to prevent further data exfiltration.

A88.

Answer: D) Cross-Site Request Forgery (CSRF)

Explanation:

CSRF tricks users into executing unwanted actions.

A89.

Answer: B) Federation

Explanation:

Federation allows single login across multiple organizations/systems.

A90.

Answer: B) Disconnect infected systems from the network

Explanation:

Isolate first to stop the spread of ransomware.

Practice Questions 91–100

Q91.

Which of the following terms describes preventing unauthorized access by forcing a user to authenticate again after a period of inactivity?

- A) Session Lock
 - B) Password Complexity
 - C) Single Sign-On
 - D) Federation
-

Q92.

What type of test involves assessing the physical, administrative, and technical safeguards without exploiting vulnerabilities?

- A) Vulnerability Scan
 - B) Penetration Test
 - C) Risk Assessment
 - D) Business Impact Analysis
-

Q93.

Which component is critical for ensuring confidentiality when sending sensitive data across the Internet?

- A) Hashing
 - B) Encryption
 - C) Load Balancing
 - D) IDS
-

Q94.

What is the purpose of implementing redundant power supplies in servers?

- A) Improve encryption performance
- B) Increase network bandwidth
- C) Enhance system availability
- D) Provide faster processing

Q95.

Which of the following MOST accurately defines tokenization?

- A) Encrypting all data in a database
 - B) Replacing sensitive data elements with a unique identifier
 - C) Hashing user passwords before storage
 - D) Obfuscating source code to protect intellectual property
-

Q96.

An attacker uses a vulnerability in a software program that has not yet been patched. What kind of attack is this?

- A) Zero-Day
 - B) Man-in-the-Middle
 - C) Cross-Site Scripting
 - D) Phishing
-

Q97.

What is the BEST method to mitigate the impact of social engineering attacks?

- A) Install firewalls
 - B) Security Awareness Training
 - C) Regular Penetration Testing
 - D) Conduct Full Backups
-

Q98.

Which type of malware is specifically designed to provide persistent, hidden access to a compromised system?

- A) Ransomware
 - B) Trojan
 - C) Rootkit
 - D) Worm
-

Q99.

A backup strategy uses the Grandfather-Father-Son method. What is this primarily

designed to achieve?

- A) Ensure zero data loss
 - B) Maintain multiple historical versions of backups
 - C) Accelerate disaster recovery
 - D) Improve real-time replication
-

Q100.

What security tool intercepts and controls traffic between a user and the Internet to enforce company policies?

- A) Firewall
 - B) VPN
 - C) Proxy Server
 - D) Load Balancer
-

Answers and Explanations 91–100

A91.

Answer: A) Session Lock

Explanation:

Session locks require reauthentication after inactivity to prevent unauthorized access.

A92.

Answer: C) Risk Assessment

Explanation:

Risk assessments evaluate safeguards without actively exploiting vulnerabilities.

A93.

Answer: B) Encryption

Explanation:

Encryption protects data confidentiality during transmission.

A94.

Answer: C) Enhance system availability

Explanation:

Redundant power supplies help keep servers running during power failures.

A95.

Answer: B) Replacing sensitive data elements with a unique identifier

Explanation:

Tokenization swaps real data for safe, meaningless tokens.

A96.

Answer: A) Zero-Day

Explanation:

Zero-day attacks exploit unknown or unpatched vulnerabilities.

A97.

Answer: B) Security Awareness Training

Explanation:

Training users helps them recognize and avoid social engineering.

A98.

Answer: C) Rootkit

Explanation:

Rootkits maintain hidden, persistent access by deeply integrating with systems.

A99.

Answer: B) Maintain multiple historical versions of backups

Explanation:

Grandfather-Father-Son rotation ensures backup version history.

A100.

Answer: C) Proxy Server

Explanation:

Proxies filter, control, and log user Internet traffic to enforce policies.