SecurityX Test Prep

Free Practice Test — 30 Real Exam-Style Questions

with full answer key & explanations

Unlock the full bank of 1511 questions
+ unlimited timed mock exams + mistake book

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

What you unlock: all 1511 questions • unlimited timed mock exams • mistake book • instant explanations

Also on iOS & Android — and watch the full Q&A walkthrough on YouTube @CertsQuizPrep

Practice Questions

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

Want the other 1481+ questions & full timed mock exams? Unlock at https://certs.theorypractice.app/securityx

1. Which of the following is an advantage of using elliptic curve cryptography (ECC) over RSA?

A. ECC is typically faster to implement in hardware.
B. ECC is less complex to understand and implement than RSA.
C. ECC generates longer keys, making it more secure.
D. ECC requires shorter key lengths to achieve comparable security.

2. A system administrator notices an employee with a company-issued laptop has installed software not available in the official repositories. What is the likely security issue with the laptop?

A. There is a BIOS/firmware incompatibility.
B. The laptop has been rooted.
C. The laptop's data has been encrypted.
D. An eFuse has been activated.

3. Which of the following techniques involves examining and monitoring server traffic in real-time to identify and mitigate potential security threats?

A. Static code analysis
B. Network traffic analysis
C. Peering
D. Sandboxing

Also on iOS & Android — and watch the full Q&A walkthrough on YouTube @CertsQuizPrep

Unlock all 1511 questions + timed mock exams
→ **https://certs.theorypractice.app/securityx**
$2.99/week or $6.99/month · cancel anytime · scan to start

Unofficial study material · not affiliated with any certifying body

4. BrightFuture Corp. uses an extensive IoT network for industrial monitoring. To ensure no unauthorized access to their sensor data, BrightFuture Corp. produces and securely stores its own cryptographic keys, without granting any access to their IoT service provider. What approach to key management is BrightFuture Corp. using?

A. HYOK
B. BYOK
C. BYOD
D. A RRSIG

5. A security specialist is evaluating a company's procedures for maintaining secure backups of sensitive data. They find that: encryption is enforced for all backups; access to backup media requires multi-factor authentication (MFA); all backup activities are logged and audited; and backup data can be deleted by an administrator. Based on this information, what should the specialist recommend?

A. Disable encryption for all backups
B. Stop logging and auditing backup activities
C. Disallow an administrator from deleting backup data
D. Allow backup data to be accessed without MFA

6. A cybersecurity team needs to identify potential vulnerabilities in their network devices. Which of the following tools is NOT primarily used for vulnerability scanning?

A. OpenVAS
B. Qualys
C. Wireshark
D. Nessus

Want the other 1481+ questions & full timed mock exams? Unlock at https://certs.theorypractice.app/securityx

7. Which of the following is a protocol used for secure remote management and communication?

A. SNMP
B. SSH
C. FTP
D. HTTP

Unlock all 1511 questions + timed mock exams
→ **https://certs.theorypractice.app/securityx**
$2.99/week or $6.99/month · cancel anytime · scan to start

Unofficial study material · not affiliated with any certifying body

8. What does the Wireshark "tcp.flags.syn == 1 and tcp.flags.ack == 0" filter do?

A. Filter for TCP SYN packets
B. Capture all network traffic
C. Filter for UDP packets only
D. Show network traffic from root user

9. All of the following are key sources for obtaining information on network vulnerabilities EXCEPT:

A. OVAL
B. NVD
C. ISO
D. US-CERT

Also on iOS & Android — and watch the full Q&A walkthrough on YouTube @CertsQuizPrep

10. TechCorp aims to identify security vulnerabilities in its applications during development, before the applications are moved to cloud infrastructure. Which security tool should TechCorp implement to achieve this goal?

A. Vulnerability Scanner
B. SAST
C. DAST
D. Port Scanner

11. Which of the following is a widely accepted framework for managing and improving an organization's overall cybersecurity posture, covering areas such as risk management, communications, and governance?

A. COBIT
B. PCI-DSS
C. HIPAA
D. NIST Cybersecurity Framework

12. During a cybersecurity exercise, you create a fake online persona to gather sensitive data from a company's employees. What type of intelligence gathering is this?

A. TECHINT
B. HUMINT
C. SIGINT
D. SOCMINT

Unlock all 1511 questions + timed mock exams
→ **https://certs.theorypractice.app/securityx**
$2.99/week or $6.99/month · cancel anytime · scan to start
Unofficial study material · not affiliated with any certifying body

Want the other 1481+ questions & full timed mock exams? Unlock at https://certs.theorypractice.app/securityx

13. A database administrator wants to ensure their database servers do not have any vulnerabilities that attackers could exploit. Which of the following tools would provide the MOST benefit in this scenario?

A. Nessus
B. Wireshark
C. traceroute
D. John The Ripper

14. Identify the four primary steps in the Incident Response Life Cycle as defined by NIST.

A. Identification, Containment, Eradication, Investigation
B. Discovery, Containment, Remediation, Reporting
C. Preparation, Detection and Analysis, Containment, Eradication, and Recovery, Post-Incident Activity
D. Preparation, Detection, Response, Mitigation

15. Firewalls operate at which layer of the OSI model? They enforce rules using what tables?

A. 4, Access Control Lists (ACL)
B. 3, IP tables
C. 5, MAC filtering
D. 2, Distributed Control System (DCS)

Also on iOS & Android — and watch the full Q&A walkthrough on YouTube @CertsQuizPrep

16. In a network security environment, it is often necessary to configure access control lists (ACLs) to ensure proper traffic flow. Which of the following is the correct syntax for an ACL rule that will permit all TCP traffic from source IP address 192.168.10.10 to destination IP address 172.16.20.20?

A. access-list 200 192.168.10.10 TCP permit 172.16.20.20
B. access-list 200 172.16.20.20 permit TCP 192.168.10.10
C. access-list 200 permit 192.168.10.10 TCP any 172.16.20.20
D. access-list 200 permit TCP 192.168.10.10 any 172.16.20.20 any

Unlock all 1511 questions + timed mock exams
→ **https://certs.theorypractice.app/securityx**
$2.99/week or $6.99/month · cancel anytime · scan to start
Unofficial study material · not affiliated with any certifying body

17. Alice, a network administrator, sets a policy to send an alert if bandwidth utilization of a network link exceeds 80% during office hours. What type of threshold is this?

A. State-based
B. Historical
C. Adaptive
D. Fixed

18. Which of the following is a primary advantage of using a TPM (Trusted Platform Module) in a security architecture?

A. Protection against physical theft
B. Provisioning high processing power for encryption
C. Ensuring constant system uptime
D. Secure storage for encryption keys

Want the other 1481+ questions & full timed mock exams? Unlock at https://certs.theorypractice.app/securityx

19. TechCorp develops proprietary algorithms that they include in their software packages. In their efforts to ensure client trust, what method can TechCorp employ to assure clients that the software they receive is authentic and tamper-free?

A. Digital signature
B. Third-party audit
C. Checksum verification
D. Sandboxing

20. As an IT security analyst for Tech Corp, you've been assigned to implement a solution that monitors and detects unauthorized devices connecting to the company's wired network. Which of the following tools would provide the BEST solution?

A. WIDS
B. HIDS
C. VPN
D. NIDS

Unlock all 1511 questions + timed mock exams
→ **https://certs.theorypractice.app/securityx**
$2.99/week or $6.99/month · cancel anytime · scan to start
Unofficial study material · not affiliated with any certifying body

21. An online retail company seeks to ensure that external payment processing services can securely and effectively handle customer transactions. This system must define how payment requests will be sent and how confirmations will be received. What type of solution will allow for this?

A. Proxy server
B. API gateway
C. Firewall
D. Load balancer

Also on iOS & Android — and watch the full Q&A walkthrough on YouTube @CertsQuizPrep

22. Where can firewall devices be strategically placed within a corporate network?

A. At the network perimeter and at key internal segment points
B. Only at the network perimeter, not at internal segments
C. Only at key internal segment points, not at the network perimeter
D. At the network perimeter or internal segments, but not both

23. Which of the following is NOT one of the principles of the Zero Trust security model?

A. Verify explicitly
B. Least privilege principle
C. Open access networks
D. Assume breach

24. An organization needs to ensure secure communication between their data center and branch offices. What solution should they implement to achieve this?

A. Remote access VPN
B. Network Access Control (NAC)
C. Network Address Translation (NAT)
D. Site-to-site VPN

Want the other 1481+ questions & full timed mock exams? Unlock at https://certs.theorypractice.app/securityx

Unlock all 1511 questions + timed mock exams
→ **https://certs.theorypractice.app/securityx**
$2.99/week or $6.99/month · cancel anytime · scan to start
Unofficial study material · not affiliated with any certifying body

25. How is information about the structure of a file, such as permissions or owner, described in a Linux file system?

A. Mapping data
B. Metadata
C. Superdata
D. XOR data

26. What is the default port used by SSH?

A. 22
B. 80
C. 21
D. 443

27. Which file transfer protocol is both platform-independent and capable of securely transferring files over a network?

A. TFTP
B. HTTP
C. SFTP
D. FTP

Also on iOS & Android — and watch the full Q&A walkthrough on YouTube @CertsQuizPrep

28. Your organization is preparing for an annual compliance audit. The compliance officer has requested you to document the current compliance status, identify areas where compliance is not met, and suggest remedies to ensure full compliance before the audit date. Which of the following should you do to meet this objective?

A. Execute MTBF analysis
B. Execute MTTR analysis
C. Perform a compliance gap analysis
D. Conduct a revenue audit based on GAAP

29. BetaTech Ltd. and GammaSolutions Co. are unable to finalize a binding contract for their joint project. Instead, they draft a document, signed by representatives from both companies, outlining the terms and expectations. What is this type of document called?

A. Service level agreement
B. Operation level agreement
C. Memorandum of understanding
D. Interconnection security agreement

Unlock all 1511 questions + timed mock exams
→ **https://certs.theorypractice.app/securityx**
$2.99/week or $6.99/month · cancel anytime · scan to start
Unofficial study material · not affiliated with any certifying body

30. In the context of cybersecurity risk management, what does SLE stand for?

A. Single Loss Event
B. Security Level Expense
C. Security Loss Estimate
D. Single Loss Expectancy

Unlock all 1511 questions + timed mock exams
→ **https://certs.theorypractice.app/securityx**
$2.99/week or $6.99/month · cancel anytime · scan to start
Unofficial study material · not affiliated with any certifying body

Answer Key & Explanations

You just practised 30 of 1511. Unlock every question + timed mocks at https://certs.theorypractice.app/securityx

1. D — ECC requires shorter key lengths to achieve comparable security.
Answer: ECC requires shorter key lengths to achieve comparable security. Elliptic curve cryptography (ECC) is known for its efficiency in key length. It provides the same level of security as RSA but with significantly shorter key sizes. This results in faster computations and less storage requirement. Contrary to the distractors, ECC is not necessarily faster to implement in hardware, and its complexity can make it challenging to understand and implement. It also does not generate longer keys but rather achieves stronger security with shorter keys.

2. B — The laptop has been rooted.
Answer: The laptop has been rooted. Rooting removes system-imposed restrictions, allowing the installation of software from any source. Encrypting data through Full-Device Encryption (FDE) ensures data security. An eFuse is used to prevent tampering with system components. BIOS and firmware issues often relate to versioning and compatibility management.

3. B — Network traffic analysis
Answer: Network traffic analysis Network traffic analysis is the process of intercepting and examining messages to deduce information from patterns in communication, which helps in identifying malicious activities and security threats in real-time. Sandboxing is a way to safely run a program in a specific isolated environment. Static code analysis involves examining code without executing it, to find vulnerabilities early in the development process. Peering is a technique for directly connecting two networks.

4. A — HYOK
Answer: HYOK With an HYOK (hold your own key) model, customers create and manage their own keys. The IoT service provider does not have access to the keys and cannot decrypt the data. With a BYOK (bring your own key) model, customers create and manage their own keys, but the IoT service provider is allowed access to the keys and can decrypt the data. BYOD (bring your own device) is related to employees using their own devices to access corporate resources. A RRSIG (resource record digital signature) record is a type of DNSSEC record.

5. C — Disallow an administrator from deleting backup data
Disallow an administrator from deleting backup data. Implementing strong security controls, such as disallowing any user (including administrators) from deleting backup data, is critical. Enforcing MFA, encryption, and logging and auditing activities are essential practices to ensure secure backups.

6. C — Wireshark
Correct answer: Wireshark Wireshark is a network protocol analyzer used to capture and analyze network traffic, not a vulnerability scanner. Nessus is a widely used vulnerability scanner that helps identify vulnerabilities, configuration issues, and policy compliance. OpenVAS (Open Vulnerability Assessment System) is also a comprehensive vulnerability scanning tool to detect security issues. Qualys is a cloud-based service that provides vulnerability scanning, compliance management, and other security services.

Unlock all 1511 questions + timed mock exams
→ **https://certs.theorypractice.app/securityx**
$2.99/week or $6.99/month · cancel anytime · scan to start

Unofficial study material · not affiliated with any certifying body

7. B — SSH
Answer: SSH Secure Shell (SSH) is a protocol used for secure remote management and for securely accessing a remote computer over an unsecured network. It encrypts the data being transmitted, ensuring confidentiality and integrity. FTP is the File Transfer Protocol, which is used for transferring files but does not encrypt the data. HTTP stands for HyperText Transfer Protocol, used primarily for accessing websites over the internet but without built-in encryption. SNMP is the Simple Network Management Protocol, which is used for network management but typically lacks encryption.

8. A — Filter for TCP SYN packets
Answer: Filter for TCP SYN packets The Wireshark filter "tcp.flags.syn == 1 and tcp.flags.ack == 0" is used to capture TCP SYN packets. TCP SYN packets are the first step in the TCP three-way handshake and are useful for identifying network connections being initiated. The command "tcp.flags.syn == 1 and tcp.flags.ack == 0" would be used within Wireshark to filter out only SYN packets, which are used to initiate TCP connections. Other filters such as "tcp.port" for port-specific traffic and "ip.addr" for traffic from a specific IP address can be combined with this filter for more granular monitoring. Filtering for TCP SYN packets can help network security professionals monitor for new connection attempts and potential scan activities.

9. C — ISO
Answer: ISO The International Organization for Standardization (ISO) provides standards for various aspects of technology and security, but does not provide real-time information on network vulnerabilities. The United States Computer Emergency Readiness Team (US-CERT) provides security advisories. The Open Vulnerability and Assessment Language (OVAL) produces definitions for detecting vulnerabilities. The National Vulnerability Database (NVD) is a repository of vulnerability information.

10. B — SAST
Answer: SAST Static application security testing (SAST) tools analyze source code for potential security vulnerabilities such as buffer overflows and injection flaws early in the development lifecycle. This allows developers to rectify issues before deploying the application to the cloud. Dynamic application security testing (DAST) tools evaluate applications in runtime and do not analyze source code. A port scanner reviews network endpoints to identify open ports and running services. Vulnerability scanners are generally used to detect known vulnerabilities in deployed systems and applications.

11. D — NIST Cybersecurity Framework
Answer: NIST Cybersecurity Framework The NIST Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations in the US can assess and improve their ability to prevent, detect, and respond to cyber attacks. COBIT (Control Objectives for Information and related Technologies) focuses on governance and management of enterprise IT. PCI-DSS (Payment Card Industry Data Security Standard) is a proprietary information security standard for organizations that handle branded credit cards. HIPAA (Health Insurance Portability and Accountability Act) is US legislation that provides data privacy and security provisions for safeguarding medical information.

12. B — HUMINT
Answer: HUMINT HUMINT (human intelligence) involves interacting with people to collect information or gain access. SIGINT (signals intelligence) is the collection and analysis of electronic communications and signals. SOCMINT (social media intelligence) involves monitoring and analyzing data from social media platforms. TECHINT (technical intelligence) involves gathering information on the technical characteristics and capabilities of foreign weapons and equipment.

Unlock all 1511 questions + timed mock exams
→ **https://certs.theorypractice.app/securityx**
$2.99/week or $6.99/month · cancel anytime · scan to start
Unofficial study material · not affiliated with any certifying body

13. A — Nessus
Answer: Nessus The administrator needs a vulnerability scanner. Nessus is one of the most widely used vulnerability scanners available. It is free for personal use on non-enterprise networks and can provide in-depth information about various vulnerabilities and weaknesses discovered within the database servers. Wireshark is a tool for capturing and analyzing network traffic. The traceroute command helps determine the path network traffic takes to a destination. John the Ripper is a password cracker.

14. C — Preparation, Detection and Analysis, Containment, Eradication, and Recovery, Post-Incident Activity
Answer: Preparation, Detection and Analysis, Containment, Eradication, and Recovery, Post-Incident Activity The Incident Response Life Cycle as defined by NIST consists of several steps aimed at addressing and mitigating security incidents. Initially, organizations prepare by setting up the necessary infrastructure and policies. Detection and analysis involve identifying and understanding the scope of an incident. Containment, eradication, and recovery deals with isolating affected systems, removing threats, and restoring operations. Post-incident activity includes reviewing and learning from the incident to improve future response efforts.

15. A — 4, Access Control Lists (ACL)
Answer: 4, Access Control Lists (ACL). Firewalls primarily operate at Layer 4 of the OSI model. This involves managing traffic based on TCP/UDP port numbers, which is a characteristic of the Transport layer. The rules and policies they apply to network traffic are stored in Access Control Lists (ACLs). IP tables and MAC filtering are related but not the primary methods used by firewalls. Distributed Control Systems (DCS) are unrelated to OSI model layers and firewall functions.

16. D — access-list 200 permit TCP 192.168.10.10 any 172.16.20.20 any
Answer: access-list 200 permit TCP 192.168.10.10 any 172.16.20.20 any Access control lists (ACLs) are used to filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. The correct syntax for an ACL rule follows the format: Rule name/number, Action, Protocol, Source IP, Source Port, Destination IP, Destination Port. In the correct answer, 'permit' allows the traffic, 'TCP' is the protocol specified, '192.168.10.10' is the source IP, 'any' specifies that any port can be used by the source, '172.16.20.20' is the destination IP, and 'any' specifies that any port can be used by the destination.

17. D — Fixed
Answer: Fixed Alert thresholds based on fixed numeric values or calculations are called fixed thresholds. An 80% bandwidth utilization threshold is an example of a fixed value. State-based thresholds are triggered when a system state changes, such as a change in operational mode or network status. Historical thresholds consider past and present values and are often used to compare different periods. Adaptive is a distractor answer. Adaptive thresholds adjust based on varying conditions, such as user load or varying network traffic patterns.

18. D — Secure storage for encryption keys
Answer: Secure storage for encryption keys A Trusted Platform Module (TPM) provides secure storage for encryption keys and other security-related credentials. It helps ensure the integrity of a system by securely storing cryptographic keys used for encryption, preventing tampering and unauthorized access. However, TPMs do not protect against physical theft, provide high processing power for encryption tasks, or ensure a constant system uptime. Device encryption protects the data on the device, while secure storage protects the keys and credentials used to encrypt the data itself.

Unlock all 1511 questions + timed mock exams
→ **https://certs.theorypractice.app/securityx**
$2.99/week or $6.99/month · cancel anytime · scan to start
Unofficial study material · not affiliated with any certifying body

19. A — Digital signature
Digital signature is a security method used to guarantee the authenticity and integrity of software packages. It involves applying a cryptographic signature to the software using a trusted key, ensuring that the software has not been tampered with from the time it was signed. Third-party audit refers to a review conducted by an independent organization to confirm compliance and effectiveness but is not specifically for ensuring software authenticity. Checksum verification checks for data integrity but does not confirm the authenticity of the creator. Sandboxing is an isolation technique to run code in a secure environment, not specifically for ensuring authenticity.

20. D — NIDS
Answer: NIDS A NIDS (network intrusion detection system) is designed to monitor and analyze network traffic to detect unauthorized devices and other suspicious activities on a network. WIDS (wireless intrusion detection system) is used for monitoring wireless networks, not wired networks. HIDS (host intrusion detection system) focuses on individual endpoints or devices. VPN (virtual private network) is a tunneling protocol for secure communications, not a monitoring tool.

21. B — API gateway
Answer: API gateway An Application Programming Interface (API) gateway handles interactions between different types of systems. An API gateway can be used to manage API calls from external sources, such as payment processing services, and securely facilitates the sending of requests and receiving of confirmations. A firewall is a security device that monitors and controls incoming and outgoing network traffic. A load balancer distributes network or application traffic across multiple servers. A proxy server acts as an intermediary for requests from clients seeking resources from other servers.

22. A — At the network perimeter and at key internal segment points
Answer: At the network perimeter and at key internal segment points Firewalls are essential for protecting a corporate network. They should be positioned at both the network perimeter to guard against external threats and at key internal segments to monitor and control traffic within the network.

23. C — Open access networks
Answer: Open access networks The principles of the Zero Trust security model include assume breach, verify explicitly, and least privilege. Open access networks are not a principle of the Zero Trust security model.

24. D — Site-to-site VPN
Answer: Site-to-site VPN A site-to-site VPN connects separate networks over the internet to function as a single network. This provides a secure, encrypted connection for data transfer. A remote access VPN is typically used to create a secure tunnel for individual users to connect to an internal network. Network Access Control (NAC) manages authorization of devices before connection, while Network Address Translation (NAT) allows multiple devices on a local network to access external networks using a single public IP address.

25. B — Metadata
Answer: Metadata. Metadata provides information about the structure and attributes of a file, such as permissions, owner, and timestamps in a Linux file system. Superdata and XOR data are non-existent terms used as distractors.

26. A — 22
Answer: 22. By default, SSH (Secure Shell) uses port 22. Port 80 is used for HTTP, port 21 is used for FTP, and port 443 is used for HTTPS.

Unlock all 1511 questions + timed mock exams
→ **https://certs.theorypractice.app/securityx**
$2.99/week or $6.99/month · cancel anytime · scan to start
Unofficial study material · not affiliated with any certifying body

27. C — SFTP
Answer: SFTP SFTP (SSH File Transfer Protocol) is a secure and platform-independent method for transferring files over a network, as it leverages SSH (Secure Shell) for encryption. FTP (File Transfer Protocol) lacks inherent security features and generally operates without encryption. TFTP (Trivial File Transfer Protocol) is a simplified version of FTP without authentication and encryption mechanisms. HTTP (HyperText Transfer Protocol) is primarily used for transferring web pages and data over the web but lacks specific focus on secure file transfers.

28. C — Perform a compliance gap analysis
Answer: Perform a compliance gap analysis A compliance gap analysis identifies the current state of compliance, desired compliance state, and necessary steps to achieve full compliance. GAAP (Generally Accepted Accounting Principles) is not directly relevant to the compliance audit preparation. MTBF (Mean Time Between Failures) and MTTR (Mean Time to Repair) analyses are distractors and do not directly address compliance requirements.

29. C — Memorandum of understanding
Answer: Memorandum of understanding An MOU (memorandum of understanding) is an agreement between multiple parties that is often non-binding, but formally details a shared understanding or agreement. An ISA (interconnection security agreement) is a specific telecommunications contract related to network connections. An OLA (operation level agreement) is an agreement about responsibilities between different support teams. An SLA (service level agreement) is a minimum guaranteed service level a provider commits to. For example, an SLA may specify 99.9% uptime and 1-hour support response times.

30. D — Single Loss Expectancy
Answer: Single Loss Expectancy The single loss expectancy (SLE) is a measure of the monetary loss or impact of a single occurrence of a threat. It is often used in risk assessments to estimate the potential financial impact of security incidents.

Unlock all 1511 questions + timed mock exams
→ **https://certs.theorypractice.app/securityx**
$2.99/week or $6.99/month · cancel anytime · scan to start
Unofficial study material · not affiliated with any certifying body

Ready to pass?

Unlock the full SecurityX Test Prep bank, every explanation, and unlimited timed mock exams.

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

Watch the full video walkthrough on YouTube @CertsQuizPrep

Unlock all 1511 questions + timed mock exams
→ **https://certs.theorypractice.app/securityx**
$2.99/week or $6.99/month · cancel anytime · scan to start

Unofficial study material · not affiliated with any certifying body