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.leads4pass.com/gnsa.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following statements are true about WPA?

A. WPA-PSK requires a user to enter an 8-character to 63-character passphrase into a wireless client.

B. Shared-key WPA is vulnerable to password cracking attacks if a weak passphrase is used.

C. WPA-PSK converts the passphrase into a 256-bit key.

D. WPA provides better security than WEP.

Correct Answer: ABCD

WPA stands for Wi-Fi Protected Access. It is a wireless security standard. It provides better security than WEP (Wired Equivalent Protection). Windows Vista supports both WPA-PSK and WPA-EAP. Each of these is described as follows:

WPA-PSK: PSK stands for Preshared key. This standard is meant for home environment. WPA-PSK requires a user to enter an 8- character to 63-character passphrase into a wireless client. The WPA converts the passphrase into a 256-bit

key.

WPA-EAP: EAP stands for Extensible Authentication Protocol. This standard relies on a back-end server that runs Remote AuthenticationDial-In User Service for user authentication. Note: Windows Vista supports a user to use a smart card

to connect to a WPA-EAP protected network.

Shared-key WPA is vulnerable to password cracking attacks if a weak passphrase is used. To protect against a brute force attack, a truly random passphrase of 13 characters (selected from the set of 95 permitted characters) is probably

sufficient.

QUESTION 2

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to identify the secure terminals from where the root can be allowed to log in.

Which of the following Unix configuration files can you use to accomplish the task?

A. /etc/services

B. /etc/ioports

C. /proc/interrupts

D. /etc/securetty

Correct Answer: D

In Unix, the /etc/securetty file is used to identify the secure terminals from where the root can be allowed to log in.

Answer: B is incorrect. In Unix, the /etc/ioports fileshows which I/O ports are in use at the moment.

Answer: A is incorrect. In Unix, the /etc/services file is the configuration file that lists the network services that the system supports. Answer: C is incorrect. In Unix, the /proc/interrupts file is the configuration file that shows the interrupts in use

and how many of each there has been.

QUESTION 3

You are concerned about possible hackers doing penetration testing on your network as a prelude to an attack. What would be most helpful to you in finding out if this is occurring?

A. Examining your antivirus logs

B. Examining your domain controller server logs

C. Examining your firewall logs

D. Examining your DNS Server logs

Correct Answer: C

Firewall logs will show all incoming and outgoing traffic. By examining those logs, you can do port scans and use other penetration testing tools that have been used on your firewall.

QUESTION 4

Which of the following commands can be used to intercept and log the Linux kernel messages?

A. syslogd

B. klogd

C. sysklogd

D. syslog-ng

Correct Answer: BC

The klogd and sysklogd commands can be used to intercept and log the Linux kernel messages.

QUESTION 5

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.