98-367 Q&As

Security Fundamentals

Pass Microsoft 98-367 Exam with 100% Guarantee

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

https://www.pass4itsure.com/98-367.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

What are three major attack vectors that a social engineering hacker may use? (Choose three.)

A. Telephone

B. Reverse social engineering

C. Waste management

D. Honey pot systems

E. Firewall interface

Correct Answer: ABC

QUESTION 2

Where should you lock up the backup tapes for your servers?

A. The server room

B. A filing cabinet

C. The tape library

D. An offsite fire safe

Correct Answer: D

Backup tapes should be stored off site, preferably in a fire safe, so that the data is available should a fire, flood, or other disaster affect the location were the servers are.

QUESTION 3

Which of the following is the process used by attackers for listening to the network traffic?

A. Eavesdropping

B. Subnetting

C. Sanitization

D. Hacking

Correct Answer: A

Eavesdropping is the process of listening to private conversations. It also includes attackers listening the network traffic. For example, it can be done over telephone lines (wiretapping), email, instant messaging, and any other method of

communication considered private.

Answer: C is incorrect. Sanitization is the process of removing sensitive information from a document or other medium so that it may be distributed to a broader audience. When dealing with classified information, sanitization attempts to

reduce the document\\'s classification level, possibly yielding an unclassified document. Originally, the term sanitization was applied to printed documents; it has since been extended to apply to computer media and the problem of data

remanence as well.

Answer: D is incorrect. Hacking is a process by which a person acquires illegal access to a computer or network through a security break or by implanting a virus on the computer or network.

Answer: B is incorrect. Subnetting is a process through which an IP address network is divided into smaller networks. It is a hierarchical partitioning of the network address space of an organization into several subnets. Subnetting creates

smaller broadcast domains. It helps in the better utilization of the bits in the Host ID.

QUESTION 4

You are an intern at Litware, Inc. Your manager asks you to make password guess attempts harder by limiting login attempts on company computers. What should you do?

A. Enforce password sniffing.

B. Enforce password history.

C. Make password complexity requirements higher.

D. Implement account lockout policy.

Correct Answer: D

Reference: http://technet.microsoft.com/en-us/library/dd277400.aspx

QUESTION 5

Mark works as a Security Administrator for TechMart Inc. The company has a a Windows-based network. Mark has gone through a security audit for ensuring that the technical system is secure and protected. While this audit, he identified many areas that need improvement. He wants to minimize the risk for potential security threats by educating team members in the area of social engineering, and providing basic security principle knowledge while stressing the Con?dentiality, Integrity, and Availability triangle in the training of his team members . Which of the following ways will Mark use for educating his team members on the social engineering process?

A. He will call a team member while behaving to be someone else for gaining access to sensitive information.

B. He will use group policies to disable the use of floppy drives or USB drives.

C. He will develop a social awareness of security threats within an organization.

D. He will protect against a Distributed Denial of Services attack.

Correct Answer: A

Social engineering can be defined as any type of behavior used to inadvertently or deliberately aid an attacker in gaining

access to an authorized user\\'s password or other sensitive information. Social engineering is the art of convincing people and making them disclose useful information such as account names and passwords. This information is further exploited by hackers to gain access to a user\\'s computer or network. This method involves mental ability of people to trick someone rather than their technical skills. A user should always distrust people who ask him for his account name, password, computer name, IP address, employee ID, or other information that can be misused.

Answer: B is incorrect. The group policies are used to disable the use of floppy drives or USB drives to ensure physical security of desktop computers. Several computers are able to use the mechanism of attaching a locking device to the desktops, but disabling USB and floppy drives can disable a larger set of threats. Answer: D is incorrect. While stressing the Con? dentiality, Integrity, and Availability triangle in the training of users, the process of providing availability is related to security training to ensure the protection against a Distributed Denial of Services attack.