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

Peter works as a Web Developer for XYZ CORP. He is developing a Web site for the company. Peter specifies MARGINHEIGHT="0" and MARGINWIDTH="0" in one of the Web pages.

How will this affect the Web page?

A. It will create a borderless page structure when viewed in any browser.

B. It will create a borderless page structure when viewed in Netscape Navigator.

C. It will delete all the text from the margins.

D. It will create a borderless page structure when viewed in Internet Explorer.

Correct Answer: B

The MARGINHEIGHT and MARGINWIDTH attributes are used in the tag to adjust the top and left margins of a Web page to be displayed in Netscape Navigator. Specifying MARGINHEIGHT="0" and MARGINWIDTH="0" within the

tag will create a borderless page structure when viewed in Netscape Navigator.

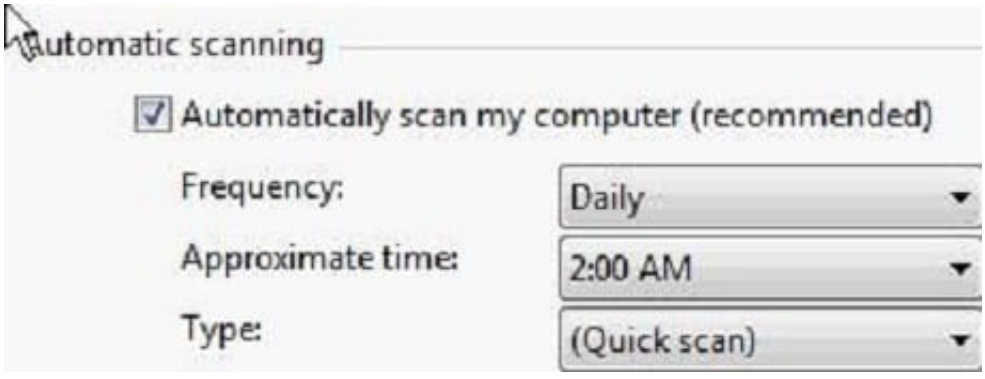
Answer: D is incorrect. The TOPMARGIN and LEFTMARGIN attributes are used in the tag to adjust the top and left margins of a Web page to be displayed in Internet Explorer. Specifying TOPMARGIN="0" and LEFTMARGIN="0"

within the tag will create a borderless page structure when viewed in Internet Explorer.

Answer C is incorrect. These attributes are used to adjust margins and not to delete text from margins.

QUESTION 2

You have purchased a laptop that runs Windows Vista Home Premium. You want to protect your computer from malicious applications, such as spyware, while connecting to the Internet. You configure Windows Defender on your laptop to schedule scan daily at 2 AM as shown in the image below:



You want Windows Defender to scan the laptop for all the known spyware and other potentially unwanted software, including the latest one. You do not want to manually perform this task.

Which of the following actions will you perform to accomplish the task?

A. Create a scheduled task to download definition files for Windows Defender every Sunday.

B. Configure Windows Defender to use the definition file placed on the Microsoft Update site for scanning the laptop.

C. Select the Check for updated definitions before scanning check box in the Automatic Scanning section.

D. Click the arrow beside the Help button Click the Check for updates option.

Correct Answer: C

According to the question, Windows Defender should scan the laptop for all the known spyware and other potentially unwanted software, including the latest one. Windows Defender uses definitions to scan the system. Definitions are files that include the information of known spyware and potentially unwanted software. To scan a computer for the latest spyware, Windows Defender requires the latest definition files available on the Internet. For this, you have to configure Windows Defender to check for the latest definitions and download them, if available, before scanning the computer. Furthermore, the question also states that the task must be performed automatically. In order to accomplish the task, you will have to select the Check for updated definitions before scanning check box in the Automatic Scanning section.

QUESTION 3

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He copies the whole structure of the We-are-secure Web site to the local disk and obtains all the files on the Web site.

Which of the following techniques is he using to accomplish his task?

A. Eavesdropping

B. Fingerprinting

C. Web ripping

D. TCP FTP proxy scanning

Correct Answer: C

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: A is incorrect. Eavesdropping is the intentional interception of data (such as e-mail, username, password, credit card, or calling card number) as it passes from a user\\'s computer to a server, or vice versa. There are high-tech methods of eavesdropping. It has been demonstrated that a laser can be bounced off a window and vibrations caused by the sounds inside the building can be collected and turned back into those sounds. The cost of high-tech surveillance has made such instruments available only to the professional information gatherer, however. But as with all high-tech electronics, falling prices are making these more affordable to a wider audience. Answer: D is incorrect. In TCP FTP proxy (bounce attack) scanning, a scanner connects to an FTP server and requests it to start data transfer to a third system. The scanner uses the PORT FTP command to find out whether or not the data transfer process is listening to the target system at a certain port number. It then uses the LIST FTP command to list the current directory, and the result is sent over the server. If the data transfer is successful, it clearly indicates that the port is open. If the port is closed, the attacker receives the connection refused ICMP error message. Answer: B is incorrect. Fingerprinting is the easiest way to detect the Operating System (OS)of a remote system. OS detection is important because, after knowing the target system\\'s OS, it becomes easier to hack into the system. The comparison of data packets that are sent by the target system is done by fingerprinting. The analysis of data packets gives the attacker a hint as to which operating system is being used by the remote system. There are two types of fingerprinting techniques as follows: Active fingerprinting 2.Passive fingerprinting

In active fingerprinting ICMP messages are sent to the target system and the response message of the target system shows which OS is being used by the remote system. In passive fingerprinting the number of hops reveals the OS of the remote system.

QUESTION 4

Which of the following NFS mount options specifies whether a program using a file via an NFS connection should stop and wait for the server to come back online, if the host serving the exported file system is unavailable, or if it should report an error?

A. intr

B. hard or soft

C. nfsvers=2 or nfsvers=3

D. fsid=num

Correct Answer: B

The hard or soft NFS mount options are used to specify whether a program using a file via an NFS connection should stop and wait (hard) for the server to come back online, if the host serving the exported file system is unavailable, or if it

should report an error.

Answer: A is incorrect. The intr NFS mount option allows NFS requests to be interrupted if the server goes down or cannot be reached. Answer: C is incorrect. The nfsvers=2 or nfsvers=3 NFS mount options are used to specify which version

of the NFS protocol to use. Answer: D is incorrect. The fsid=num NFS mount option forces the file handle and file attributes settings on the wire to be num.

QUESTION 5

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

Which of the following IEEE-based traffic can be sniffed with Kismet?

A. 802.11g

B. 802.11n

C. 802.11b

D. 802.11a

Correct Answer: ABCD

Kismet can sniff IEEE 802.11a, 802.11b, 802.11g, and 802.11n-based wireless network traffic.

Latest GNSA Dumps GNSA Practice Test GNSA Exam Questions