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.geekcert.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

Which of the following protocols transmits user credentials as plaintext?

A. CHAP

B. MS-CHAP v2

C. PAP

D. MS-CHAP

Correct Answer: C

Password Authentication Protocol (PAP) is the least sophisticated authentication protocol, used mostly when a client calls a server running an operating system other than Windows. PAP has a number of security vulnerabilities because it

transmits user credentials as plaintext.

Answer: A is incorrect. Challenge Handshake Authentication Protocol (CHAP) is an authentication protocol that uses a secure form of encrypted authentication. Using CHAP, network dial-up connections are able to securely connect to almost

all PPP servers.

Answer: B is incorrect. Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) is the new version of MS-CHAP. MS-CHAP v2 provides the highest level of security and encryption for dial-up connection in the

environment consisting of both Windows NT and Windows 2000/XP dial-up clients. It provides mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving data. Answer: D is incorrect.

Microsoft created the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) to authenticate remote Windows workstations. It is designed especially for Windows 95, Windows 98, Windows NT, and Windows 2000 networking

products. This protocol provides data encryption along with password encryption.

QUESTION 2

Which of the following is a central, secure database in which Windows stores all hardware configuration information, software configuration information, and system security policies?

A. Registry

B. Program files folder

C. DLL file

D. Configuration file

Correct Answer: A

The registry is a central, secure database in which Windows stores all hardware configuration information, software configuration information, and system security policies.

The registry is the central storage for all configuration data. It stores Windows operating system configuration, computer hardware configuration, configuration information about Win32-based applications, and user preferences in a hierarchical

database file.

Answer: B, C, and D are incorrect. The Program files folder, DLL file, or Configuration file is not a central, secure database in which Windows stores all hardware configuration information, software configuration information, and system

security policies.

QUESTION 3

Which of the following is an authentication protocol?

A. Kerberos

B. LDAP

C. TLS

D. PPTP

Correct Answer: A

Kerberos is an industry standard authentication protocol used to verify user or host identity. Kerberos v5 authentication protocol is the default authentication service for Windows 2000. It is integrated into the administrative and security model,

and provides secure communication between Windows 2000 Server domains and clients.

Answer: C is incorrect. Transport Layer Security (TLS) is an application layer protocol that uses a combination of public and symmetric key processing to encrypt data.

Answer: B is incorrect. Lightweight Directory Access Protocol (LDAP) is a protocol used to query and modify information stored within directory services. Answer: D is incorrect. Point-to-Point Tunneling Protocol (PPTP) is a method for

implementing virtual private networks. PPTP does not provide confidentiality or encryption. It relies on the protocol being tunneled to provide privacy. It is used to provide secure, low-cost remote access to corporate networks through public

networks such as the Internet. Using PPTP, remote users can use PPP- enabled client computers to dial a local ISP and connect securely to the corporate network through the Internet. PPTP has been made obsolete by Layer 2 Tunneling

Protocol (L2TP) and IPSec.

QUESTION 4

Before you deploy Network Access Protection (NAP), you must install:

A. Internet Information Server (IIS)

B. Network Policy Server (NPS)

C. Active Directory Federation Services

D. Windows Update Service

Correct Answer: B

Reference: http://technet.microsoft.com/en-us/library/bb681008.aspx

QUESTION 5

Mark works as a Desktop Administrator for TechMart Inc. The company has a Windows-based network. He has bees assigned a project to upgrade the browsers to Internet Explorer (IE) 8 for working with the latest Internet technologies Mark wants to ensure that the company uses a number of the security features built into the browser while maintaining functionality within the company\\'s intranet. Mark is also educating his users to be good Internet citizens and use the safe web sur?ng. Mark asked his team to be assured that they are on a secured website. What they will do?

A. Take a look for a padlock in the lower right corner of the browser and https:// in the address bar.

B. Provide protection against a Distributed Denial of Services attack.

C. Call a team member while behaving to be someone else for gaining access to sensitive information.

D. Go into the Internet Options, select the Security, and add the intranet site to the list of Local Intranet Site.

Correct Answer: A

To be sure that the team members are on a secure site, they are required to look for a padlock in the lower right corner of the browser and https:// in the address bar. It will not guarantee that the site is secure but can be used. Answer: D is incorrect. The Internet zone feature in IE 8 can be configured and users are enabled to easily browse the local intranet without disturbing the security levels by using the following steps: 1.Go into the Internet Options and select the Security. 2.Add the intranet site to the list of Local Intranet Site. Answer: C is incorrect. 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 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.