Free Security+ Practice Test

Free Security+ Practice Test - Updated for SY0-701

30 Questions + Answer Explanations

Updated 2026 | Strategy Box for each question | Answer Key Included

1

Which attack involves overwhelming a system with traffic from multiple compromised devices?

A Phishing | B DDoS | C Brute force | D Spoofing

STRATEGY BOX:

A Distributed Denial of Service (DDoS) attack uses multiple systems (a botnet) to flood a target, making services unavailable.

✓ **Correct Answer: B. DDoS**

2

What type of malware encrypts data and demands payment for decryption?

A Trojan | B Ransomware | C Worm | D Adware

STRATEGY BOX:

Ransomware encrypts files and demands ransom, spreading through phishing or malicious downloads.

✓ **Correct Answer: B. Ransomware**

3

Which attack exploits human trust to steal sensitive information?

A SQL injection | B Phishing | C MITM | D DoS

STRATEGY BOX:

Phishing depends on deception through emails or messages to trick users into revealing credentials or data.

✓ **Correct Answer: B. Phishing**

4

What is the primary goal of a man-in-the-middle (MITM) attack?

A Crash servers | B Intercept communication | C Delete files | D Encrypt data

STRATEGY BOX:

MITM attacks intercept and possibly alter communication between two parties without their knowledge.

✓ **Correct Answer: B. Intercept communication**

5

Which attack manipulates SQL queries to access unauthorized data?

A Cross-site scripting | B SQL injection | C Brute force | D Session hijacking

STRATEGY BOX:

SQL injection inserts malicious code into input fields to manipulate database queries.

✓ **Correct Answer: B. SQL injection**

6

What type of attack uses repeated password guesses?

A Dictionary attack | B Brute force attack | C Replay attack | D Smurf attack

STRATEGY BOX:

Brute force systematically tries all password combinations until the correct one is found.

✓ **Correct Answer: B. Brute force attack**

7

Which attack exploits vulnerabilities in web applications by injecting scripts?

A XSS | B DDoS | C ARP poisoning | D DNS poisoning

STRATEGY BOX:

Cross-site scripting (XSS) injects malicious scripts into trusted websites.

✓ **Correct Answer: A. XSS**

8

What is the goal of credential stuffing attacks?

A Encrypt traffic | B Reuse leaked credentials | C Block users | D Scan ports

STRATEGY BOX:

Credential stuffing uses stolen username-password pairs across multiple sites.

✓ **Correct Answer: B. Reuse leaked credentials**

9

Which attack involves redirecting traffic to fake websites?

A DNS spoofing | B Phishing | C Keylogging | D Smishing

STRATEGY BOX:

DNS spoofing manipulates DNS records to redirect users to malicious sites.

DNS spoofing manipulates DNS records to redirect users to malicious sites.

✓ **Correct Answer: A. DNS spoofing**

10

What is the purpose of a zero-day exploit?

A Patch systems	**B** Use unknown vulnerabilities	**C** Encrypt data	**D** Monitor traffic

STRATEGY BOX:

Zero-day exploits target vulnerabilities unknown to vendors, leaving no available patch.

✓ **Correct Answer: B. Use unknown vulnerabilities**

11

What is the first step in risk management?

A Mitigation	**B** Risk identification	**C** Monitoring	**D** Transfer

STRATEGY BOX:

Risks must be identified before they can be assessed or mitigated.

✓ **Correct Answer: B. Risk identification**

12

What does vulnerability scanning primarily do?

A Encrypt data	**B** Detect system weaknesses	**C** Block attacks	**D** Monitor bandwidth

STRATEGY BOX:

It identifies known security flaws in systems and applications.

✓ **Correct Answer: B. Detect system weaknesses**

13

Which tool simulates attacks to test system security?

A SIEM	**B** Penetration testing	**C** Firewall	**D** Antivirus

STRATEGY BOX:

Penetration testing actively exploits vulnerabilities to assess security posture.

✓ **Correct Answer: B. Penetration testing**

14

What is risk acceptance?

A Fixing vulnerabilities | B Ignoring all risks | C Accepting potential impact without action | D Transferring risk

STRATEGY BOX:
Organizations may accept risk if the mitigation cost exceeds the impact.

✓ **Correct Answer: C. Accepting potential impact without action**

15

What is a false positive in vulnerability scanning?

A Real attack detected | B Non-existent vulnerability flagged | C System crash | D Malware infection

STRATEGY BOX:
A false positive incorrectly identifies a harmless condition as a threat.

✓ **Correct Answer: B. Non-existent vulnerability flagged**

16

What is the purpose of patch management?

A Increase bandwidth | B Fix known vulnerabilities | C Encrypt files | D Monitor users

STRATEGY BOX:
Patch management updates software to fix security weaknesses.

✓ **Correct Answer: B. Fix known vulnerabilities**

17

What is residual risk?

A Total eliminated risk | B Risk after controls are applied | C New risk introduced | D Ignored risk

STRATEGY BOX:
It is the remaining risk after security measures are implemented.

✓ **Correct Answer: B. Risk after controls are applied**

18

What does CVSS measure?

A Encryption strength | B Vulnerability severity | C Network speed | D Firewall rules

STRATEGY BOX:
Common Vulnerability Scoring System rates the severity of vulnerabilities.

✓ **Correct Answer: B. Vulnerability severity**

19

What is the goal of risk transference?

- **A** Remove risk
- **B** Shift risk to third party
- **C** Ignore risk
- **D** Increase risk

STRATEGY BOX:

Insurance or outsourcing transfers financial impact to another party.

✓ **Correct Answer: B. Shift risk to third party**

20

Which document defines acceptable risk levels?

- **A** SLA
- **B** Risk appetite statement
- **C** Firewall policy
- **D** Audit log

STRATEGY BOX:

It defines how much risk an organization is willing to tolerate.

✓ **Correct Answer: B. Risk appetite statement**

21

What is the core principle of Zero Trust?

- **A** Trust internal users
- **B** Never trust, always verify
- **C** Block all traffic
- **D** Open access internally

STRATEGY BOX:

Zero Trust assumes no implicit trust and requires continuous verification.

✓ **Correct Answer: B. Never trust, always verify**

22

What does network segmentation achieve?

- **A** Increase speed
- **B** Limit lateral movement
- **C** Remove firewalls
- **D** Encrypt traffic

STRATEGY BOX:

It isolates network parts to prevent attacker movement.

✓ **Correct Answer: B. Limit lateral movement**

23

What is the role of a DMZ?

- **A** Encrypt data
- **B** Separate public services from the internal network
- **C** Block all traffic
- **D** Store backups

STRATEGY BOX:

A DMZ provides controlled access to public-facing services.

✓ **Correct Answer: B. Separate public services from the internal network**

24

What is cloud hybrid architecture?

A Only on-prem systems	B Combination of cloud and on-prem resources	C No cloud usage	D Peer-to-peer network

STRATEGY BOX:

Hybrid environments combine local and cloud infrastructure.

✓ **Correct Answer: B. Combination of cloud and on-prem resources**

25

What is the function of a VPN?

A Increase bandwidth	B Secure encrypted tunnel	C Scan viruses	D Block websites

STRATEGY BOX:

VPNs create encrypted communication channels over public networks.

✓ **Correct Answer: B. Secure encrypted tunnel**

26

What is identity federation?

A Multiple passwords	B Shared authentication across systems	C Firewall rule	D Antivirus method

STRATEGY BOX:

It allows users to access multiple systems using one identity.

✓ **Correct Answer: B. Shared authentication across systems**

27

What does MFA improve?

A Network speed	B Authentication security	C Storage capacity	D CPU performance

STRATEGY BOX:

Multi-factor authentication adds layers beyond passwords.

✓ **Correct Answer: B. Authentication security**

28

What is the purpose of a SIEM system?

- **A** Encrypt data
- **B** Centralized log monitoring
- **C** Block attacks
- **D** Manage users

STRATEGY BOX:

SIEM collects and analyzes security events in real time.

✓ **Correct Answer: B. Centralized log monitoring**

29

What is the least privileged principle?

- **A** Maximum access
- **B** Minimum necessary access
- **C** Guest access
- **D** Admin access

STRATEGY BOX:

Users only get the permissions required for their role.

✓ **Correct Answer: B. Minimum necessary access**

30

What does endpoint detection and response (EDR) do?

- **A** Stores backups
- **B** Monitors and responds to endpoint threats
- **C** Encrypts files
- **D** Manages DNS

STRATEGY BOX:

EDR detects suspicious activity on endpoints and responds in real time.

✓ **Correct Answer: B. Monitors and responds to endpoint threats**