SY0-101

(Security+)

Total Questions: 1101

Last Updated: Feb 25, 2009

Document version: 8.27.11

Thanks for purchasing techXams' Study Guide,

techXams' SY0-101 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

Which of the following is NOT a valid access control mechanism?

A. DAC (Discretionary Access Control) list.
B. SAC (Subjective Access Control) list.
C. MAC (Mandatory Access Control) list.
D. RBAC (Role Based Access Control) list.

Answer: B

Explanation:

The three basic access control mechanisms are: MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). There is no SAC (Subjective Access Control) list.

Incorrect Answers:

C: The three basic access control mechanisms are: MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). MAC is based on predefined access privileges to a resource.
A: The three basic access control mechanisms are: MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). DAC is based on the owner of the resource allowing other users access to that resource.
D: The three basic access control mechanisms are: MAC (Mandatory Access Control), DAC (Discretionary Access Control) and RBAC (Role Based Access Control). RBAC is based on the role or responsibilities users have in the organization.

References:

Michael Cross, Norris L. Johnson, Jr. and Tony Piltzecker, Security+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, pp. 8-10. Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004,
p. 13.

Question: 2

Which of the following best describes an access control mechanism in which access control decisions are based on the responsibilities that an individual user or process has in an organization?

A. MAC (Mandatory Access Control)
B. RBAC (Role Based Access Control)
C. DAC (Discretionary Access Control)

D. None of the above.

Answer: B

Explanation:

Access control using th rs have in the organization. These us emented system wide.

Incorrect Answers:

A: Access control using to a resource.
C: Access control using owing other users access to that resourc
D: Access control using sers have in the organization.

References:

Michael Cross, Norris and DVD Training System, Rockland, MA ney, Security+ Study Guide, 2nd Edition, Al p. 13.

Question: 3

Which of the follow t allows the data owner to create and

B.
C. LBAC
D. DACs (Dis

Answer: D

Explanation:

The DAC model allows the owner of a resou access privileges to that resource. This model is dynamic in nature and all s the owner of the resource to grant or revoke access to individuals or groups of individuals.

Incorrect Answers:

A: Access control usin ...s to a resource.
B: Access control usin ...users have in the organization.
C: Access control usin ...eges they have been granted to an object.

References:

Michael Cross, Norris ... and DVD Training System, Rockland, MA ...tt Dulaney, Security+ Study Guide, 2nd Edit ...
p. 13.

Question: 4

Which of the follow ...ccess Control) model?

A. DAC (Discretio ... or process, leaving room for a Trojan ...
B. DAC (Discretio ...ers to use those certificates.
C. DAC (Discretio ...r, allowing anyone to use an account.
D. DAC (Discretio ...

Answer: A

Explanation:

ac ...as is the res ...ious code is not h ...

References:

Michael Cross, Norris L. Johnson, Jr. and ...curity+ Study Guide and DVD Training System, Rockland, MA, Syngress, 2002, p. 72 ...astore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p. 393.

SY0-101 Demo Exam

Question: 5

Which of the follow ular access to protected objects?

A. Capabilities
B. Access control l
C. Permission bits
D. Profiles

Answer: B

Explanation:

Access control lists en cified users or systems, or grant certa t of access controls to be established in yo dministrator to design and adapt the

References:

Mike Pastore and Emr a, Sybex, 2004, pp. 13, 216, 219

Question: 6

You work as the sec ssions on a file object in a network cess Control). The ACL (Access Control ecute User A: Read, Write, - User Other Read, Write, - User "A" is the ow up. What effective

A.
B. User
C. User B has
D. User B has read

Answer: A

Explanation:

ACLs have a list of users and their associated acce that they have been granted to a resource such as a file. When a user attempts to access a resource the ACL is checked to see if the user has the required privileges, if the required privileges are not found, access is denied. In this ACL, User B does not have an associated access privilege to the resource. Therefore User B has no permissions on the resource and will not be able to access it.

Incorrect Answers: B, C, D: In this ACL, User B does not have an associated access privilege to the resource. Therefore User B has absolutely no permissions on the resource.

References:

Mike Pastore and Emi…da, Sybex, 2004, pp. 13, 211 Michael Cross…ly Guide and DVD Training System, Rock…

Question: 7

You work as the sec… a RBAC (Role Based Access Contr… e security implementation. Th… ters, and mailboxes and four… ng Sales, Marketing, Manage… ent needs access to different resources… u create to support the RBAC (Role Bas…

A. File, printer, an…
B. Sales, marketin…
C. User and works…
D. Allow access a…

Answer: B

Explanation:

Access control using t… rs have in the organization. These r… division into different department… BAC model could be…

Incorrect A…

A: The RBAC model is … inter, and mailbox roles. These resource roles … ccess requirements to them.
C: The RBAC model is based on user ro… tween users and machines. Grouping all users together does not differentiate be… erent access requirements of different users based on the role that those user… ulfill in the organization.
D: By implementing allow access and deny access roles, we would create only two options: access to all resources or no access. This does not differentiate between the different access requirements of different users based on the role that those users fulfill in the organization.

References:

Michael Cross, Norris and DVD Training System, Rockland, MA aney, Security+ Study Guide, 2nd Edition, Al p. 13.

Question: 8

With regard to DAC ing statements are true?

A. Files that don't
B. The administra
C. The operating s
D. Each object has

Answer: D Explanat

The DAC model allow hat resource. Thus, access control is entir er the resource.

Incorrect Answers:

A: Each file does have ser to whom the creator of the file has
B: The creator of the tor

References:

Michael Cross, Norris L. J ide and DVD Training System, Rockland, MA, Syngre nett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, p. 13.

Question: 9

Which of the followi... ndatory Access Control) environmer...

A. Access control li...
B. Ownership
C. Group members...
D. Sensitivity label...

Answer: D

Explanation:

Mandatory Access Con... governments. All objects are given secur... cordingly. Then all users are given specifi... s.

Incorrect Answers:

A: DAC uses an Access ... granted access to a resource.
B: DAC is based on the ... rols access to that resource.
C: RBAC is based on gr... fulfill in the organization and the st...

References:

Michael Cross, Norris L... and DVD Training System, Rockland, MA, ... ey, Security+ Study Guide, 2nd Edition, Ala... p. 13.

Question: 10

Which of the following... ecisions to be based on security labels associate...

A. MAC (Mandatory Access Control)
B. RBAC (Role Based Access Control)
C. LBAC (List Based Access Control)
D. DAC (Discretionary Access Control)

Explanation:

Answer: A

Mandatory Access Control is a strict hierarchical model usually associated with governments. All objects are given secu cordingly. Then all users are given specifi s.

Incorrect Answers:

A: RBAC is based on gr fulfill in the organization and the s
C: LBAC is based on a l n object. This list is usually created by the
D: DAC is based on the trols access to that resource.

References:

Michael Cross, Norris L and DVD Training System, Rockland, MA ney, Security+ Study Guide, 2nd Edition, Ala p. 13.

Question: 11

Which of the followi earance and data classification?

A. RBAC (Role Base
B. NDAC (Non-Disc
C. MAC (Mandator
D. DAC (Discretion

r: C

Explanati

MAC is a strict hierar nd categorizing data by department. User data.

Incorrect Answers:

A: RBAC is based on the role users fulfill in the organization.
B: There is no NDAC.
D: DAC is based on the ownership of a resource. The owner of the resource controls access to that resource.

References:

Michael Cross, Norris and DVD Training System, Rockland, MA aney, Security+ Study Guide, 2nd Edition, Al p. 13.

Question: 12

Which of the follow ntrol)?

A. Uses levels of s
B. Allows owners cuments.
C. Uses access cor
D. Uses access cor

Answer: A

Explanation:

MAC is a strict hierarc e and categorizing data by department. U ta.

Incorrect Answers:

B: DAC is based on ow s access to that resource. C, D: DAC ar sers who have been granted access to a re

References:

Sy ay Guide, 2 p. 13.

Question: 13

Which of the following terms best repres AC (Mandatory Access Control) model?

A. Lattice
B. Bell La-Padula
C. BIBA
D. Clark and Wilson

Answer: A

Explanation:

The word lattice is use ess permission. In other words, a user's a model that is based on classifying data on st have the correct level of security clearа sed on.

Incorrect Answers:

B: TheBell La-Padu has a higher security rating than that w rmation from being written to a lower n which is used in MAC. However, it
C: TheBIBA model ed with information integrity.
D: TheClark and W only be accessed through applicatio horized modification, errors, and fraud f

References:

Mike Pastore and Emr a, Sybex, 2004, pp. 455, 267-269.

Question: 14

Which of the follow onse mechanisms?

D. Sma

Answer: B

Explanation:

An synchronous password generator, ver that generates a challenge (a large number or string) which is encrypted key of the token device and has that token device's public key so it can verify authent of the request (which is independent from the time factor). That challenge can also include a hash of transmitted data, so not only can the authentication be assured; but also the data integrity.

Reference:

Todd King, The Security+ Training Guide, Que Publishing, Indianapolis, 2003, Part 1, Chapter 1

Question: 15

Which of the followi… rovide for a large number of users?

A. Self service pass…
B. Locally saved pa…
C. Multiple access …
D. Synchronized pa…

Answer: A

Explanation:

A self service password… password, they can reset it on their own (u… hen receiving a new temporary password o… help desk. For a system with many use…

Incorrect answers:

B: Locally saved passw… orks and large amounts of users.
C: A multi-factor syste… rt of the authentication process…
D: Synchronized passw…

Reference: Todd Kin… ianapolis, 2003, Part 1, Chapter 2

Question: 16

Which of the following provid… intercepted password?

A. VPN (Virtual Private Network).
B. PPTP (Point-to-Point Tunneling Protocol).
C. One time password.
D. Complex password requirement.

Explanation:

Answer: C

A one time password is simply a password that has to be changed every time you log on; effectively making any intercepted the legitimate user happens to login them word it would probably already be ex hours.

Incorrect Answers:

A: VPN tunnels through ate networks. However, these conne col, such as PPTP, and an encryption prot
B: PPTP is a tunneling p ate against interception.
D: Complex password r sing brute force and dictionary attacks. How epted.

References:

Michael Cross, Norris L nd DVD Training System, Rockland, MA, mmett Dulaney, Security+ Study Guide,

Question: 17

Which of the followi

A. A workstation o e user enters when prompted along wi
B. A workstation o r enters when

D. her should

Answer: A

Explanation:

A common authentication technique v mpted (the challenge) to provide some private information (the response). M tems that rely on smart cards are based on challenge-response. A user is given a code (th lenge) which he or she enters into the smart card. The smart card then displays a new code (the response) that the user can present to log in.

Incorrect Answers:

B: Challenge-response sessions do not generate random login Emails but random challenges.
C: Challenge-response sessions encrypt the challenge or the response. The con
D: The purpose of aut ticated.

References:

Michael Cross, Norris and DVD Training System, Rockland, MA
http://www.weboped

Question: 18

Which of the follow ectly?

A. Dynamic IP (Int
B. Separate netwo
C. Token authenti
D. Time synchroni

Answer: D

Explanation:

Time synchronization ime as part of the authentication proces (KDC) to orchestrate the process. The KDC m, or a system) and provides it with a tick e against other principles. This occurs another principle. Kerberos is quickly be only significant weakness is that the K the authentication

Incorrect

A: This is irrelevant.
B: Time synchronization is
C: Tokens devices are not as esse zation is.

Reference:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004,
p.17

Question: 19

Why are clocks used

A. To ensure prop
B. To ensure ticke
C. To generate the
D. To benchmark

Answer: B

Explanation:

The actual verification ...or. The authenticator contains the client's id... is up-to-date and is not an old one that ha... henticator is checked against the current tir... ne (typically within five minutes) then the... res your system clocks to be loosely sy... ed in Version 5 to be whatever you want).

Incorrect answers:

A: Proper connections...
C: Generating seed va...
D: You do not need ti... tion algorithms.

References:

http://www.faqs.org/...

Which of... authentication...

A. Kerberos can be sus... authorized access.
B. Kerberos tickets can be sp... K resources.
C. Kerberos requires a centrally m... r and resource passwords.
D. Kerberos uses clear text passwords.

Explanation:

Answer: C

If the key distribution centre is down, all of other systems dependent on those keys won't be able to function.

Incorrect answers:

A: This will not prever
B: This will not prever
D: Encryption is part c

Reference:

Mike Pastore and Emr la, Sybex, 2004, p.17

Question: 21

You work as the sec ensure that only encrypted passwor ation protocol should you use?

A. PPTP (Point-to-
B. SMTP (Simple M
C. Kerberos
D. CHAP (Challeng

Answer: D

Explanation:

CHAP is commonly us entication within an

Incorrect answ

A: PPTP is a tunneling prot
B: SMTP is a protocol for sendin
C: Kerberos is an authentication sche de keys) embedded within messages.

Reference:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004,
p.112

Question: 22

Which of the follow

A. Authentication
B. SAM (Sequenti server.
C. Application da
D. Authentication

Answer: A

Explanation:

Kerberos authenticat e process. The KDC authenticates the pri rovides it with a ticket. Once this ticke inciples. This occurs automatically when a

Incorrect answers:

B: SAM is not require
C: There is no need fo
D: A privilege server a

Reference:

Mike Pastore and Em da, Sybex, 2004, pp.16-17

When do andshake process?

A. When establishing a on is established.
B. Only when establishing a
C. Only when establishing a conne
D. Only when disconnecting.

Answer: A

Explanation:

CHAP performs the ha d then at random intervals during the tr

Incorrect answers:

B: CHAP also challeng
C: CHAP also challeng
D: CHAP also challeng

Reference:

Mike Pastore and Emi da, Sybex, 2004, p.15

Question: 24

For which of the fol

A. Accountability
B. Certification
C. Authorization
D. Authentication

Answer: D

Explanation:

Biometrics devices us

A: Account
B: Certification
C: Authorization is no

References:

Mike Pastore and Emmett Dulaney, Security+ St Guide, 2nd Edition, Alameda, Sybex, 2004, pp 18-19

Question: 25

Which of the following is the most costly method of an authentication?

A. Passwords
B. Tokens
C. Biometrics
D. Shared secrets

Answer: C

Explanation:
Biometrics

These technologies ar sed over the next few years. Many companie rol. Implementations have been limited in n these technologies.

Incorrect answers: A

Passwords, tokens and re not as costly as biometrics.

References:

Mike Pastore and Emr a, Sybex, 2004, pp. 18-19, 265

Question: 26

Which of the follow

D. One

Answer: C

Explanation:

Biometrics is the use of authenticating their unique physiological body parts. Just like in the movies, a user places t finger print scanner or they put their eyes against a retinal scanner. If the ima matches what's on the database, it authenticates the user. Since a persons fingerprint, blood vessel print, or retinal image is unique the only way the system can authenticate is if the proper user is there. The only way an unauthorized user to get access is to physically kidnap the authorized user and force them through the system. For this reason, biometrics are the strongest (and the costliest) for of authentication.

Incorrect answers:

A: Tokens are not as reliable as biometrics.
B: Usernames and passwords can be intercepted.
D: One time passwor choices given.

References:

Mike Pastore and Em da, Sybex, 2004, pp. 18-19, 265

Question: 27

Which of the follov browser?

A. Do not upgrad
B. Disable any un
C. Connect to the ection.
D. Implement a f

Answer: B

Explanation:

Features that make w GI scripts, and cookies all pose security conc wser security level to High) is the best met nd within every users reach.

Incorrect answers:

A: As newer versions wever, this is not the

Hov
and an e
D: This does n

Reference:

Mike Pastore and Emmett Dulaney, Secur , 2nd Edition, Alameda, Sybex, 2004, pp.112-114

Question: 28

How many ports in TCP/IP (Transmission Control Protocol/Internet Protocol) are vulnerable to being

A. 32
B. 1,024
C. 65,535
D. 16,777,216

Answer: C

Explanation:

Internet Control Mess…vn attack signatures. The Ping utility uses I…k or may be the attack itself. If a host …MP traffic, this behavior should set o…econnaissance used to discover informatic…en a precursor to such activity. Port sca… port 65535, or random. A knowledge… an alert.

Reference: Kirk Hau… Cram 2 (Exam SYO-101), Que Publishin…mmett Dulaney, Security+ Study Gui…. 67

Question: 29

Which of the follow…r require?

B. …
C. 53
D. 55

Answer: C

Explanation:

Port 53 is used for Domain Name System (D…eries

Incorrect answers:

A: Ports 20 and 21 are associated with FTP, where 20 are used for file transfer data and 21 for command and control data.
B: Telnet uses port 23.
D: DHCP makes use of port 55.

Reference:

Microsoft Corporation ... aining Kit e-Book, Microsoft Press, Redm...
http://www.iana.org/...

Question: 30

Which of the follow... hat is larger than the buffer was desig...

A. Brute Force atta...
B. Buffer overflow...
C. Man in the mid...
D. Blue Screen of ...
E. SYN flood
F. Spoofing attack...

Answer: B

Explanation:

Buffer overflows occu... mmed to accept. This situation can caus... the system sending the data with tempora...

Incorrect answers:

A: A brute force attack... occurs... pack...
D: WinNu... running Windows NT 3.... ad data in the TCP header. Instead ... NT to the Blue Screen of Death (BSOD). ... ater.
E: A SYN flood attack forces a v... number of connections for each connection the initiator opens... e so quickly, the victim system has no time to free dangling, incomplete con... its resources are consumed.
F: A spoofing attack is simply an attempt by someone or something masquerading as someone else. This type of attack is usually considered an access attack.

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 135

Question: 31

Which of the follow ne Transport Control Program (TC

A. Buffer Overflow
B. SYN Attack
C. Smurf
D. Birthday Attack

Answer: B

Explanation:

SYN flood is a DoS atta e receiving station tries to respond to eac esources. All incoming connections ed. Change this if you want but in the SY ation with a spoofed return address of som on sends out this SYN packets (pings the bro to respond to the ping, thus overloading re, the hacker may send only 1 SYN packe what does the barrage of return pack

Incorrect answers:

A: Buffer overflow atta lly long input strings) into the buffer than it

C: A smurf attack is an with a false "from"

D: A

References:

Mike Pastore and Emmett Dula , Alameda, Sybex, 2004, p 530

Question: 32

Which of the following attacks uses ICMP (Internet Control Message Protocol) and improperly formatte rget computer?

A. Man in the midd
B. Smurf attack
C. Ping of death at
D. TCP SYN (Transr

Answer: C

Explanation:

The Ping of Death atta 5 bytes to the target computer. IP packets c capable of creating them. Carefully progra llegal IP packets, but some failed to do this. ximum size the underlying layer can ha reassembled by the receiver. For ethernet

Incorrect Answers:

A: A man in the middle onents of the data stream.
B: The "smurf" attack, t in the category of network-level attacks a echo (ping) traffic at IP broadcast addres
D: In a TCP SYN attack e completed. This causes the connection CP users.

Reference:

Mike Pastore and Emm a, Sybex, 2004,