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

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

QUESTION 1

Which of the following responsibilities does not come under the audit process?

A. Reporting all facts and circumstances of their regular and illegal acts.

B. Planning the IT audit engagement based on the assessed level of risk.

C. Reviewing the results of the audit procedures.

D. Applying security policies.

Correct Answer: ABC

According to the standards of ISACA, an auditor should hold the following responsibilities: Planning the IT audit engagement based on an assessed level of risk. Designing audit procedures of irregular and illegal acts. Reviewing the results of

the audit procedures. Assuming that acts are not isolated. Determining why the internal control system failed for that act. Conducting additional audit procedures. Evaluating the results of the expanded audit procedures. Reporting all facts and

circumstances of the irregular and illegal acts. Distributing the report to the appropriate internal parties, such as managers.

Answer: D is incorrect. The auditor is not responsible for applying security policies.

QUESTION 2

Zorp is a proxy firewall suite developed by Balabit IT Security.

Which of the following statements are true about Zorp?

A. It allows the administrators to fine-tune proxy decisions.

B. Zorp aims for compliance with the Common Criteria/Application Level Firewall Protection Profile for Medium Robustness.

C. It allows full analysis of embedded protocols.

D. The GPL versionof Zorp lacks much of the usability and functions from the other versions.

Correct Answer: ABC

Zorp is a proxy firewall suite developed by Balabit IT Security. Its core framework allows the administrator to fine-tune proxy decisions (with its built-in script language), and fully analyze embedded protocols (such as SSL with an embedded POP3 or HTTP protocol). The FTP, HTTP, FINGER, WHOIS, TELNET, and SSL protocols are fully supported with an application-level gateway. Zorp aims for compliance with the Common Criteria/Application Level Firewall Protection Profile for Medium Robustness. Zorp is released under GNU/GPL and commercial license too. The GPL version is completely usable and functional; however, it lacks some of the more advanced functions available in the commercially available version only. Some of the Zorp supported protocols are Finger, Ftp, Http, Pop3, NNTP, IMAP4, RDP, RPC, SIP, SSL, SSH, Telnet, Whois, LDAP, RADIUS, TFtp, SQLNet NET8, Rsh, etc. Answer: D is incorrect. The GPL version of Zorp is completely usable and functional; however, it lacks some of the more advanced functions

available in the commercially available version only.

QUESTION 3

Which of the following Web authentication techniques uses a single sign-on scheme?

A. NTLMauthentication

B. Digest authentication

C. Microsoft Passport authentication

D. Basic authentication

Correct Answer: C

Microsoft Passport authentication is based on single sign-on authentication in which a user needs to remember only one username and password to be authenticated for multiple services. The Passport is a suite of services for authenticating users across a number of applications. The Passport single sign-on service is an authentication service allowing users to create a single set of credentials that will enable them to sign in to any participating site that supports the Passport service. It enables the use of one set of credentials to access any Passport-enabled site such as MSN, Hotmail, and MSN Messenger.

QUESTION 4

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using the Linux operating system. He wants to use a wireless sniffer to sniff the We-are-secure network.

Which of the following tools will he use to accomplish his task?

A. WEPCrack

B. Kismet

C. Snadboy\\'s Revelation

D. NetStumbler

Correct Answer: B

According to the scenario, John will use Kismet. Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card that supports raw monitoring (rfmon) mode. Kismet can sniff 802.11b,

802.11a, 802.11g, and802.11n traffic. Kismet can be used for the following tasks:

To identify networks by passively collecting packets

To detect standard named networks

To detect masked networks

To collect the presence of non-beaconing networks via data traffic

Answer: D is incorrect. NetStumbler is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. It detects wireless networks and marks their relative position with a GPS.

Answer: A is incorrect. WEPCrack is an open source tool that breaks IEEE 802.11 WEP secret keys.

Answer: C is incorrect. Snadboy\\'s Revelation is not a sniffer. It is used to see the actual password behind the asterisks.

QUESTION 5

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. John is working as a root user on the Linux operating system. He has recently backed up his entire Linux hard drive into the my_backup.tgz file. The size of the my_backup.tgz file is 800MB. Now, he wants to break this file into two files in which the size of the first file named my_backup.tgz.aa should be 600MB and that of the second file named my_backup.tgz.ab should be 200MB.

Which of the following commands will John use to accomplish his task?

A. split --verbose -b 200m my_backup.tgz my_backup.tgz

B. split --verbose -b 200m my_backup.tgz my_backup.tgz

C. split --verbose -b 600m my_backup.tgz my_backup.tgz

D. split --verbose -b 600m my_backup.tgz my_backup.tgz

Correct Answer: D

According to the scenario, John wants to break the my_backup.tgz file into two files in which thesize of the first file named my_backup.tgz.aa should be 600MB and that of the second file named my_backup.tgz.ab should be 200MB. Hence,

he will use the the split --verbose -b 600 my_backup.tgz my_backup.tgz. command, which will automatically break the first file into 600MB named my_backup.tgz.aa, and the rest of the data (200MB) will be assigned to the second file named

my_backup.tgz.ab. The reason behind the names is that the split command provides suffixes as \\'aa\\', \\'ab\\', \\'ac\\', ..., \\'az\\', \\'ba\\', \\'bb\\', etc. in the broken file names by default. Hence, both conditions, the file names as well as the file sizes, match with

this command.

Note: If the size of the tar file my_backup.tgz is 1300MB, the command split --verbose -b 600 my_backup.tgz my_backup.tgz. breaks the my_backup.tgz file into three files,i.e., my_backup.tgz.aa of size 600MB, my_backup.tgz.ab of size

600MB, and my_backup.tgz.ac of size 100MB.

Latest GNSA Dumps GNSA VCE Dumps GNSA Exam Questions