



SY0-201

(CompTIA Security+ (2008 Edition) Exam)

Total Questions: 397

Last Updated: Apr 06, 2009

Document version: 8.27.11

Thanks for purchasing techXams' Study Guide,

techXams' SY0-201 study guide is a comprehensive compilation of questions and answers that have been developed by our team of certified professionals. In order to prepare for the actual exam, all you need is to study the content of this guide. An average of approximately 10 to 20 hours should be spent to study this guide and you will surely pass your exam. It's our guarantee.

Disclaimer

Neither this guide nor any material in this guide is sponsored, endorsed or affiliated with any of the respective vendor. All trademarks are properties of their respective owners.

Guarantee

If you study this guide properly and still unable to pass the exam, please send us a scanned copy of your official score at: refund@techeXams.ws. We will happily reimburse the cost of this study guide or send you an exchange of study guide of your choice free of cost.

Feedback

If you find any possible improvement, then please do let us know. We are always interested in improving the quality of this product. Feedback can be send at: feedback@techeXams.ws

Copyright

techXams holds the copyright of this material. techXams grants you a limited license to view and study this material, either for personal or commercial use. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Question: 1

Who is responsible for establishing access permissions to network resources in the DAC access control model?

- A. The system administrator.
- B. The owner of the resource.
- C. The system administrator and the owner of the resource.
- D. The user requiring access to the resource.

Answer: B

Question: 2

The Public Key Infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. The public key infrastructure is based on which encryption schemes?

- A. Symmetric
- B. Quantum
- C. Asymmetric
- D. Elliptical curve

Answer: C

Question: 3

Why will a Faraday cage be used?

- A. To find rogue access points
- B. To allow wireless usage
- C. To mitigate data emanation
- D. To minimize weak encryption

Answer: C

Question: 4

Which definition best defines what a challenge-response session is?

- A. A challenge-response session is a workstation or system that produces a random challenge string that the user provides, when prompted, in conjunction with the proper PIN (Personal Identification Number).
- B. A challenge-response session is a workstation or system that produces a random login ID that the user provides, when prompted, in conjunction with the proper PIN (Personal Identification Number).
- C. A challenge-response session is a special hardware device used to produce random text in a cryptography system.

2

D. A challenge-response session is the authentication mechanism in the workstation or system that does not determine whether the owner should be authenticated.

Answer: A

Question: 5

The hashing algorithm used in NTLMv2 is not possible to derive the original input number. Which hashing algorithm?

- A. NTLMv2
- B. LANMAN
- C. NTLM
- D. VLAN

possible to derive the original input number. Which hashing algorithm?

Answer: A

Question: 6

For which reason are clocks used in Kerberos authentication?

- A. Clocks are used to generate timestamps.
- B. Clocks are used to generate random numbers.
- C. Clocks are used to generate session keys.
- D. Clocks are used to generate symmetric keys.

algorithm.

Answer: B

Question: 7

Network utilization on a port can be high. Which of the following is a sign that the port can handle the traffic? When utilization is abnormal, which of the following is a sign that the port can handle the traffic?

Network traffic that the port can handle. Whether network utilization is abnormal, which of the following is a sign that the port can handle the traffic?

- C. System logs show high utilization.
- D. Security logs show high utilization.

Answer: B

Question: 8

To reduce vulnerabilities on a web server, an administrator should adopt which of the following preventative measures?

- A. Use packet sniffing software on all inbound communications
- B. Apply the most recent manufacturer updates and patches to the server.
- C. Enable auditing on the web server and periodically review the audit logs

D. Block all Domain Name Service (DNS) requests coming into the server.

Answer: B

Question: 9

A travel reservation facing website. Any organization. One statement is correct

- A. RAID
- B. Warm site
- C. Proxy server
- D. Single point of

ons via a public
 cial damage for this
 ase servers. Which

SY0-201 Demo Exam

Answer: D

Question: 10

Which of the follow

- A. Birthday
- B. Buffer overflow
- C. Spam
- D. Brute force

Answer: B

Question: 11

An Intrusion detecti
 unwanted attempts

spe

- A. Signature
- B. Behavior-base
- C. Anomaly-based
- D. Heuristic-based

ned to detect
 nputer systems.

Answer: A

Question: 12

The employees at a company use a network of networked computers. The MCQ asks: Which of the following is not an advantage of that instant messaging is

- A. Communication is asynchronous
- B. Communication is synchronous
- C. Has no common bandwidth requirements
- D. Uses weak encryption

Answer: B

Question: 13

How is access control implemented in the RBAC model?

- A. The system administrator
- B. The owner of the resource
- C. The role or responsibility of the user
- D. None of the above

Answer: C

Question: 14

Removable storage devices are subject to several risks. Which of the following is the GREATER risk?

- A. Availability of data
- B. Integrity of data
- C. Not enough space
- D. Confidentiality

Question: 15

A VPN typically provides protection over:

- A. An intranet
- B. A modem
- C. A network interface card
- D. The Internet

SY0-201 Demo Exam

Answer: D

Question: 16

In which authentication protocol is the concept of a challenge-response used?

- A. CHAP
- B. PAP
- C. Kerberos
- D. RADIUS

Answer: C

Question: 17

Which of the following cannot claim that the data received is authentic?

- A. Anti-aliasing
- B. Data integrity
- C. Asymmetric cryptography
- D. Non-repudiation

Answer: D

Question: 18

Coaxial cable is a cable with an inner conductor surrounded by a tubular insulating layer typically made of polyethylene, which is then surrounded by a thin layer of braided shielding, or of a thin insulating layer on the outside.

Which of the following is a tubular insulating layer typically made of polyethylene, which is then surrounded by a thin layer of braided shielding, or of a thin insulating layer on the outside?

- A. Coaxial cable
- B. Fiber optic cable
- C. Twisted pair cable
- D. Diffraction grating

Answer: B

Question: 19

Which of the following portions of a corporate network is between the Internet and an internal network?

- A. IDS
- B. Demilitarized zone (DMZ)
- C. Filter router
- D. Bastion host

SY0-201 Demo Exam

Question: 20

A technician is conducting a forensic analysis of a system. Which step should be taken FIRST?

- A. Search for Trojans
- B. Look for hidden files
- C. Get a binary copy of the system
- D. Analyze temporal data

Answer: B

Question: 21

Which of the following is NOT a type of network access to a corporate network?

- A. Extranet
- B. Intranet
- C. VLAN
- D. Demilitarized zone

Answer: C

Question: 22

In a secure environment, which protocol is better?

- A. RADIUS because it is more secure
- B. TACACS because it is more secure
- C. TACACS because it is more secure

Answer: A

Question: 23

Which of the following types of firewalls is NOT a Layer 7 of the OSI model?

- A. Application-proxy
- B. Network address translation (NAT)
- C. Packet filters
- D. Stateful inspection

Answer: B

Answer: A

Question: 24

Which threat is increased by the introduction of removable storage devices such as USB hard drives to networks?

- A. Increased loss of data
- B. Introduction of malware
- C. Removal of sensitive data
- D. Introduction of denial of service

such as USB hard

Answer: C

Question: 25

Which goals can be achieved by implementing a security policy?

- A. To ensure that security is maintained
- B. To ensure that security is consistent
- C. To ensure that security is effective
- D. To ensure that security is enforceable

).

cy

Answer: C, D

Question: 26

A newly hired security specialist discovers that a network device has default settings that should be changed regularly.

- A. Install software updates
- B. Change the default settings
- C. Change the default password
- D. Perform a factory reset

ork security. The
; the network OS
are not required to
o take?

Answer: C

Question: 27

Which of the following can be used to implement a procedure to control inbound and outbound traffic on a network segment?

- A. Proxy
- B. NIDS
- C. ACL
- D. HIDS

Answer: C

Question: 28

Giving each user or group of users the minimum amount of access to perform their job is an example of which of the following?

- A. Least privilege
- B. Defense in depth
- C. Separation of duties
- D. Access control

SY0-201 Demo Exam

Answer: A

Question: 29

Which one of the following is a type of social engineering attack?

- A. Blue jacking.
- B. Bluesnarfing.
- C. Discovery mode.
- D. A smurf attack.

Answer: D

Question: 30

A company implements a security solution that requires users to use a device as a form of authentication. This implementation would violate which of the following?

- A. Keep the solution simple.
- B. Use a device as a form of authentication.

Answer: B

Question: 31

In computing, the Basic Input/Output System (BIOS) is a firmware interface known as the System BIOS, is a de facto standard defining a firmware interface for IBM PC Compatible computers. A user is concerned with the security of their laptop BIOS. The user would not like anyone to be able to access control functions except themselves. Which of the following could make the BIOS more secure?

- A. Password
- B. Flash the BIOS

- C. Encrypt the hard drive
- D. Create an access-list

Answer: A

Question: 32

A company is upgrading its network infrastructure. All users on the same floor and network segment are experiencing slow network performance. Which devices should be used to segment the network?

- A. Router
- B. Hub
- C. Switch
- D. Firewall

Which devices should be used to segment the network of users on the same floor and network segment experiencing slow network performance?

Answer: C

Question: 33

In computing, a Uniform Resource Identifier (URI) that specifies the location of a resource on the Internet. When a URI is used to retrieve a resource, which attack will most likely occur if the URI has changed?

- A. ARP poisoning
- B. DLL injection
- C. DNS poisoning
- D. DDoS attack

Which attack will most likely occur if the Uniform Resource Identifier (URI) has changed, when a URI is used to retrieve a resource on the Internet?

Answer: C

Question: 34

When

- A. Notify the user
- B. Determine the cause
- C. Contact law enforcement
- D. Contain the problem.

Answer: D

SY0-201 Demo Exam