GNSA Q&As

GIAC Systems and Network Auditor

Pass GIAC GNSA Exam with 100% Guarantee

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

https://www.passapply.com/gnsa.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following techniques can be used to determine the network ranges of any network?

A. Whois query

B. SQL injection

C. Snooping

D. Web ripping

Correct Answer: A

Whois queries are used to determine the IP address ranges associated with clients. A whois query can be run on most UNIX environments. In a Windows environment, the tools such as WsPingPro and Sam Spade can be used to perform

whois queries. Whois queries can also be executed over the Web from www.arin.net and www.networksolutions.com.

Answer: B is incorrect. A SQL injection attack is a process in which an attacker tries to execute unauthorized SQL statements. These statements can be used to delete data from a database, delete database objects such as tables, views,

stored procedures, etc. An attacker can either directly enter the code into input variables or insert malicious code in strings that can be stored in a database. For example, the following line of code illustrates one form of SQL injection attack:

query = "SELECT * FROM users WHERE name = \\'" + userName + "\\';"

This SQL code is designed to fetch the records of any specified username from its table of users. However, if the "userName" variable is crafted in a specific way by a malicious hacker, the SQL statement maydo more than the code author

intended. For example, if the attacker puts the "userName" value as \\' or \\'\\'=\\', the SQL statement will now be as follows:

SELECT * FROM users WHERE name = \\'\\' OR \\'\\'=\\'\\';

Answer: D is incorrect. Web ripping is a technique in which the attacker copies the whole structure of a Web site to the local disk and obtains all files of the Web site. Web ripping helps an attacker to trace the loopholes of the Web site.

Answer: C is incorrect. Snooping is an activity of observing the content that appears on a computer monitor or watching what a user is typing. Snooping also occurs by using software programs to remotely monitor activity on a computer or

network device. Hackers or attackers use snooping techniques and equipment such as keyloggers to monitor keystrokes, capture passwords and login information, and to intercept e-mail and other private communications. Sometimes,

organizations also snoop their employees legitimately to monitor their use of organizations\\' computers and track Internet usage.

QUESTION 2

Which of the following statements is true about a relational database?

A. It is difficult to extend a relational database.

B. The standard user and application program interface to a relational database is Programming Language (PL).

C. It is a collection of data items organized as a set of formally-described tables.

D. It is a set of tables containing data fitted into runtime defined categories.

Correct Answer: C

A relational database is a collection of data items organized as a set of formally-described tables from which data can be accessed or reassembled in many different ways without having to reorganize the database tables. Answer: B is incorrect. The standard user and application program interface to a relational database is the structured query language (SQL). Answer: A is incorrect. In addition to being relatively easy to create and access, a relational database has the important advantage of being easy to extend. Answer: D is incorrect. A relational database is a set of tables containing data fitted into predefined categories. Each table (which is sometimes called a relation) contains one or more data categories in columns. Each row contains a unique instance of data for the categories defined by the columns.

QUESTION 3

John works as a Network Auditor for XYZ CORP. The company has a Windows-based network. John wants to conduct risk analysis for the company.

Which of the following can be the purpose of this analysis? (Choose three)

A. To ensure absolute safety during the audit

B. To analyze exposure to risk in order to support better decision-making and proper management of those risks

C. To try to quantify the possible impact or loss of a threat

D. To assist the auditor in identifying the risks and threats

Correct Answer: BCD

There are many purposes of conducting risk analysis, which are as follows: To try to quantify the possible impact or loss of a threat To analyze exposure to risk in order to support better decision-making and proper management of those risks To support risk-based audit decisions To assist the auditor in determining the audit objectives To assist the auditor in identifying the risks and threats Answer: A is incorrect. The analysis of risk does not ensure absolute safety. The main purpose of using a risk-based audit strategy is to ensure that the audit adds value with meaningful information.

QUESTION 4

HOTSPOT

You work as a Network Administrator of a Windows 2000 Active Directory-based single domain network. You have configured your Windows XP Professional computer at home to have a static IP address assigned by your Internet service

provider (ISP). It is always connected to the Internet through a modem. You have enabled the Internet Connection Firewall for the Internet connection. You use the PING command to check the connectivity of your home computer from

office,

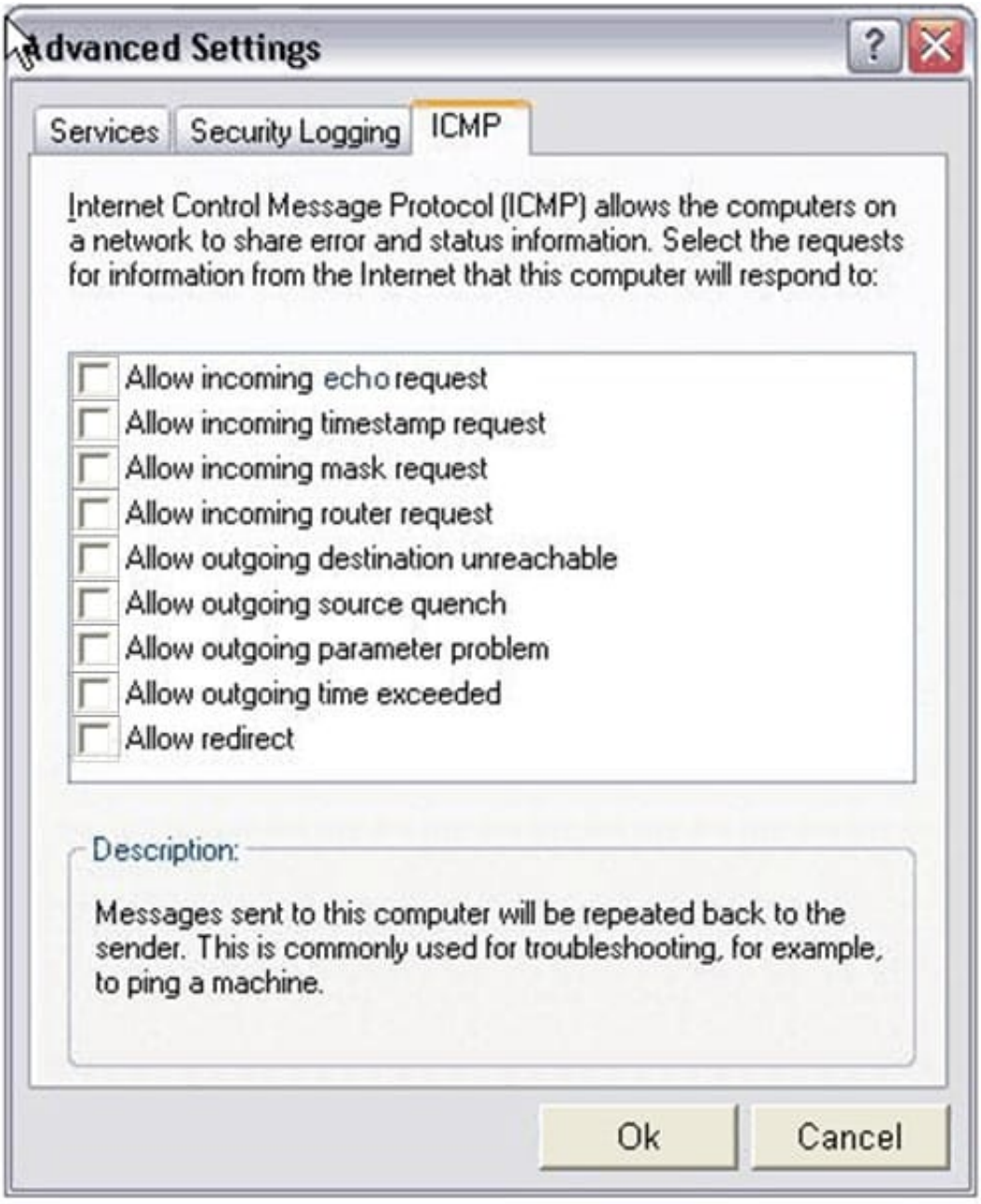
but you receive the following error message:

Request timed out.

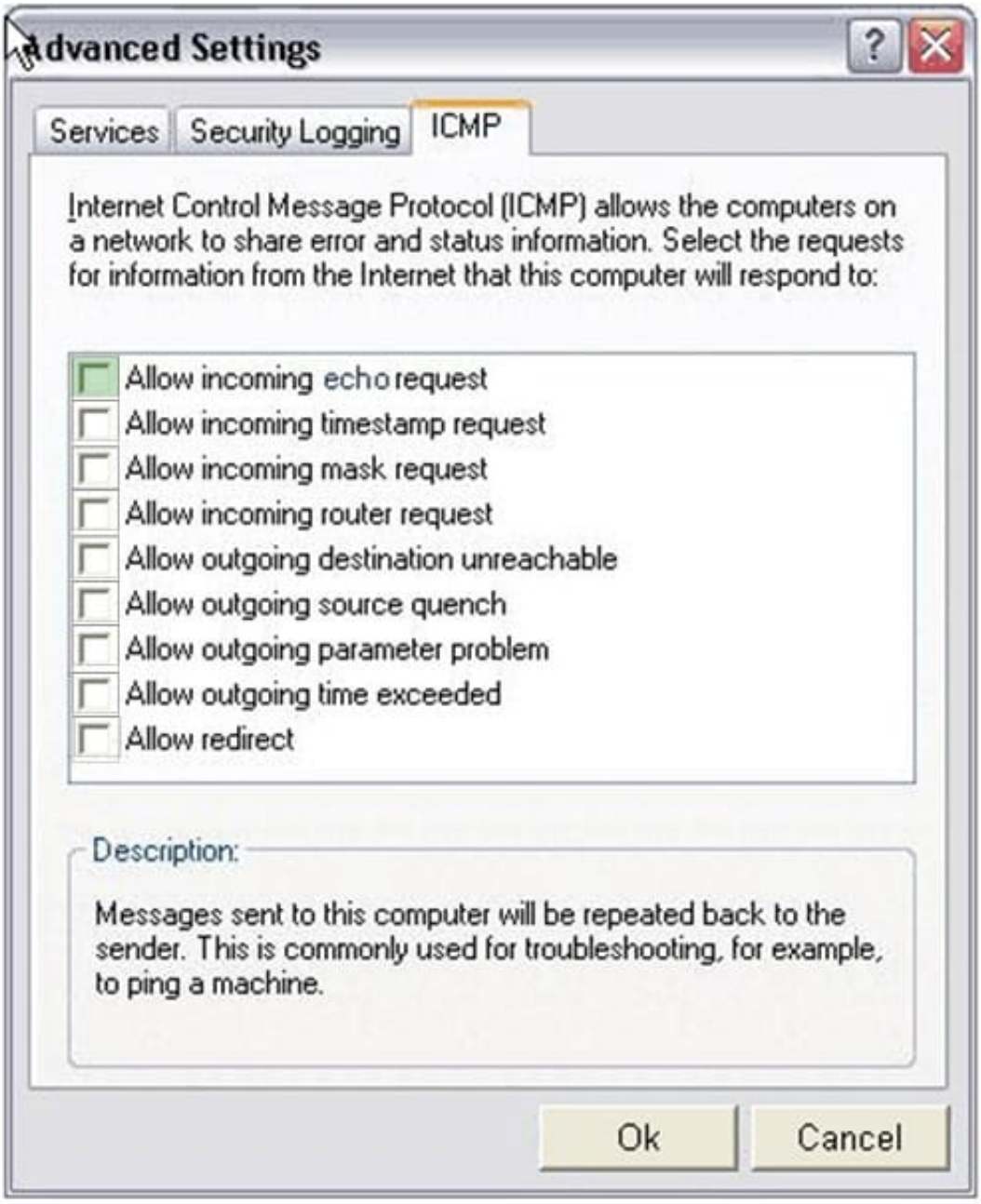
On examining the log file of the Internet Connection Firewall on your home computer, you find DROP ICMP messages. You want to ping your home computer without compromising on security.

Select the option in the Internet Connection Firewall Advanced Settings dialog box, which will be required to be checked to accomplish the task.

Hot Area:



Correct Answer:



The Internet Connection Firewall setting on your home computer is preventing PING from echoing messages. Selecting the Allow incoming echo request check box on the ICMP tab of the Internet Connection Firewall Advanced Settings dialog box will enable your computer to echo messages back to the sender.

QUESTION 5

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He successfully performs a brute force attack on the We-are-secure server. Now, he suggests some countermeasures to avoid such brute force attacks on the We-are-secure server.

Which of the following are countermeasures against a brute force attack?

A. The site should use CAPTCHA after a specific number of failed login attempts.

B. The site should increase the encryption key length of the password.

C. The site should restrict the number of login attempts to only three times.

D. The site should force its users to change their passwords from time to time.

Correct Answer: AC

Using CAPTCHA or restricting the number of login attempts are good countermeasures against a brute force attack.

Latest GNSA Dumps GNSA PDF Dumps GNSA Exam Questions