CompTIA Security+ Exam Preps

Free Practice Test — 30 Real Exam-Style Questions

with full answer key & explanations

Unlock the full bank of 1172 questions
+ unlimited timed mock exams + mistake book

Practice on the web: https://certs.theorypractice.app/comptiasecurity
$2.99 / week · $6.99 / month · cancel anytime

What you unlock: all 1172 questions • unlimited timed mock exams • mistake book • instant explanations

Study offline on the free app — search your exam on the App Store or Google Play

Practice Questions

Try all 30 first, then check the answer key at the back.

1. A company needs to secure communication between multiple branch offices over the internet. Which technology would suit this requirement?

A. Firewall
B. Load balancer
C. Proxy server
D. VPN

2. In the context of wireless security protocols, what is the primary purpose of the WPA2 protocol?

A. Integrity
B. Encryption
C. Key exchange
D. Authentication

3. A growing organization wants to ensure that its employees can access important documents and collaborate seamlessly. They are looking for a solution that allows for file redundancy and does not rely on an expensive, centralized server infrastructure. What would be the best option to provide network-connected storage with redundancy, similar to RAID 1 mirroring?

A. External Hard Drive
B. Cloud-Based Storage
C. DAS (Direct Attached Storage)
D. NAS

4. Review the following description and identify which cloud computing model is being referenced: A cloud environment that offers computing resources such as virtual machines, storage, and networking on a pay-as-you-go basis, enabling the deployment and operation of personal or business applications.

A. XaaS
B. IaaS
C. SaaS
D. PaaS

5. A network administrator notices that their network is experiencing delays and high latency. They determine that one part of the network needs to be able to communicate data more quickly and efficiently within a specific segment. What type of network topology would best allow for direct data transmission between multiple devices within the same segment?

A. Star
B. Bus
C. Ring
D. Mesh

6. You are providing cybersecurity consulting for a healthcare enterprise concerned about unauthorized access to their patient records. Which of the following is an effective measure to enhance the security of their database systems?

A. Implement regular security updates and patches
B. Increase the frequency of data backups
C. Enable daily system reboots
D. Conduct thorough scans once a month

7. An organization needs to adopt a streamlined approach to manage its cloud infrastructure more effectively. They are looking for a methodology to plan, deploy, and manage their cloud services efficiently. Which of the following methodologies should the organization choose?

A. Service-oriented architecture
B. Cloud service life cycle
C. Cloud patch management
D. Cloud deployment testing

8. Understanding the various security zones is crucial in designing secure network architectures. Which type of zone is primarily used to host publicly accessible services, such as web servers?

A. Internal Network
B. Guest Network
C. VLAN (Virtual Local Area Network)
D. DMZ (Demilitarized Zone)

9. An organization has identified that its email communications are at risk of interception and wants to ensure that emails are encrypted during transmission. The solution should utilize TLS for encryption, leveraging existing security infrastructure. Which of the following protocols should the organization implement?

A. POP3
B. IMAP
C. SMTP with STARTTLS
D. SMTP

10. A network engineer is configuring a VPN and needs to use a protocol that ensures secure communication by providing end-to-end encryption, mutual authentication, and data integrity. Which protocol should they implement?

A. AH
B. L2TP
C. PPTP
D. ESP

11. A network administrator is looking to implement secure file transfer across the organization's internal network. The network already has a PKI set up for internal use, and the administrator wants to leverage this existing infrastructure. Which of the following protocols should they implement?

A. HTTP
B. FTPS
C. FTP
D. SCP

12. Which software development methodology was introduced by Kent Beck and emphasizes customer satisfaction, speed, and flexibility?

A. Scrum
B. Lean
C. Extreme Programming (XP)
D. Waterfall

13. An IT administrator needs to configure firewall rules and wants to specify which types of network traffic are permissible. What part of the firewall rules specifies the traffic that should be allowed?

A. Deny rule
B. Log rule
C. Monitor rule
D. Allow rule

14. Which of the following methods is designed to discover encryption keys by trying common phrases and words?

A. Password spraying attack
B. Dictionary attack
C. Brute force attack
D. Rainbow table attack

15. An attacker has intercepted an encrypted communications channel and managed to obtain encrypted messages. They then utilize a precomputed set of hash values to recover the original messages. Which type of attack employs precomputed hash values to decrypt previously intercepted encrypted data?

A. Rainbow table attack
B. Brute force attack
C. Man-in-the-middle attack
D. Phishing attack

16. A financial analyst within a company receives a personalized email that requests an Excel file containing the latest quarterly earnings report. The email appears to be from a senior executive and includes specific details about recent company meetings. What type of targeted phishing attack is this?

A. Whaling
B. Pharming
C. Tailgating
D. Spear phishing

17. A university decided to force students to use their campus network and not personal cellular data. They used a device to interrupt students' cellular signals, making it difficult for them to access the network via their mobile data. Which of the following devices did they MOST LIKELY use?

A. Load balancers
B. Proxy servers
C. Cellular jammers
D. Firewalls

18. During a wireless authentication process, a user unknowingly connects to a rogue access point masquerading as a legitimate one. This allows an attacker to intercept and eavesdrop on all communications between the user and the actual network. Which type of attack permits an attacker to intercept and monitor communications by deceiving the user into connecting to a rogue network?

A. DNS Poisoning
B. Trojan Horse
C. Evil Twin
D. Phishing

19. An IT manager receives an urgent email from someone claiming to be the CEO requesting immediate access to confidential files. What term describes the tactic used by the attacker in this social engineering scenario?

A. Pretexting
B. Phishing
C. Spear phishing
D. Watering hole attack

20. An employee at Johnson Corp. notices that their computer is running slower than usual and sees multiple pop-up messages claiming that the system is heavily corrupted. The messages suggest downloading an urgent security update to fix the problem. After installing the suggested update, the employee finds more warnings about system infections and a further decline in computer performance. What is the MOST LIKELY cause of the issue?

A. Trojan
B. Ransomware
C. Adware
D. Phishing

21. An organization is implementing a technology to authenticate users locally without involving remote servers. This technology verifies a user's credentials locally on their device. Which of the following is an example of such a localized authentication method suitable for this situation?

A. Kerberos
B. RADIUS
C. OAuth
D. SAML

22. A security administrator at XYZ Corp. is assessing the organization's security controls and identifying any gaps. They have reviewed access controls, logging mechanisms, network segmentation, and encryption protocols, and have conducted a vulnerability assessment. Which of the following control categories is the administrator auditing?

A. Technical
B. Administrative
C. Physical
D. Detective

23. A compliance officer at Tech Solutions Inc. is evaluating different measures to ensure the security of the company's data. They have completed assessments of encrypting sensitive data, implementing security policies, and using biometric access controls. Which of the following control types is being evaluated?

A. Corrective
B. Compensating
C. Preventive
D. Detective

24. Encryption is an example of which of the following types of security controls?

A. Deterrent
B. Preventative
C. Corrective
D. Compensating

25. Organizations often rely on threat intelligence platforms to predict and respond to potential cyber threats proactively. These platforms play a key role in safeguarding digital assets by providing real-time information on emerging threats. What is one commonly used threat intelligence platform by security professionals?

A. Cyberduck
B. MISP
C. SketchUp
D. Wireshark

26. TechSec Inc. experienced a data breach, and the company is currently under investigation by cybersecurity authorities. TechSec Inc. has been ordered to preserve all electronic communications from the past two years pertinent to the investigation. What action has been implemented in this scenario?

A. An assertion of the chain of custody
B. A data encryption mandate
C. A requirement to perform a vulnerability scan
D. An application of a legal hold

27. A cybersecurity analyst needs to verify that the configuration of two network devices is identical to ensure network integrity. Which of the following actions should they take?

A. Compare checksums of configuration files
B. Manually review configuration settings
C. Run a virus scan on the devices
D. Reset to factory settings and reconfigure

28. Triage of different security events to determine the most serious threat relies on what type of evidence?

A. Admissible
B. Competent
C. Critical
D. Relevant

29. Which of the following tools provides comprehensive cybersecurity threat intelligence reports?

A. Snort
B. tcpdump
C. FireEye
D. Wireshark

30. Which of the following network devices is the MOST volatile? Device Volatility Router High Firewall Medium Switch Low Backup Server Very Low

A. Firewall
B. Switch
C. Router
D. Backup Server

Answer Key & Explanations

1. D — VPN
A VPN (Virtual Private Network) is a technology that establishes a secure connection over the internet, ensuring that data transmitted between branch offices is encrypted and secure.

2. B — Encryption
Answer: Encryption WPA2 (Wi-Fi Protected Access 2) is a security protocol used to protect wireless networks. It provides encryption of data transmitted over the network, ensuring that only authorized devices can access and read the data. While WPA2 incorporates components of key exchange and authentication, its primary function is to encrypt data to maintain confidentiality.

3. D — NAS
Answer: NAS NAS (Network Attached Storage) provides a cost-effective way to ensure file redundancy without relying on a centralized server. Using RAID 1 mirroring, data is duplicated across multiple drives, ensuring that if one drive fails, the other can take over without data loss.

4. B — IaaS
Answer: IaaS Infrastructure as a Service (IaaS) refers to a model where the cloud provider manages the fundamental computing resources like virtual machines, storage, and networking. Customers can then deploy and operate their software applications on this infrastructure. Software as a Service (SaaS) is a model in which the cloud provider develops and offers a fully-managed solution to customers. Examples include Gmail and Office 365. Platform as a Service (PaaS) is a model in which the cloud provider manages an environment where customers can create applications. Examples include hosted development environments, web servers, and databases. Anything as a Service (XaaS) is a broad term that refers to the delivery of various services over the cloud, including SaaS, PaaS, and IaaS.

5. D — Mesh
Answer: Mesh A mesh topology allows for direct data transmission between multiple devices without the need for a central switch or hub. This topology can handle high traffic and reduce latency, making it ideal for efficient communication within a specific segment of the network.

6. A — Implement regular security updates and patches
Correct Answer: Implement regular security updates and patches Applying regular updates and security patches ensures that any identified vulnerabilities in database systems are mitigated promptly. Neglecting updates can leave systems exposed to new threats. Regularly updating and patching systems bolsters their security against potential breaches.

7. B — Cloud service life cycle
Answer: Cloud service life cycle The cloud service life cycle is a framework that helps organizations effectively plan, deploy, manage, and retire cloud services. It typically includes phases such as development, deployment, operation, and decommissioning, ensuring that cloud services are managed efficiently and securely.

8. D — DMZ (Demilitarized Zone)
The DMZ (Demilitarized Zone) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually the internet. This zone adds an additional layer of security to an organization's local area network (LAN) by segregating the external services from the internal network.

9. C — SMTP with STARTTLS
Answer: SMTP with STARTTLS SMTP with STARTTLS is a method used to take advantage of TLS encryption to secure email transmissions. This is critical to protect the data and credentials from potentially being intercepted during transmission. While SMTP by itself sends data in plaintext, STARTTLS upgrades the connection to use TLS. Other protocols like POP3 and IMAP also handle email but without explicit mentioning of using TLS encryption, they're not secure.

10. D — ESP
The Encapsulating Security Payload (ESP) protocol offers encryption, authentication, and integrity for VPNs, which ensures secure communication. ESP can encrypt both the payload and the headers of packets in tunnel mode, providing comprehensive security.

11. B — FTPS
Answer: FTPS FTPS (File Transfer Protocol Secure) allows for secure file transfer and utilizes SSL/TLS for encryption. It can leverage a Public Key Infrastructure (PKI) to manage certificates, ensuring secure and authenticated transfers across the network.

12. C — Extreme Programming (XP)
Answer: Extreme Programming (XP) Extreme Programming (XP) is a software development methodology that emphasizes customer satisfaction, speed, and flexibility. Developed by Kent Beck, XP encourages frequent releases in short development cycles, which improves productivity and introduces checkpoints at which new customer requirements can be adopted. Waterfall, Scrum, and Lean are also software development methodologies but have different principles and practices focused on other aspects of software development.

13. D — Allow rule
Answer: Allow rule Firewall rules consist of different directives for various types of network traffic. An allow rule specifies the traffic that is explicitly permitted to pass through the firewall. Conversely, a deny rule blocks specified traffic. Log rules may record details about traffic without necessarily allowing or denying it, and monitor rules could be used to observe traffic patterns.

14. B — Dictionary attack
Answer: Dictionary attack A dictionary attack targets encryption keys by trying variants of common phrases and words, similar to how it targets passwords. A brute force attack attempts every possible key, which guarantees eventual success but can be time-consuming. A rainbow table attack involves precomputing a lookup table for keys and their hashes, effective against unsalted encryption. Password spraying attacks use a single weak key on many different encrypted files or accounts.

15. A — Rainbow table attack
Rainbow table attacks utilize precomputed hash tables to quickly convert encrypted hash values back to their original plaintext form without brute-force computation.

16. D — Spear phishing
Spear phishing attacks are highly targeted attacks where attackers use specific information about the victim or their organization to make the attack seem more credible. In this case, the attacker uses details about recent meetings to make the financial analyst believe the email is legitimate.

17. C — Cellular jammers
Answer: Cellular jammers Cellular jammers can be used to interrupt cellular signals. They can be employed to disrupt mobile data connections by creating interference that blocks mobile communication.

18. C — Evil Twin
Answer: Evil Twin. An evil twin attack involves setting up a rogue access point that appears to be legitimate, tricking users into connecting to it. Once the connection is established, the attacker can intercept and eavesdrop on the communications between the user and the actual network. This type of attack exploits the wireless authentication process.

19. A — Pretexting
Answer: Pretexting Pretexting is part of social engineering. The attacker creates a convincing scenario or pretext to deceive the victim into revealing sensitive information, often impersonating someone in a position of authority or trust.

20. A — Trojan
Answer: Trojan Trojans often mimic legitimate software, attempting to trick users into installing them. In many cases, these are disguised as security updates or antivirus software. Once installed, they can cause significant damage, including additional malware installations and system slowdowns, often leading to the system becoming unusable.

21. A — Kerberos
Kerberos is a protocol for authenticating service requests between trusted hosts across an untrusted network, such as the internet. Unlike RADIUS, OAuth, and SAML which are used for remote or internet-based authentication, Kerberos can be utilized for local authentication.

22. A — Technical
Technical controls involve the use of technology to protect systems and data. These controls are installed and configured by administrators and work autonomously to maintain security.

23. C — Preventive
Answer: Preventive Preventive controls are security measures that aim to prevent security incidents and breaches. Encrypting sensitive data makes it unreadable to unauthorized users, implementing security policies ensures that employees follow best practices to avoid incidents, and biometric access controls ensure that only authorized individuals can access secure areas or information.

24. B — Preventative
Correct answer: Preventative Security controls can be classified into one of six different types, including: Preventative: Preventative controls stop a security incident from occurring. Encryption is an example of preventative control because it protects data before unauthorized access occurs. Corrective: Corrective controls mitigate a security incident after it has occurred. For example, backups are corrective because they can restore data after an incident. Detective: Detective controls identify if a security incident has occurred. Intrusion detection systems (IDS) and monitoring tools are examples of detective controls. Deterrent:

Deterrent controls disincentivize an attacker from performing a malicious action. Physical deterrents include things like barbed wire fences or visible CCTV cameras. Compensating: Compensating controls are alternatives to primary controls, often used when ideal controls are infeasible. For instance, hiring a security guard in lieu of a damaged fence. Physical: Physical controls manage or prevent physical access to resources. Examples include locks and fences.

25. B — MISP
Answer: MISP MISP (Malware Information Sharing Platform) is a widely used threat intelligence platform that helps security professionals collect, correlate, and share information about various cyber threats. By leveraging MISP, organizations can enhance their security posture and improve incident response capabilities.

26. D — An application of a legal hold
Answer: An application of a legal hold When an organization is required by legal authorities to retain evidence, it is referred to as a legal hold. This ensures that all relevant data is preserved in its current state until the investigation or litigation is concluded.

27. A — Compare checksums of configuration files
Answer: Compare checksums of configuration files Comparing the checksums of the configuration files ensures that the configurations are identical without the risk of human error. Checksums provide a reliable method to verify data integrity.

28. C — Critical
Correct answer: Critical During triage in incident response, critical evidence is instrumental in identifying the most serious threats requiring immediate attention. Relevant evidence relates to the matter at hand but may not indicate severity. Admissible evidence is suitable for legal proceedings. Competent evidence is lawfully obtained and credible. To prioritize effectively, it's crucial to distinguish the most critical evidence.

29. C — FireEye
Answer: FireEye FireEye is a leading provider of cybersecurity solutions that offer comprehensive threat intelligence reports, helping organizations to understand and mitigate cybersecurity threats. Wireshark, Snort, and tcpdump are primarily network analysis and packet sniffing tools, used for inspecting network traffic but do not provide comprehensive threat intelligence reports.

30. C — Router
Answer: Router The volatility of network devices refers to how quickly data on the device can be lost or altered. Routers are highly volatile because they store ephemeral data such as routing tables and device configurations that are frequently modified. In contrast, backup servers have very low volatility because they store long-term, persistent data. Device Volatility Router High Firewall Medium Switch Low Backup Server Very Low

Ready to pass?

Unlock the full CompTIA Security+ Exam Preps bank, every explanation, and unlimited timed mock exams.

Scan to start practising
https://certs.theorypractice.app/comptiasecurity

Also on iOS & Android — search your exam name on the App Store or Google Play