

Exam4Test SY0-201 Exams

CompTIA CompTIA Security+(2008 Edition) Exam



Practice Exam: SY0-201

Exam Number/Code: SY0-201

Exam Name: CompTIA Security+(2008 Edition) Exam

Questions and Answers: 469 Q&As

Exam Description

Order : [SY0-201 Exam](#)

1. Exam4Test offer free update service for three month.

After you purchase our product, we will offer free update in time for three month.

2. High quality and Value for the SY0-201 Exam.

Exam4Test **Practice Exams** for SY0-201 are written to the highest standards of technical accuracy, provided by our certified subject matter experts and published authors for development.

3. 100% Guarantee to Pass Your **Security** exam and get your *Security Certification*.

We guarantee your success in the first attempt. If you do not pass the **Security** "SY0-201" (CompTIA Security+(2008 Edition) Exam on your first attempt, send us the official result. We will give you a FULLY REFUND of your purchasing fee and send you another same value product for free.

4. Exam4Test Security SY0-201 Exam Downloadable.

Our PDF or Testing Engine Preparation Material of Security SY0-201 exam provides everything which you need to pass your exam. The Security Certification details are researched and produced by our Professional Certification Experts who are constantly using industry experience to produce precise, and logical. You may get "SY0-201 exam" questions from different websites or books, but logic is the key. Our Product will help you not only pass in the first CompTIA Security+(2008 Edition) Exam(Security) exam try, but also save your valuable time.

Comprehensive questions with complete details about SY0-201 exam.

SY0-201 exam questions accompanied by exhibits. Verified Answers Researched by Industry Experts and almost 100% correct.

Drag and Drop questions as experienced in the Real Security exam. SY0-201 exam questions updated on regular basis.

Like actual Security Certification exams, SY0-201 exam preparation is in multiple-choice questions (MCQs). Tested by many real Security exams before publishing.

Try free Security exam demo before you decide to buy it in <http://www.Exam4Test.com>

High quality and Valued for the SY0-201 Exam: 100% Guarantee to Pass Your SY0-201 exam and get your Security Certification. Come to <http://www.Exam4Test.com> The easiest and quickest way to get your Security Certification.

Exam4Test professional provides Security SY0-201 the newest Q&A, completely covers SY0-201 test original topic. With our completed Security resources, you will minimize your Security cost and be ready to pass your SY0-201 test on Your First Try, 100% Money Back Guarantee included!

SY0-201 Exam Study Guide

SY0-201 exam is regarded as one of the most favourite [Security Certifications](#). Many IT professionals prefer to add SY0-201 exam among their credentials. Exam4Test not only caters you all the information regarding the SY0-201 exam but also provides you the excellent SY0-201 study guide which makes the certification exam easy for you.

Exam4Test Engine Features

Comprehensive questions and answers about SY0-201 exam

SY0-201 exam questions accompanied by exhibits

Verified Answers Researched by Industry Experts and almost 100% correct

SY0-201 exam questions updated on regular basis

Same type as the certification exams, SY0-201 exam preparation is in multiple-choice questions (MCQs).

Tested by multiple times before publishing

Try free SY0-201 exam demo before you decide to buy it in Exam4Test.com

Exam4Test Help You Pass Any IT Exam

[Exam4Test.com](#) offers incredible career enhancing opportunities. We are a team of IT professionals that focus on providing our customers with the most up to date material for any IT certification exam. This material is so effective that we Guarantee you will pass the exam or your money back.

Exam : CompTIA SY0-201

Title : CompTIA Security+

(2008 Edition) Exam

1. Which of the following should a technician recommend to prevent physical access to individual office areas? (Select TWO).

- A. Video surveillance
- B. Blockade
- C. Key card readers
- D. Mantrap
- E. Perimeter fence

Answer: CD

2. Which of the following type of attacks requires an attacker to sniff the network?

- A. Man-in-the-Middle
- B. DDoS attack
- C. MAC flooding
- D. DNS poisoning

Answer: A

3. All of the following can be found in the document retention policy EXCEPT:

- A. type of storage media.
- B. password complexity rules.
- C. physical access controls.
- D. retention periods.

Answer: B

4. Which of the following type of attacks is TCP/IP hijacking?

- A. Birthday
- B. ARP poisoning
- C. MAC flooding
- D. Man-in-the-middle

Answer: D

5. A CEO is concerned about staff browsing inappropriate material on the Internet via HTTPS. It has been suggested that the company purchase a product which could decrypt the SSL session, scan the content and then repackage the SSL session without staff knowing. Which of the following type of attacks is similar to this product?

- A. Replay
- B. Spoofing
- C. TCP/IP hijacking
- D. Man-in-the-middle

Answer: D

6. When deploying 50 new workstations on the network, which of following should be completed FIRST?

- A. Install a word processor.
- B. Run the latest spyware.
- C. Apply the baseline configuration.
- D. Run OS updates.

Answer: C

7. Which of the following are the functions of asymmetric keys?

- A. Decrypt, decipher, encode and encrypt
- B. Sign, validate, encrypt and verify
- C. Decrypt, validate, encode and verify
- D. Encrypt, sign, decrypt and verify

Answer: D

8. The marketing department wants to distribute pens with embedded USB drives to clients. In the past this client has been victimized by social engineering attacks which led to a loss of sensitive data. The security administrator advises the marketing department not to distribute the USB pens due to which of the following?

- A. The risks associated with the large capacity of USB drives and their concealable nature
- B. The security costs associated with securing the USB drives over time
- C. The cost associated with distributing a large volume of the USB pens
- D. The security risks associated with combining USB drives and cell phones on a network

Answer: A

9. Snort, TCPDump and Wireshark are commonly used for which of the following?

- A. Port scanning
- B. Host monitoring
- C. DDoS attacks
- D. Network sniffing

Answer: D

10. Which of the following BEST describes using a third party to store the public and private keys?

- A. Public key infrastructure
- B. Recovery agent
- C. Key escrow
- D. Registration authority

Answer: C

11. Classification of information is critical to information security because it:

- A. defines what information should have the highest protection.

- B. demonstrates that the company is using discretionary access control (DAC).
- C. allows a company to share top secret information.
- D. is a requirement for service level agreements (SLA).

Answer: A

12. Which of the following algorithms have the smallest key space?

- A. IDEA
- B. SHA-1
- C. AES
- D. DES

Answer: D

13. Which of the following could BEST assist in the recovery of a crashed hard drive?

- A. Forensics software
- B. Drive optimization
- C. Drive sanitization
- D. Damage and loss control

Answer: A

14. Which of the following can be used to encrypt FTP or telnet credentials over the wire?

- A. SSH
- B. HTTPS
- C. SHTTP
- D. S/MIME

Answer: A

15. An administrator in a small office environment has implemented an IDS on the network perimeter to detect malicious traffic patterns. The administrator still has a concern about traffic inside the network originating between client workstations. Which of the following could be implemented?

- A. HIDS
- B. A VLAN
- C. A network router
- D. An access list

Answer: A

16. A CRL contains a list of which of the following type of keys?

- A. Both public and private keys
- B. Steganographic keys
- C. Private keys
- D. Public keys

Answer: A

17. An instance where a biometric system identifies users that are authorized and allows them access is called which of the following?

- A. False negative
- B. True negative
- C. False positive
- D. True positive

Answer: D

18. A corporation has a contractual obligation to provide a certain amount of system uptime to a client. Which of the following is this contract an example of?

- A. PII
- B. SLA

- C. Due diligence
- D. Redundancy

Answer: B

19. Which of the following BEST describes the form used while transferring evidence?

- A. Booking slip
- B. Affidavit
- C. Chain of custody
- D. Evidence log

Answer: C

20. A company takes orders exclusively over the Internet. Customers submit orders via a web-based application running on the external web server which is located on Network A. Warehouse employees use an internal application on its own server, to pick and ship orders, located on Network B. Any changes made after the order is placed are handled by a customer service representative using the same internal application. All information is stored in a database, which is also located on Network B.

The company uses these four sets of user rights:

- NONE
- ADD (read existing data, write new data)
- CHANGE (read, write and change existing data)
- READ (read existing data)

The company has 2 different network zones:

- Network A, the DMZ, a public accessible network
- Network B, the internal LAN, accessible from company systems only

The company wants to restrict warehouse employee access. Which of the following permissions is the MOST appropriate for the warehouse employees?

- A. READ on Network B, NONE on Network A
- B. ADD on Network A, NONE on Network B
- C. CHANGE on Network A, ADD on Network B
- D. READ on Network A and B

Answer: A

[More SY0-201 Information](#)

Related SY0-201 Exams

SY0-201 *CompTIA Security+(2008 Edition) Exam*

sy0-101 *SECURITY+ CERTIFICATION*

BR0-001 *CompTIA Bridge Exam - Security+*

BR0-002 *CompTIA Network + Bridge Exam*

Other CompTIA Exams

<u>220-702</u>	<u>220-603</u>	<u>CT0-101</u>	<u>TK0-201</u>	<u>N10-103</u>	<u>xk0-001</u>	<u>220-602</u>	<u>PD1-001</u>
<u>220-601</u>	<u>IK0-002</u>	<u>HT0-102</u>	<u>N10-004</u>	<u>220-604</u>	<u>n10-003</u>	<u>BR0-001</u>	<u>SY0-201</u>
<u>EK0-002</u>	<u>RF0-001</u>	<u>JK0-016</u>	<u>220-303</u>				