JK0-022 Q&As

CompTIA Security+ Certification

Pass CompTIA JK0-022 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/jk0-022.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A new web server has been provisioned at a third party hosting provider for processing credit card transactions. The security administrator runs the netstat command on the server and notices that ports 80, 443, and 3389 are in a `listening\\' state. No other ports are open. Which of the following services should be disabled to ensure secure communications?

A. HTTPS

B. HTTP

C. RDP

D. TELNET

Correct Answer: B

HTTP uses port 80. HTTP does not provide encrypted communications. Port 443 is used by HTTPS which provides secure encrypted communications. Port 3389 is used by RDP (Remote Desktop Protocol) which does provide encrypted communications.

Incorrect Answers:

A: HTTPS uses port 443. HTTPS uses SSL or TLS certificates to secure HTTP communications. HTTPS (HTTP over SSL or HTTP Secure) is the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sublayer under regular HTTP application layering. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTP is secure so this answer is incorrect.

C: RDP (Remote Desktop Protocol) is used to remotely connect to a Windows computer. RDP uses encrypted communications and is therefore considered secure. This answer is therefore incorrect.

D: Telnet uses port 23. This is not one of the ports listed as open in the question. This answer is therefore incorrect.

References:

http://searchsoftwarequality.techtarget.com/definition/HTTPS
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 2

Which of the following concepts is a term that directly relates to customer privacy considerations?

A. Data handling policies

B. Personally identifiable information

C. Information classification

D. Clean desk policies

Correct Answer: B

Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This

data can be anything from the person\\'s name to a fingerprint (think biometrics), credit card number, or patient record. This has a direct relation to customer privacy considerations.

Incorrect Answers:

A: Data handling policies would refer to only those users needing to work with it should be able to access the data.

C: Information classification is done by confidentiality and comprises of three categories, namely: public use, internal use and restricted use.

D: Clean Desk Policy Information is used to protect data and your business, encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project they are working on at that moment. All sensitive information should be put away when the employee is away from their desk.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 404, 409, 412

QUESTION 3

Which of the following is a penetration testing method?

A. Searching the WHOIS database for administrator contact information

B. Running a port scanner against the target\\'s network

C. War driving from a target\\'s parking lot to footprint the wireless network

D. Calling the target\\'s helpdesk, requesting a password reset

Correct Answer: D

QUESTION 4

A technician wants to implement a dual factor authentication system that will enable the organization to authorize access to sensitive systems on a need-to-know basis. Which of the following should be implemented during the authorization stage?

A. Biometrics

B. Mandatory access control

C. Single sign-on

D. Role-based access control

Correct Answer: A

This question is asking about "authorization", not authentication.

Mandatory access control (MAC) is a form of access control commonly employed by government and military environments. MAC specifies that access is granted based on a set of rules rather than at the discretion of a user. The

rules that govern MAC are hierarchical in nature and are often called sensitivity labels, security domains, or classifications.

MAC can also be deployed in private sector or corporate business environments. Such cases typically involve the following four security domain levels (in order from least sensitive to most sensitive):

Public Sensitive Private Confidential

A MAC environment works by assigning subjects a clearance level and assigning objects a sensitivity label--in other words, everything is assigned a classification marker. Subjects or users are assigned clearance levels. The name of the clearance level is the same as the name of the sensitivity label assigned to objects or resources. A person (or other subject, such as a program or a computer system) must have the same or greater assigned clearance level as the resources they wish to access. In this manner, access is granted or restricted based on the rules of classification (that is, sensitivity labels and clearance levels). MAC is named as it is because the access control it imposes on an environment is mandatory. Its assigned classifications and the resulting granting and restriction of access can\\'t be altered by users. Instead, the rules that define the environment and judge the assignment of sensitivity labels and clearance levels control authorization. MAC isn\\'t a very granularly controlled security environment. An improvement to MAC includes the use of need to know: a security restriction where some objects (resources or data) are restricted unless the subject has a need to know them. The objects that require a specific need to know are assigned a sensitivity label, but they\\'re compartmentalized from the rest of the objects with the same sensitivity label (in the same security domain). The need to know is a rule in and of itself, which states that access is granted only to users who have been assigned work tasks that require access to the cordoned-off object. Even if users have the proper level of clearance, without need to know, they\\'re denied access. Need to know is the MAC equivalent of the principle of least privilege from DAC

Incorrect Answers:

A: Biometrics is used in authentication. Biometrics includes fingerprints and retina scans. This question is asking about "authorization", which generally comes after authentication.

C: Single sign-on is used to access multiple systems with a single login. Single sign-on is used for authentication, not authorization.

D: Role-based access control (RBAC) defines access to resources based on job role. We need to authorize access to sensitive systems on a need-to-know basis. Therefore, the default access should be "no access" unless the person can prove a `need to know\\'. RBAC would give everyone performing a role access to the sensitive system.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 278- 284.

QUESTION 5

Which of the following presents the STRONGEST access control?

A. MAC

B. TACACS

C. DAC

D. RBAC

Correct Answer: A

A: With Mandatory Access Control (MAC) all access is predefined. This makes it the strongest access control of the options presented in the question. Incorrect Answers:

B: TACACS refers to a client-server-oriented environment similar to that of RADIUS and is in essence an authentication service. It is an older authentication protocol common to UNIX networks that allows a remote access server to forward a user\\'s logon password to an authentication server to determine whether access can be allowed to a given system.

C: With Discretionary Access Control (DAC) access control incorporates some flexibility.

D: With Role-Based Access Control (RBAC) access control allows the user\\'s role to dictate access capabilities.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 146, 150