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

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.

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 algorith… possible to derive the original input nu… shing algorithm?

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

Answer: A

Question: 6

For which reason ar…

A. Clocks are used…
B. Clocks are used…
C. Clocks are used…
D. Clocks are used… gorithm.

Answer: B

Question: 7

Network utilization … m traffic that the port can handle. Wh… whether network utilization is abnorm…

C. Sy…
D. Securit…

Answer: B

Question: 8

To reduce vulnerabilities on a web server, a… ministrator 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 ... ons via a public facing website. Any ... cial damage for this organization. One w... ase servers. Which statement is correct...

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

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... ned to detect unwanted attempts... nputer systems. spec...

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

Answer: A

SY0-201 Demo Exam

Question: 12

The employees at a networked computers. The MC nstant messaging is that instant messag

A. Communicatio
B. Communicatio
C. Has no commo
D. Uses weak enc

Answer: B

Question: 13

How is access contr ol model?

A. The system adr
B. The owner of t
C. The role or resp
D. None of the ab

Answer: C

Question: 14

Removable storage self. Which of the following is the GRE

A. Availability of d
B. Integrity of dat
C. Not enough spa
D. Confidentiality

Question

A VPN typically pr 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 authentica concept?

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

Answer: C

Question: 17

Which of the follow received an email cannot claim that th

A. Anti-aliasing
B. Data integrity
C. Asymmetric cry
D. Non-repudiatio

Answer: D

Question: 18

Coaxial cable is a ca a tubular insulating layer typi ctric constant, all of which is then sur e woven wire for flexibility, or of a thi a thin insulating layer on the outside le?

D. Dif

Answer: B

Question: 19

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

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

SY0-201 Demo Exam

Answer: B

Question: 20

A technician is cond… Which step should be taken FIRST?

A. Search for Troja…
B. Look for hidden…
C. Get a binary cop…
D. Analyze tempor…

Answer: C

Question: 21

Which of the followi… access to a network?

A. Extranet
B. Intranet
C. VLAN
D. Demilitarized zo…

Answer: A

Question: 22

In a secure environm… better?

A. RADIUS because…
B. TACACS because…
C. TACACS because…

…nswer: B

Question: 23

Which of the following types… layer 7 of the OSI model?

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

SY0-201 Demo Exam

Answer: A

Question: 24

Which threat is incr… e such as USB hard drives to networks?

A. Increased loss …
B. Introduction of …
C. Removal of sen…
D. Introduction of …

Answer: C

Question: 25

Which goals can be …).

A. To ensure that …
B. To ensure that …
C. To ensure that … cy
D. To ensure that …

Answer: C, D

Question: 26

A newly hired secur… ork security. The security specialist d… ; the network OS has default settings… are not required to be changed regularl… o take?

A. Install software…

D. P…

Answer: C

Question: 27

Which of the following can be used t… rocedure 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 g job is an example of which of the follo

A. Least privilege
B. Defense in dept
C. Separation of du
D. Access control

Answer: A

Question: 29

Which one of the fol

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

Answer: D

Question: 30

A company impleme ntation would violate which of the

A. Keep the soluti
B. Use a device as

Answer: B

Question: 31

In computing, the Basic Input/Ou known as the System BIOS, is a de facto standard defining a firmware M PC Compatible computers. A user is concerned with the security of their lapt OS. 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 upgra... users on the same floor and network s... lowing network devices should be u...

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

Answer: C

Question: 33

In computing, a Un... esource Identifier (URI) that specifies ... echanism for retrieving it. When ... RL has changed, which attack will M...

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

Answer: C

Question: 34

Wh...

A. Notify ...
B. Determine th...
C. Contact law enfor...
D. Contain the problem.

Answer: D

SY0-201 Demo Exam