CompTIA

Free Practice Test — 30 Real Exam-Style Questions

with full answer key & explanations

Unlock the full bank of 3020 questions
+ unlimited timed mock exams + mistake book

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

What you unlock: all 3020 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 new MX record has been requested in DNS as part of a server setup. Which service most requires a correctly configured MX record to function?

A. FTP server
B. Load balancer
C. Firewall DMZ
D. Mail server

2. A network administrator is experiencing high CPU utilization on a monitoring server caused by continuous SNMP polling of hundreds of devices. How should the administrator reduce this CPU load without sacrificing monitoring capability?

A. Remove SNMP polling and configure SNMP traps on each network device
B. Remove SNMP polling and implement snmpwalk on each network device
C. Modify SNMP polling to occur only during business hours
D. Upgrade SNMP to the latest version to address vulnerabilities

3. What benefit does MIMO technology bring to the 802.11n wireless standard?

A. Channel bonding
B. Gigabit wireless bandwidth
C. Channel expansion
D. Multipath support

4. What is the minimum recommended twisted-pair copper cable category for 1000BASE-T (Gigabit Ethernet) networks?

A. Cat 5e
B. Cat 3
C. Cat 5
D. Cat 6

5. Wi-Fi Protected Setup (WPS) supports four modes for adding devices to a network. Which mode has serious security vulnerabilities due to a brute-force attack?

A. Near-field communication
B. Push button
C. PIN
D. USB

6. Which term describes hackers who operate in a morally ambiguous space — working without explicit authorization but often with good intentions, such as reporting discovered vulnerabilities?

A. Blue hat
B. White hat
C. Black hat
D. Gray hat

7. You are configuring data classification labels for your organization's R&D file server. Users typically label documents as contractor, public, or internal. What classification label should be applied to the organization's trade secrets?

A. High
B. Low
C. Proprietary
D. Top secret

8. The CEO reports that his computer will not allow anyone to log in without entering credit card payment information. Investigation reveals he downloaded a file shared by a friend on social media, after which the computer restarted and showed the payment demand. What type of attack best describes this scenario?

A. The CEO downloaded and executed Ransomware
B. The CEO executed a Rootkit which gave backdoor access to a hacker
C. The CEO was the target of a spear phishing social engineering attack
D. A botnet is attacking the CEO's computer and disabling login attempts

9. In a spanning-tree topology, what value is used to determine which port on a non-root switch becomes the root port?

A. Lowest port MAC address
B. Port priority number and MAC address
C. Highest port priority number
D. Path cost

10. Which protocol is used to resolve a MAC address from a known IP address?

A. ARP
B. FTP
C. IMAP
D. NTP

11. Which technology provides a flexible and secure wireless communications system that can supplement or fully replace a wired Ethernet LAN?

A. PHLAN
B. MAN
C. WLAN
D. CRAN

12. An employee on extended business travel uses a personal mobile device to handle sensitive company data. Which of the following is the most critical measure to put in place?

A. An acceptable use policy governing how the personal device may be used for work
B. An NDA ensuring that company data stored on the personal device stays confidential
C. Real-time remote monitoring of the device's activity and usage
D. A consent-to-monitoring policy covering company audits of the personal device

13. Which of the following are examples of secure VPN tunneling protocols? (Choose 2)

A. WEP
B. IPsec
C. bcrypt
D. TLS

14. What security component is composed of hardware, software, and firmware that together enforce a system's security policy?

A. Access Monitor
B. Reference Monitor
C. Access Kernel
D. Security Kernel

15. Nathan wants to restrict company-issued mobile devices so they can only be used within the organization's physical premises. What type of authentication should he deploy?

A. Biometrics
B. PINs
C. Content-aware authentication
D. Context-aware authentication

16. What is the name of the hardware-based security chip that stores cryptographic keys and protects sensitive information on a device?

A. TFTP
B. SLP
C. DMZ
D. TPM

17. Gabrielle wants to use a single cable that carries both digital audio and digital video signals. Which connector type should Malcolm recommend?

A. RGB
B. S-video
C. HDMI
D. RCA

18. Which device uses satellites to determine your geographic location and can be used for turn-by-turn navigation?

A. Headset
B. E-reader
C. GPS device
D. Smart camera

19. Which command opens the System Information tool in Windows?

A. msinfo64
B. mscnfg32
C. msconfig
D. msinfo32

20. Which of the following file systems provides the best security features?

A. NTFS
B. FAT32
C. Local Security Policy
D. Privacy filter

21. What is the primary benefit of retaining audit logs for an extended period in a cybersecurity program?

A. To enforce strict password policies
B. To encrypt all network traffic
C. To eliminate the need for security policies
D. To support forensic investigations and incident response

22. The CISO has requested a report identifying which incident response processes need improvement following a recent security incident. What type of document addresses this request?

A. Preparation
B. Containment
C. Detection
D. Lessons learned

23. Which network device forwards packets across multiple networks and uses routing tables to determine the optimal path to a destination?

A. Switches
B. Hubs
C. Routers
D. Bridges

24. Under what circumstances is it acceptable to yell at a user?

A. When they repeat a mistake for the fifth time
B. When they repeat the same mistake a second time
C. When they interrupt your troubleshooting
D. Never

25. You are purchasing an inkjet printer cartridge for home use and want an MSDS (Material Safety Data Sheet) for it. How do you obtain one?

A. Ask the store to provide one at the time of purchase.
B. You are not legally permitted to obtain an MSDS for consumer products.
C. Visit the printer cartridge manufacturer's website.
D. It is included in the product packaging.

26. Which CPU component handles primary processing operations?

A. ALU
B. Registers
C. Pipeline
D. FPU

27. A technician cannot find a mechanical reason for a printer failure and asks you to restart the Windows background service that manages the printer queue. What is the name of that service?

A. Maintenance Services
B. WinPrint
C. Print Spooler
D. Windows Printing Services

28. Which feature built into modern memory modules allows a motherboard to automatically configure memory at the correct speed and latency settings?

A. Spinning pinwheel
B. SPD
C. Virtual memory
D. Triple-channel

29. In a client-server network, what mechanism ensures that data from a client application is delivered to the correct server application?

A. IP address
B. Slot number
C. port number
D. MAC address

30. You are auditing a system that stores credit card data. You notice that the credit card numbers in stored records are partially obscured — for example, only the last four digits are visible. Which data protection technique does this represent?

A. Sensitive Data Replacement (SDR)
B. Data anonymization
C. Data masking
D. Tokenization

Answer Key & Explanations

1. D — Mail server
An MX (Mail Exchanger) DNS record designates the server responsible for receiving email for a domain. A mail server relies on this record for inbound message delivery. Load balancers, FTP servers, and firewall DMZ configurations do not depend on MX records.

2. A — Remove SNMP polling and configure SNMP traps on each network device
Switching from continuous SNMP polling to SNMP traps is the most effective solution. With traps, each network device sends a notification to the management station only when a specific event occurs, eliminating constant polling and significantly reducing CPU load while maintaining monitoring coverage.

3. D — Multipath support
MIMO (Multiple-Input Multiple-Output) technology in 802.11n leverages multiple antennas to take advantage of multipath propagation, improving signal reliability and throughput by using multiple simultaneous data streams.

4. A — Cat 5e
Cat 5e (Category 5 enhanced) is the minimum recommended cable grade for 1000BASE-T. Its tighter specifications and improved signal quality over standard Cat 5 make it capable of supporting Gigabit Ethernet (1000 Mbps) speeds.

5. C — PIN
WPS PIN mode was shown to be susceptible to brute-force attacks, allowing attackers to recover the WPS PIN and gain network access. The vulnerability was publicly demonstrated, leading to recommendations to disable WPS PIN mode.

6. D — Gray hat
Gray hat hackers operate without formal authorization but generally do not intend to cause harm. They may expose vulnerabilities and report them to the affected parties rather than exploiting them. Black hat hackers act maliciously for personal gain. White hat hackers operate with full authorization as ethical hackers. Blue hat hackers are sometimes hired by companies specifically to test systems before launch.

7. C — Proprietary
Proprietary is a confidentiality classification used for information whose disclosure could damage a company's competitive position. 'High' and 'Low' are generic risk labels for internal data. 'Top secret' is a government classification label not typically used in commercial organizations.

8. A — The CEO downloaded and executed Ransomware
The described behavior—blocking system access and demanding payment—is characteristic of ransomware. The malware holds the system hostage until a fee is paid. While targeted delivery via social media could suggest spear phishing, the information provided best supports a ransomware conclusion. A botnet or rootkit would not typically display a payment demand on the login screen.

9. D — Path cost
In spanning tree, the root port on each non-root switch is the port with the lowest path cost to the root bridge. Path cost is calculated based on link bandwidth; lower bandwidth links have higher cost. When multiple links have equal cost, other tiebreakers such as port priority or MAC address are used.

10. A — ARP
ARP (Address Resolution Protocol) maps a known IP address to the corresponding MAC address on a local network, enabling Layer 2 frame delivery.

11. C — WLAN
A Wireless Local Area Network (WLAN) can augment or replace a wired Ethernet LAN, offering flexible connectivity within a local area.

12. C — Real-time remote monitoring of the device's activity and usage
Real-time remote monitoring of the personal device during extended travel allows continuous oversight, enabling prompt detection and response to any unauthorized access or suspicious activity involving sensitive company data.

13. B — IPsec
IPsec (Internet Protocol Security) authenticates and encrypts IP packets to establish secure VPN tunnels. TLS (Transport Layer Security) encrypts communications over networks and is also used in VPN implementations. bcrypt is a password hashing algorithm, not a tunneling protocol. WEP is a deprecated and insecure wireless encryption standard, not a VPN protocol.

14. D — Security Kernel
The Security Kernel comprises hardware, software, and firmware components that collectively implement and enforce the security policy of a computer system.

15. D — Context-aware authentication
Context-aware authentication uses contextual signals such as geolocation to enforce location-based access policies, ensuring devices can only be authenticated within the facility's boundaries. PINs and biometrics verify identity but cannot enforce location restrictions. 'Content-aware authentication' is a fabricated term.

16. D — TPM
A TPM (Trusted Platform Module) is a dedicated hardware security chip that stores cryptographic keys and other sensitive data, providing a hardware root of trust for the device. A DMZ is a network security zone. SLP is the Service Location Protocol. TFTP is the Trivial File Transfer Protocol — none of these are encryption key storage devices.

17. C — HDMI
HDMI transmits both digital audio and digital video over a single cable. S-video is an older analog video-only connector. RGB requires separate cables per color channel. RCA connectors are analog and typically carry audio or composite video separately.

18. C — GPS device
GPS (Global Positioning System) devices communicate with satellites to pinpoint your location. Because they require a clear line of sight to satellites, signal quality can be reduced in bad weather or dense environments.

19. D — msinfo32
Typing msinfo32 in the Windows search box or Run dialog opens the System Information tool, which provides details about hardware, system components, and software.

20. A — NTFS
NTFS (New Technology File System) offers superior security compared to FAT32 through support for file and folder permissions and encryption. Privacy filter and Local Security Policy are not file systems.

21. D — To support forensic investigations and incident response
Long-term audit log retention provides historical records that can be analyzed during forensic investigations, incident response activities, and compliance audits, enabling organizations to reconstruct events and gather evidence.

22. D — Lessons learned
A lessons-learned report is produced after an incident to review what went well, what did not, and which processes need improvement. It is a key output of the post-incident activity phase and is used to strengthen future incident response capabilities.

23. C — Routers
Routers operate at Layer 3 of the OSI model and use routing tables to determine the best path for forwarding packets across different networks. Switches forward frames within a single network based on MAC addresses. Bridges connect two network segments. Hubs broadcast traffic to all connected ports.

24. D — Never
It is never acceptable to get angry or raise your voice at a customer or user under any circumstances.

25. C — Visit the printer cartridge manufacturer's website.
The MSDS can be downloaded from the manufacturer's website. Retailers are not required to provide one at purchase, and it is not required to be included in packaging. OSHA regulations do allow consumers to obtain MSDS documents, and it is advisable to have them in case of an emergency.

26. A — ALU
The Arithmetic Logic Unit (ALU) is responsible for performing the primary processing duties within the CPU.

27. C — Print Spooler
The Print Spooler is the Windows service that manages print job queuing and communication between applications and printers. Restarting it often resolves stalled or unresponsive printing.

28. B — SPD
The Serial Presence Detect (SPD) chip on a memory module stores information about the module's speed, capacity, and latency, enabling the motherboard to configure memory settings correctly at startup.

29. C — port number
Port numbers direct client application data to the appropriate server application. Common port numbers such as those used by Telnet, SSH, and SMTP are frequently tested on the CompTIA A+ exam.

30. C — Data masking
Data masking replaces sensitive data values with altered or partially hidden versions, allowing records to be used or displayed without exposing the complete sensitive value. Showing only the last four digits of a credit card number is a classic example of data masking. Tokenization replaces the sensitive value with a

non-sensitive token that references the original via a secure lookup. Anonymization removes or alters data so it can no longer be linked to an individual.

Ready to pass?

Unlock the full CompTIA bank, every explanation, and unlimited timed mock exams.

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

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