GSNA Q&As

GIAC Systems and Network Auditor

Pass GIAC GSNA Exam with 100% Guarantee

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

https://www.pass4itsure.com/gsna.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 tools can be used to perform tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing?

A. L0phtcrack

B. Obiwan

C. Cain

D. John the Ripper

Correct Answer: C

Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks:

1.

Dictionary attack

2.

Bruteforce attack

3.

Rainbow attack

4.

Hybrid attack Answer: A is incorrect. L0phtcrack is a tool which identifies and remediate security vulnerabilities that result from the use of weak or easily guessed passwords. It recovers Windows and Unix account passwords to access user and administrator accounts. Answer: D is incorrect. John the Ripper is a fast password cracking tool that is available for most versions of UNIX, Windows, DOS, BeOS, and Open VMS. It also supports Kerberos, AFS, and Windows NT/2000/ XP/2003 LM hashes. John the Ripper requires a user to have a copy of the password file. Answer: B is incorrect. Obiwan is a Web password cracking tool that is used to perform brute force and hybrid attacks. It is effective against HTTP connections for Web servers that allow unlimited failed login attempts by the user. Obiwan uses wordlists as well as alphanumeric characters as possible passwords.

QUESTION 2

You work as a Network Administrator for XYZ CORP. The company has a Windows-based network. You want to configure the ACL with a Cisco router.

Which of the following router prompts can you use to accomplish the task?

A. router(config-if)#

B. router(config)#

C. router(config-ext-nacl)#

D. router#

Correct Answer: C

The auditor of a Cisco router should be familiar with the variety of privilege modes. The current privilege mode can be quickly identified by looking at the current router prompt. The prime modes of a Cisco router are as follows:

1.

#Nonprivileged mode: router>

2.

#Priviledged mode: router#

3.

#Global configuration mode: router(config)#

4.

#Interface configuration mode: router(config-if)#

5.

#ACL configuration mode: router(config-ext-nacl)#

6.

#Boot loader mode: router(boot)

7.

#Remote connectivity config mode: router(config-line)#

QUESTION 3

The employees of CCN Inc. require remote access to the company\\'s proxy servers. In order to provide solid wireless security, the company uses LEAP as the authentication protocol.

Which of the following is supported by the LEAP protocol?

A. Dynamic key encryption

B. Public key certificate for server authentication

C. Strongest security level

D. Password hash for client authentication

Correct Answer: AD

LEAP can use only password hash as the authentication technique. Not only LEAP, but EAP-TLS, EAP- TTLS, and

PEAP also support dynamic key encryption and mutual authentication. Answer: C is incorrect. LEAP provides only a moderate level of security. Answer: B is incorrect. LEAP uses password hash for server authentication.

QUESTION 4

A Cisco router can have multiple connections to networks. These connections are known as interfaces for Cisco Routers. For naming each interface, Cisco generally uses the type of interface as part of the name.

Which of the following are true about the naming conventions of Cisco Router interfaces?

A. An interface connected to a serial connection always starts with an S.

B. An interface connected to a Token Ring segment always starts with To.

C. An Ethernet interface that is fast always starts with an F.

D. An interface connected to an Ethernet segment of the network always starts with an En.

Correct Answer: ABC

A Cisco router can have multiple connections to networks. These connections are known as interfaces for Cisco Routers. For naming each interface, Cisco generally uses the type of interface as part of the name. Following are some of the naming conventions of Cisco Router interfaces:

1.

An Ethernet interface that is fast always starts with an F.

2.

An interface connected to a serial connection always starts with an S.

3.

An interface connected to an Ethernet segment of the network always starts with an E.

4.

An interface connected to a Token Ring segment always starts with To.

QUESTION 5

An auditor assesses the database environment before beginning the audit. This includes various key tasks that should be performed by an auditor to identify and prioritize the users, data, activities, and applications to be monitored.

Which of the following tasks need to be performed by the auditor manually?

A. Classifying data risk within the database systems

B. Monitoring data changes and modifications to the database structure, permission and user changes, and data viewing activities

C. Analyzing access authority

D. Archiving, analyzing, reviewing, and reporting of audit information

Correct Answer: AC

The Internal Audit Association lists the following as key components of a database audit:

Create an inventory of all database systems and use classifications. This should include production and test data. Keep it up-to-date.

Classify data risk within the database systems. Monitoring should be prioritized for high, medium, and low risk data.

Implement an access request process that requires database owners to authorize the "roles" granted to database accounts (roles as in Role Based Access and not the native database roles). Analyze access authority. Users with higher

degrees of access permission should be under higher scrutiny, and any account for which access has been suspended should be monitored to ensure access is denied, attempts are identified.

Assess application coverage. Determine what applications have built-in controls, and prioritize database auditing accordingly. All privileged user access must have audit priority. Legacy and custom applications are the next highest priority to

consider, followed by the packaged applications. Ensure technical safeguards. Make sure access controls are set properly. Audit the activities. Monitor data changes and modifications to the database structure, permission and user changes,

and data viewing activities. Consider using network-based database activity monitoring appliances instead of native database audit trails.

Archive, analyze, review, and report audit information. Reports to auditors and IT managers must communicate relevant audit information, which can be analyzed and reviewed to determine if corrective action is required. Organizations that

must retain audit data for long-term use should archive this information with the ability to retrieve relevant data when needed.

The first five steps listed are to be performed by the auditor manually. Answers B, D are incorrect. These tasks are best achieved by using an automated solution.