



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

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

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)

2

D. None of the above.

Explanation:

Access control using the organization. These users are wide.

Incorrect Answers:

- A: Access control using
- C: Access control using access to that resource
- D: Access control using organization.

References:

Michael Cross, Norris I System, Rockland, MA Guide, 2nd Edition, Al p. 13.

Question: 3

Which of the following owner to create and

- B. ...
- C. LBAC
- D. DACs (Discretionary Access Control)

Explanation:

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

Answer: B

Users have in the implemented system

to a resource. allowing other users

Users have in the

and DVD Training Money, Security+ Study

that allows the data

Answer: D

SY0-101 Demo Exam

Incorrect Answers:

- A: Access control using...
- B: Access control using...
- C: Access control using...

...s to a resource.
 ...users have in the
 ...leges they have been

References:

Michael Cross, Norris
 System, Rockland, MA
 Study Guide, 2nd Edit
 p. 13.

...and DVD Training
 ...t Dulaney, Security+

Question: 4

**Which of the follow
 model?**

- A. DAC (Discretio
 room for a Trojan
- B. DAC (Discretio
 certificates.
- C. DAC (Discretio
 use an account.
- D. DAC (Discretio

...ccess Control)

...or process, leaving
 ...ers to use those
 ...r, allowing anyone to

Answer: A

Explanation:

acc...
 the res...
 code is not in...

...is is
 ...rious

References:

Michael Cross, Norris L. Johnson, Jr. and
 System, Rockland, MA, Syngress, 2002, p. 720.
 Guide, 2nd Edition, Alameda, Sybex, 2004,
 p. 393.

...Security+ Study Guide and DVD Training
 ...store and Emmett Dulaney, Security+ Study

Question: 5

Which of the following is used to control access to protected objects?

- A. Capabilities
- B. Access control lists
- C. Permission bits
- D. Profiles

Explanation:

Access control lists are used in operating systems, or grant certain permissions to be established in your system design and adapt the system to your needs.

References:

Mike Pastore and Emr...
 13, 216, 219

ular access to

Answer: B

specified users or
 t of access controls
 administrator to

a, Sybex, 2004, pp.

SY0-101 Demo Exam

Question: 6

You work as the security administrator for a network. You have configured an ACL (Access Control List) on a file server. The ACL is configured as follows:
 Read, Write, - User B
 - User "A" is the owner of the file.

- A. User A has read and write permissions.
- B. User B has read and write permissions.
- C. User B has read permissions.
- D. User B has read, write, and execute permissions.

Explanation:

ACLs have a list of users and their associated access privileges 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.

permissions on a file
 (Access Control List). The
 execute User A:
 Other Read, Write,
 up. What effective

Answer: A

5

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 Em... la, Sybex, 2004, pp.
 13, 211 Michael Cross... ly Guide and DVD
 Training System, Rock

Question: 7

You work as the security administrator for a company. You are implementing a RBAC (Role Based Access Control) model for the security implementation. The company has three departments: Sales, Marketing, and Accounting. Each department has different needs access to resources. You create to support the RBAC (Role Based Access Control) model.

- A. File, printer, and mailbox roles
- B. Sales, marketing, and accounting roles
- C. User and worksite roles
- D. Allow access and deny access roles

Answer: B

Explanation:

Access control using the RBAC model is based on the roles that users have in the organization. These roles are based on the different departmental needs. The RBAC model could be implemented by creating roles for each department.

Incorrect Answers:

- A: The RBAC model is based on the roles that users have in the organization. Printer, and mailbox roles. These resource roles do not differentiate between users based on their access requirements to them.
- C: The RBAC model is based on user roles, not on the relationship between users and machines. Grouping all users together does not differentiate between users based on their different access requirements of different users based on the role that those users fulfill 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.

SY0-101 Demo Exam

References:

Michael Cross, Norris L. Johnson and DVD Training System, Rockland, MA, Syngress, Security+ Study Guide, 2nd Edition, Alameda, Sybex, p. 13.

and DVD Training
 aney, Security+ Study

Question: 8

With regard to DAC, which of the following statements are true?

ing statements are

- A. Files that don't have permissions are not affected by DAC.
- B. The administrator can change permissions on any file.
- C. The operating system enforces DAC.
- D. Each object has a DAC.

Answer: D Explanation:

The DAC model allows the administrator to control access control is entirely up to the administrator.

that resource. Thus, the administrator controls access to the resource.

Incorrect Answers:

- A: Each file does have permissions, but DAC is not enforced by the operating system.
- B: The administrator can change permissions on any file, but DAC is not enforced by the operating system.
- C: The operating system enforces DAC, but DAC is not enforced by the operating system.

user to whom the resource is assigned. The administrator controls access to the resource.

References:

Michael Cross, Norris L. Johnson and DVD Training System, Rockland, MA, Syngress, Security+ Study Guide, 2nd Edition, Alameda, Sybex, p. 13.

and DVD Training
 mettt Dulaney, Security+ Study

SY0-101 Demo Exam

Question: 9

Which of the following is not a characteristic of Mandatory Access Control (MAC) environments?

- A. Access control lists
- B. Ownership
- C. Group membership
- D. Sensitivity labels

Explanation:

Mandatory Access Control (MAC) environments are used by governments. All objects are given security labels. Access is granted or denied accordingly. Then all users are given specific permissions.

Incorrect Answers:

- A: DAC uses an Access Control List (ACL) to grant or deny access to a resource.
- B: DAC is based on the user's role in the organization and the sensitivity of the resource.
- C: RBAC is based on group membership in the organization and the sensitivity of the resource.

References:

Michael Cross, Norris L. Johnson, *Security+ Study Guide, 2nd Edition*, Alameda, CA: Sybex, 2008, p. 13.

Answer: D

SY0-101 Demo Exam

Question: 10

Which of the following is not a decision to be based on security labels associated with objects?

- 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 security labels according to their classification. Then all users are given specific security labels. Only users with a higher security label than the object can access it.

Incorrect Answers:

- A: RBAC is based on the role users fulfill in the organization and the security labels of the objects.
- C: LBAC is based on a list of labels usually created by the owner of the resource. This list is used to control access to that resource.
- D: DAC is based on the ownership of a resource. The owner of the resource controls access to that resource.

References:

Michael Cross, Norris L. Johnson, and DVD Training System, Rockland, MA: Sybex, 2008, Security+ Study Guide, 2nd Edition, Alameda, CA: Sybex, p. 13.

Question: 11

Which of the following is a type of data classification?

- A. RBAC (Role Based Access Control)
- B. NDAC (Non-Discretionary Access Control)
- C. MAC (Mandatory Access Control)
- D. DAC (Discretionary Access Control)

Explanation:

MAC is a strict hierarchical model usually associated with governments and categorizing data by department. Users are given specific security labels. Only users with a higher security label than the object can access it.

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
 System, Rockland, MA
 Guide, 2nd Edition, Al
 p. 13.

and DVD Training
 aney, Security+ Study

Question: 12

Which of the follow

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

ontrol)?

uments.

Answer: A

Explanation:

MAC is a strict hierarc
 data by department. U

and categorizing
 ta.

Incorrect Answers:

B: DAC is based on ow
 resource. C, D: DAC ar
 granted access to a re

s access to that
 users who have been

References:

Sys
 Guide, 2
 p. 13.

ay

Question: 13

Which of the following terms best represent MAC (Mandatory Access Control) model?

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

Answer: A

Explanation:

The word lattice is used in other words, a user's access on classifying data on a level of security clearance.

... permission. In a model that is based on, the user must have the correct clearance level.

Incorrect Answers:

- B: The Bell-LaPadula model has a higher security rating than that which is used to write to a lower MAC. However, it does not provide integrity.
- C: The Biba model provides integrity.
- D: The Clark and Westcott model is used to prevent errors, and fraud.

... has a higher security rating than that which is used in the model. The Biba model is used with information that can only be accessed through authorized modification.

References:

Mike Pastore and Emr... 455, 267-269.

... a, Sybex, 2004, pp.

Question: 14

Which of the following...

... response mechanisms?

- C. ...
- D. Sma...

Answer: B

Explanation:

An asynchronous password generator, ... a challenge (a large number or string) which is encrypted with the key of the token device and has that token device's public key so it can verify authentication 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 following provides for a large number of users?

- A. Self service password
- B. Locally saved passwords
- C. Multiple access methods
- D. Synchronized passwords

Explanation:

A self service password reset system allows users to reset it on their own (using a self service password reset system) or receive a temporary password or a help desk. For a system with many users

Incorrect answers:

- B: Locally saved passwords are not suitable for large amounts of users.
- C: A multi-factor system is not part of the authentication process.
- D: Synchronized passwords are not suitable for large amounts of users.

Reference: Todd King, The Security+ Training Guide, Part 1, Chapter 1

Answer: A

SY0-101 Demo Exam

Question: 16

Which of the following provides protection against an 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 password useless. If a legitimate user happens to login their password it would probably already be expired in a few hours.

Incorrect Answers:

- A: VPN tunnels through secure networks. However, these connections are encrypted and an encryption protocol, such as PPTP, is used to protect the data. PPTP is not secure against interception.
- B: PPTP is a tunneling protocol used for VPN connections. It is not secure against interception.
- D: Complex password resistance to dictionary attacks. However, a password can be cracked using brute force and dictionary attacks.

References:

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

SY0-101 Demo Exam

Question: 17

Which of the following

- A. A workstation or server is prompted along with the user enters when
- B. A workstation or server is prompted along with the user enters when
- C. A workstation or server is prompted along with the user enters when
- D. A workstation or server is prompted along with the user enters when

Answer: A

Explanation:

A common authentication technique is challenge-response. The user is prompted (the challenge) to provide some private information (the response). Many authentication systems that rely on smart cards are based on challenge-response. A user is given a code (the challenge) 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.

Question: 19

Why are clocks used in Kerberos authentication?

- A. To ensure proper connections
- B. To ensure tickets are not too old
- C. To generate the authenticator
- D. To benchmark system performance

Answer: B

Explanation:

The actual verification of the ticket contains the client's id and the time. If the time is not an old one that has expired, the authenticator is checked against the current time (typically within five minutes) then the system allows access. Clocks to be loosely synchronized (within whatever you want).

or. The authenticator is up-to-date and is checked against the authenticator (typically within five minutes) then the system allows access. Clocks to be loosely synchronized (within whatever you want).

Incorrect answers:

- A: Proper connections
- C: Generating seed values
- D: You do not need time synchronization algorithms.

References:

<http://www.faqs.org/>

SY0-101 Demo Exam

Which of the following is NOT a characteristic of Kerberos authentication?

- A. Kerberos can be susceptible to replay attacks.
- B. Kerberos tickets can be used to access network resources.
- C. Kerberos requires a centrally managed user 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 prevent
- B: This will not prevent
- D: Encryption is part of

Reference:

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

Question: 21

You work as the security administrator for a company. You need to ensure that only encrypted passwords are sent over the network. Which authentication protocol should you use?

- A. PPTP (Point-to-Point Tunneling Protocol)
- B. SMTP (Simple Mail Transfer Protocol)
- C. Kerberos
- D. CHAP (Challenge Handshake Authentication Protocol)

Answer: D

Explanation:

CHAP is commonly used for authentication within an IPsec tunnel.

Incorrect answers:

- A: PPTP is a tunneling protocol.
- B: SMTP is a protocol for sending email.
- C: Kerberos is an authentication scheme that uses symmetric keys embedded within messages.

Reference:

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

SY0-101 Demo Exam

Question: 22

Which of the following is not required for Kerberos authentication?

- A. Authentication
- B. SAM (Sequential) hashes
- C. Application data
- D. Authentication server

Explanation:

Kerberos authentication process. The KDC authenticates the principal and provides it with a ticket. Once this ticket is received, the client automatically when a connection is established.

server.

Answer: A

the process. The KDC provides it with a ticket. This occurs

Incorrect answers:

- B: SAM is not required for Kerberos authentication.
- C: There is no need for application data.
- D: A privilege server is not required.

Reference:

Mike Pastore and Emory D. Smith, *Windows Security*, Sybex, 2004, pp.16-17

da, Sybex, 2004,

SY0-101 Demo Exam

When does a Kerberos handshake process occur?

- A. When establishing a connection is established.
- B. Only when establishing a connection.
- C. Only when establishing a connection.
- D. Only when disconnecting.

Answer: A

Explanation:

CHAP performs the handshake at regular intervals during the transmission and then at random

Incorrect answers:

- B: CHAP also challenges the client
- C: CHAP also challenges the server
- D: CHAP also challenges the network

Reference:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p.15

Question: 24

For which of the following is authentication used?

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

Explanation:

Biometrics devices use authentication to verify the user's identity.

- A: Accountability is used to track actions performed by users.
- B: Certification is used to verify the identity of a user or device.
- C: Authorization is used to determine what resources a user or device is allowed to access.

References:

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

SY0-101 Demo Exam

Answer: D

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 are expected to be used over the next few years. Many companies have been limited in their

control. Implementations of these technologies.

Incorrect answers: A, B, D

Passwords, tokens and shared secrets are not as costly as biometrics.

are not as costly as

References:

Mike Pastore and Emr...
 18-19, 265

...a, Sybex, 2004, pp.

SY0-101 Demo Exam

Question: 26

Which of the follow

- C.
- D. One

Answer: C

Explanation:

Biometrics is the use of authenticating users based on their unique physiological body parts. Just like in the movies, a user places their finger on a finger print scanner or they put their eyes against a retinal scanner. If the image 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 passwords are not a good choice given.

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp. 18-19, 265

Question: 27

Which of the following is the best method to protect a browser?

- A. Do not upgrade the browser.
- B. Disable any unnecessary browser features.
- C. Connect to the browser through a secure connection.
- D. Implement a firewall on the computer.

Explanation:

Features that make websites more secure (such as SSL scripts, and cookies) all pose security concerns. High) is the best method to reach.

Incorrect answers:

- A: As newer versions of the browser are released, they often include security updates. However, this is not the best method to protect a browser.

- How to protect a browser and an email client.
D: This does not protect a browser.

Reference:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, pp.112-114

SY0-101 Demo Exam

Answer: B

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

Explanation:

Internet Control Mess
 The Ping utility uses IC
 attack itself. If a host
 behavior should set o
 to discover informatio
 such activity. Port sca
 random. A knowledge

Reference: Kirk Hau
 101), Que Publishin
 Security+ Study Gui

Answer: C

own attack signatures.
 k or may be the
 MP traffic, this
 reconnaissance used
 ten a precursor to
 port 65535, or
 an alert.

**Cram 2 (Exam SYO-
 mmett Dulaney,
 . 67**

Question: 29

Which of the follow

- B.
- C. 53
- D. 55

Explanation:

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

Incorrect answers:

...r require?

Answer: C

SY0-101 Demo Exam

- 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
 Microsoft Press, Redmond, WA
<http://www.iana.org/>

Training Kit e-Book,

Question: 30

Which of the following attacks is the largest the buffer was designed to handle?

Which of the following attacks is larger than

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

Answer: B

Explanation:

Buffer overflows occur when a program writes more data to a buffer than it was designed to accept. This situation can cause the system to crash or the data with temporary corruption.

...designed to accept.
 ...the system sending

Incorrect answers:

A: A brute force attack is a type of attack that occurs when an attacker repeatedly enters a password or PIN until the correct one is found.

C: A man in the middle attack is a type of attack that occurs when an attacker intercepts and possibly alters the communication between two parties.

D: WinNLS is a Windows NT 3.51 bug that occurs when running Windows NT 3.51 on a computer with a non-English locale. The bug causes the system to read data in the TCP header. Instead of the expected data, the system reads the value of the WinNLS field, which causes the system to crash with a Blue Screen of Death (BSOD).

E: A SYN flood attack forces a victim system to allocate resources for each connection the initiator opens. Because the attacker sends the SYN requests so quickly, the victim system has no time to free dangling, incomplete connections. As a result, the victim's 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.

SY0-101 Demo Exam

References:

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

Question: 31

Which of the following is a Denial of Service (DoS) attack?

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

Explanation:

SYN flood is a DoS attack where the attacker tries to respond to each incoming connection you want but in the SYN return address of some packets (pings the browser, thus overloading send only 1 SYN packet barrage of return pack

Incorrect answers:

- A: Buffer overflow attack (involves sending a very long input strings)
- C: A smurf attack is an attack where the attacker sends a packet with a false "from" address to a broadcast address, which then floods the receiving station with resources. All of the resources are used. Change this if you want to use a different IP address. Change this if you want to use a different IP address.

D: A birthday attack is a type of cryptographic attack that exploits the mathematics behind the birthday paradox in order to find collisions.

References:

Mike Pastore and Emmett Dulaney, Security+ Study Guide, 2nd Edition, Alameda, Sybex, 2004, p 530

SY0-101 Demo Exam

Answer: B

Question: 32

Which of the following attacks uses ICMP (Internet Control Message Protocol) and improperly formatted packets to flood a target computer?

- A. Man in the middle
- B. Smurf attack
- C. Ping of death attack
- D. TCP SYN (Transmission Control Protocol) attack

Answer: C

Explanation:

The Ping of Death attack sends oversized ICMP packets to a target computer. IP packets are limited to 65,535 bytes. Some early implementations of IP stacks were not capable of creating or handling packets larger than 65,535 bytes. Carefully programmed implementations of IP stacks would reject these illegal IP packets, but some failed to do this. The oversized packets would cause the underlying layer to crash or hang, preventing the receiver from receiving any further data. For ethernet networks, the maximum packet size is 1500 bytes.

65,535 bytes to the target computer. Some early implementations of IP stacks were not capable of creating or handling packets larger than 65,535 bytes. Carefully programmed implementations of IP stacks would reject these illegal IP packets, but some failed to do this. The oversized packets would cause the underlying layer to crash or hang, preventing the receiver from receiving any further data. For ethernet networks, the maximum packet size is 1500 bytes.

Incorrect Answers:

- A: A man in the middle attack intercepts and possibly alters the contents of the data stream.
- B: The "smurf" attack, a type of Denial of Service (DoS) attack, is a network-level attack that floods a target with echo (ping) traffic at IP broadcast addresses.
- D: In a TCP SYN attack, an attacker sends a SYN packet to a target, causing the connection to be completed. This causes the target to become unresponsive to other TCP users.

A: A man in the middle attack intercepts and possibly alters the contents of the data stream.

B: The "smurf" attack, a type of Denial of Service (DoS) attack, is a network-level attack that floods a target with echo (ping) traffic at IP broadcast addresses.

D: In a TCP SYN attack, an attacker sends a SYN packet to a target, causing the connection to be completed. This causes the target to become unresponsive to other TCP users.

Reference:

Mike Pastore and Emr...

..., Sybex, 2004,

SY0-101 Demo Exam