VCE & PDF
GeekCert.com

GSNA^{Q&As}

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.geekcert.com/gsna.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

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:

1.

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

2.

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

3.

 To support risk-based audit decisions

4.

 To assist the auditor in determining the audit objectives

5.

 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 2

Anonymizers are the services that help make a user\\'s own Web surfing anonymous. An anonymizer removes all the identifying information from a user\\'s computer while the user surfs the Internet. It ensures the privacy of the user in this manner. After the user anonymizes a Web access with an anonymizer prefix, every subsequent link selected is also automatically accessed anonymously.

Which of the following are limitations of anonymizers?

A. ActiveX controls

B. Plugins

C. Secure protocols

D. Java applications

E. JavaScript

Correct Answer:

QUESTION 3

In the DNS Zone transfer enumeration, an attacker attempts to retrieve a copy of the entire zone file for a domain from a DNS server. The information provided by the DNS zone can help an attacker gather user names, passwords, and other valuable information. To attempt a zone transfer, an attacker must be connected to a DNS server that is the authoritative server for that zone. Besides this, an attacker can launch a Denial of Service attack against the zone\\'s DNS servers by flooding them with a lot of requests.

Which of the following tools can an attacker use to perform a DNS zone transfer?

A. DSniff

B. Dig

C. Host

D. NSLookup

Correct Answer: BCD

An attacker can use Host, Dig, and NSLookup to perform a DNS zone transfer. Answer: A is incorrect. DSniff is a sniffer that can be used to record network traffic. Dsniff is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of the tools of Dsniff include dsniff, arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. Dsniff is highly effective for sniffing both switched and shared networks. It uses the arpredirect and macof tools for switching across switched networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, etc.

QUESTION 4

Which of the following statements about Secure Sockets Layer (SSL) are true? (Choose two)

A. It provides connectivity between Web browser and Web server.

B. It provides mail transfer service.

C. It provides communication privacy, authentication, and message integrity.

D. It uses a combination of public key and symmetric encryption for security of data.

Correct Answer: CD

Secure Sockets Layer (SSL) is a protocol used to transmit private documents via the Internet. SSL uses a combination of public key and symmetric encryption to provide communication privacy, authentication, and message integrity. Using the SSL protocol, clients and servers can communicate in a way that prevents eavesdropping and tampering of data on the Internet. Many Web sites use the SSL protocol to obtain confidential user information, such as credit card numbers.

By convention, URLs that require an SSL connection start with https: instead of http:. By default, SSL uses port 443 for secured communication. For a SSL connection between a Web browser and Web server, you must enter https, for example, "https:// www.vzen.com", instead of http as the protocol type in the URL. This will instruct the Web browser to use a different port for communication. SSL uses TCP port 443 for communication.

QUESTION 5

You have an online video library. You want to upload a directory of movies. Since this process will take several hours, you want to ensure that the process continues even after the terminal is shut down or session is closed.

What will you do to accomplish the task?

A. Use the bg command to run the process at the background.

B. Add the nohup command in front of the process.

C. Add the nohup command at the end of the process.

D. Run the process inside a GNU Screen-style screen multiplexer.

Correct Answer: BD

Whenever the nohup command is added in front of any command or process, it makes the command or process run even after the terminal is shut down or session is closed. All processes, except the \\'at\\' and batch requests, are killed when a

user logs out. If a user wants a background process to continue running even after he logs out, he must use the nohup command to submit that background command. To nohup running processes, press ctrl+z, enter "bg" and enter "disown".

The other way to accomplish the task is to run the command/process inside a GNU Screen-style screen multiplexer, and then detach the screen. GNU Screen maintains the illusion that the user is always logged in, and allows the user to

reattach at any time. This has the advantage of being able to continue to interact with the program once reattached (which is impossible with nohup alone).

Answer: C is incorrect. The nohup command works when it is added in front of a command. Answer: A is incorrect. The bg command cannot run the command or process after the terminal is shut down or session is closed.