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.certbus.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 statements is NOT true about FAT16 file system?

A. FAT16 file system works well with large disks because the cluster size increases as the disk partition size increases.

B. FAT16 file system supports file-level compression.

C. FAT16 does not support file-level security.

D. FAT16 file system supports Linux operating system.

Correct Answer: AB

FAT16 file system was developed for disks larger than 16MB. It uses 16-bit allocation table entries. FAT16 file system supports all Microsoft operating systems. It also supports OS/2 and Linux. Answer: C, D are incorrect. All these statements are true about FAT16 file system.

QUESTION 2

You work as a professional Ethical Hacker. You are assigned a project to perform blackbox testing of the security of www.we-are-secure.com. Now you want to perform banner grabbing to retrieve information about the Webserver being used by we-are-secure.

Which of the following tools can you use to accomplish the task?

A. Wget

B. WinSSLMiM

C. Whisker

D. httprint

Correct Answer: D

According to the scenario, you want to perform banner grabbing to retrieve information about the Webserver being used by we-are-secure. For this, you will use the httprint tool to accomplish the task. httprint is a fingerprinting tool that is based on Web server characteristics to accurately identify Web servers. It works even when Web server may have been obfuscated by changing the server banner strings, or by plug-ins such as mod_security or servermask. It can also be used to detect Web enabled devices that do not contain a server banner string, such as wireless access points, routers, switches, cable modems, etc. httprint uses text signature strings for identification, and an attacker can also add signatures to the signature database. Answer: A is incorrect. Wget is a Website copier that is used to analyze the vulnerabilities of a Website offline. Answer: C is incorrect. Whisker is an HTTP/Web vulnerability scanner that is written in the PERL language. Whisker runs on both the Windows and UNIX environments. It provides functions for testing HTTP servers for many known security holes, particularly the presence of dangerous CGIs. Answer: B is incorrect. WinSSLMiM is an HTTPS Man in the Middle attacking tool. It includes FakeCert, a tool used to make fake certificates. It can be used to exploit the Certificate Chain vulnerability in Internet Explorer.

QUESTION 3

You have been assigned a project to develop a Web site for a construction company. You have to develop a Web site and want to get more control over the appearance and presentation of your Web pages. You also want to increase the ability to precisely specify the location and appearance of the elements on a page and create special effects. You plan to use Cascading style sheets (CSS). You want to apply the same style consistently throughout your Web site.

Which type of style sheet will you use?

A. Internal Style Sheet

B. External Style Sheet

C. Inline Style Sheet

D. Embedded Style Sheet

Correct Answer: B

To apply the same style consistently throughout your Web site you should use external style sheet. Cascading style sheets (CSS) are used so that the Web site authors can exercise greater control on the appearance and presentation of their

Web pages. And also because they increase the ability to precisely point to the location and look of elements on a Web page and help in creating special effects. Cascading Style Sheets have codes, which are interpreted and applied by the

browser on to the Web pages and their elements.

There are three types of cascading style sheets.

1.

External Style Sheets

2.

Embedded Style Sheets

3.

Inline Style Sheets External Style Sheets are used whenever consistency in style is required throughout a Web site. A typical external style sheet uses a .css file extension, which can be edited using a text editor such as a Notepad. Embedded Style Sheets are used for defining styles for an active page. Inline Style Sheets are used for defining individual elements of a page. Reference: TechNet, Contents: Microsoft Knowledgebase, February 2000 issue PSS ID Number: Q179628

QUESTION 4

Which of the following are the drawbacks of the NTLM Web authentication scheme?

A. The password is sent in hashed format to the Web server.

B. It works only with Microsoft Internet Explorer.

C. The password is sent in clear text format to the Web server.

D. It can be brute forced easily.

Correct Answer: BD

The following are the drawbacks of the NTLM Web Authentication Scheme:

1.

NTLM Web authentication is not entirely safe because NTLM hashes (or challenge/response pairs) can be cracked with the help of brute force password guessing. The "cracking" program would repeatedly try all possible passwords,

hashing each and comparing the result to the hash that the malicious user has obtained. When it discovers a match, the malicious user will know that the password that produced the hash is the user\\'s password.

2.

This authentication technique works only with Microsoft Internet Explorer. Answer: A, C are incorrect. NTLM authentication does not send the user\\'s password (or hashed representation of the password) across the network. Instead, NTLM

authentication utilizes challenge/ response mechanisms to ensure that the actual password never traverses the network. How does it work? When the authentication process begins, the client sends a login request to the telnet server. The

server replies with a randomly generated \\'token\\' to the client. The client hashes the currently logged-on user\\'s cryptographically protected password with the challenge and sends the resulting "response" to the server. The server receives the

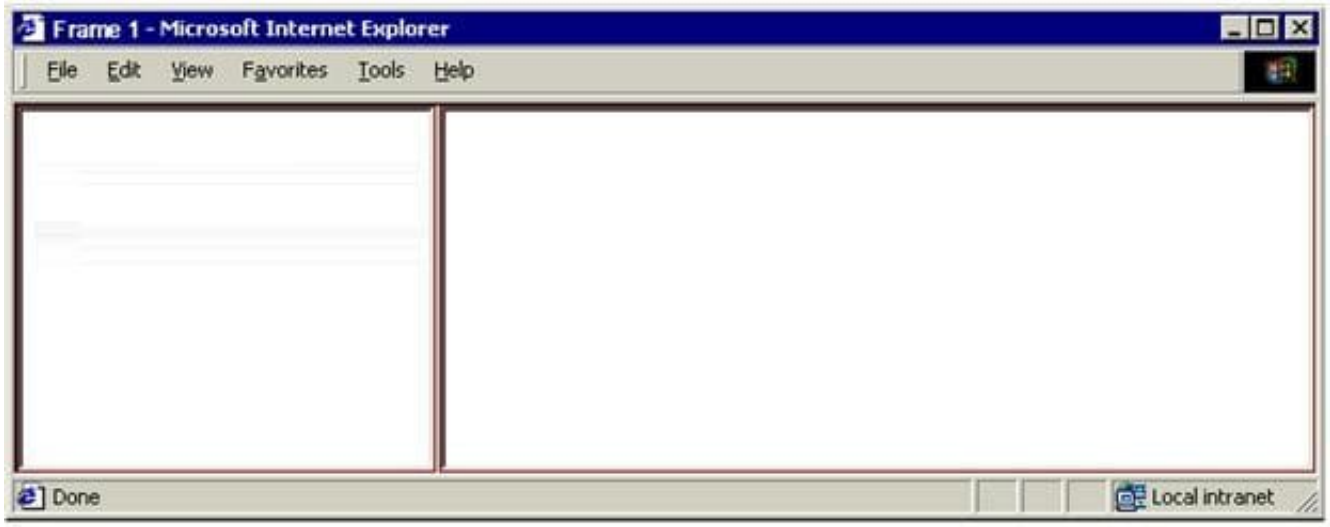
challenge-hashed response and compares it in the following manner:

The server takes a copy of the original token.

Now it hashes the token against the user\\'s password hash from its own user account database. If the received response matches the expected response, the user is successfully authenticated to the host.

QUESTION 5

Which of the following tags will create two vertical frames, as given in the image below, where the left frame is half as wide as the right one?



A.

B.

C.

D.

E.

Correct Answer: E

tag specifies a frameset used to organize multiple frames and nested framesets in an HTML document. It defines the location, size, and orientation of frames. An HTML document can either contain a tag or a

tag.

The COLS attribute of the tag defines the width of the vertical frames. The ROWS attribute defines the height of the horizontal frames. The code in answer option E will create two identical frames. The left frame will be half as

wide as the right frame because of the relative size attributes given in the tag, i.e., .

QUESTION 6

In a network, a data packet is received by a router for transmitting it to another network. In order to make decisions on where the data packet should be forwarded, the router checks with its routing table.

Which of the following lists does a router check in a routing table?

A. Available networks

B. Available packets

C. Available protocols

D. Available paths

Correct Answer: AD

A Routing table stores the actual routes to all destinations; the routing table is populated from the topology table with every destination network that has its successor and optionally feasible successor identified (if unequal-cost load-balancing

is enabled using the variance command). The successors and feasible successors serve as the next hop routers for these destinations. Unlike most other distance vector protocols, EIGRP does not rely on periodic route dumps in order to

maintain its topology table. Routing information is exchanged only upon the establishment of new neighbor adjacencies, after which only changes are sent.

Answer: C is incorrect. A routing table does not contain any list of protocols. Answer: B is incorrect. A routing table does not contain any list of packets.

QUESTION 7

You check performance logs and note that there has been a recent dramatic increase in the amount of broadcast traffic.

What is this most likely to be an indicator of?

A. Misconfigured router

B. DoS attack

C. Syn flood

D. Virus

Correct Answer: B

There are several denial of service (DoS) attacks that specifically use broadcast traffic to flood a targeted computer. Seeing an unexplained spike in broadcast traffic could be an indicator of an attempted denial of service attack.

Answer: D is incorrect. Viruses can cause an increase in network traffic, and it is possible for that to be broadcast traffic. However, a DoS attack is more likely than a virus to cause this particular problem. Answer: C is incorrect. A syn flood

does not cause increased broadcast traffic. Answer: A is incorrect. A misconfigured router could possibly cause an increase in broadcast traffic. However, this are cent problem, the router is unlikely to be the issue.

QUESTION 8

John works as a Security Professional. He is assigned a project to test the security of www.we-are- secure.com. John wants to get the information of all network connections and listening ports in the numerical form.

Which of the following commands will he use?

A. netstat -e

B. netstat ?

C. netstat -s

D. netstat ?n

Correct Answer: D

According to the scenario, John will use the netstat -an command to accomplish the task. The netstat -an command is used to get the information of all network connections and listening ports in the numerical form. The netstat command

displays protocol-related statistics and the state of current TCP/IP connections. It is used to get information about the open connections on a computer, incoming and outgoing data, as well as the ports of remote computers to which the

computer is connected. The netstat command gets all this networking information by reading the kernel routing tables in the memory. Answer: A is incorrect. The netstat -e command displays the Ethernet information. Answer: B is incorrect.

The netstat -r command displays the routing table information. Answer: C is incorrect. The netstat -s command displays per-protocol statistics.

By default, statistics are shown for TCP, UDP and IP.

QUESTION 9

Which of the following can be the countermeasures to prevent NetBIOS NULL session enumeration in Windows 2000 operating systems?

A. Denying all unauthorized inbound connections to TCP port 53

B. Disabling SMB services entirely on individual hosts by unbinding WINS Client TCP/IP from the interface

C. Editing the registry key HKLM\SYSTEM\CurrentControlSet\LSA and adding the value RestrictAnonymous

D. Disabling TCP port 139/445

Correct Answer: BCD

NetBIOS NULL session vulnerabilities are hard to prevent, especially if NetBIOS is needed as part of the infrastructure. One or more of the following steps can be taken to limit NetBIOS NULL session vulnerabilities: 1.Null sessions require access to the TCP 139 or TCP 445 port, which can be disabled by a Network Administrator.

2.

A Network Administrator can also disable SMB services entirely on individual hosts by unbinding WINS Client TCP/IP from the interface.

3.

A Network Administrator can also restrict the anonymous user by editing the registry values:

-a.Open regedit32, and go to HKLM\SYSTEM\CurrentControlSet\LSA.

-b.Choose edit > add value. Value name: RestrictAnonymous Data Type: REG_WORD Value: 2

Answer: A is incorrect. TCP port 53 is the default port for DNS zone transfer. Although disabling it can help restrict DNS zone transfer enumeration, it is not useful as a countermeasure against the NetBIOS NULL session enumeration.

QUESTION 10

Which of the following statements about system hardening are true? (Choose two)

A. It is used for securing the computer hardware.

B. It can be achieved by installing service packs and security updates on a regular basis.

C. It can be achieved by locking the computer room.

D. It is used for securing an operating system.

Correct Answer: BD

System hardening is a term used for securing an operating system. It can be achieved by installing the latest service packs, removing unused protocols and services, and limiting the number of users with administrative privileges.

QUESTION 11

You work as a Network Administrator of a TCP/IP network. You are having DNS resolution problem.

Which of the following utilities will you use to diagnose the problem?

A. PING

B. IPCONFIG

C. TRACERT

D. NSLOOKUP

Correct Answer: D

NSLOOKUP is a tool for diagnosing and troubleshooting Domain Name System (DNS) problems. It performs its function by sending queries to the DNS server and obtaining detailed responses at the command prompt. This information can be

useful for diagnosing and resolving name resolution issues, verifying whether or not the resource records are added or updated correctly in a zone, and debugging other server-related problems. This tool is installed along with the TCP/IP

protocol through the Control Panel.

Answer: A is incorrect. The ping command-line utility is used to test connectivity with a host on a TCP/IP- based network. This is achieved by sending out a series of packets to a specified destination host. On receiving the packets, the

destination host responds with a series of replies. These replies can be used to determine whether or not the network is working properly.

Answer: B is incorrect. IPCONFIG is a command-line utility used to display current TCP/IP network configuration values and update or release the Dynamic Host Configuration Protocol (DHCP) allocated leases. It is also used to display,

register, or flush Domain Name System (DNS) names. Answer: C is incorrect. TRACERT is a route-tracing Windows utility that displays the path an IP packet takes to reach the destination. It shows the Fully Qualified Domain Name (FQDN)

and the IP address of each gateway along the route to the remote host.

QUESTION 12

You work as the Network Administrator for XYZ CORP. The company has a Unix-based network. You want to set the hard disk geometry parameters, cylinders, heads, and sectors.

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

A. mke2fs

B. mkswap

C. mkfs

D. hdparm

Correct Answer: D

In Unix, the hdparm command is used to get or sethard disk geometry parameters, cylinders, heads, and sectors.

Answer: C is incorrect. In Unix, the mkfs command initializes a Unix filesystem. This is a front end that runs a separate program depending on the filesystem\\'s type.

Answer: A is incorrect. In Unix, the mke2fs command creates a Unix second extended filesystem. Answer: B is incorrect. In Unix, the mkswap command sets up a Unix swap area on a device or file.

QUESTION 13

You are the Security Administrator for an Internet Service Provider. From time to time your company gets subpoenas from attorneys and law enforcement for records of customers\\' access to the internet. What policies must you have in place to be prepared for such requests?

A. Group access policies

B. Backup policies

C. User access policies

D. Storage and retention policies

Correct Answer: D

Storage and retention policies will determine how long you keep records (such as records of customers Web activity), how you will store them, and how you will dispose of them. This will allow you to know what records you should still have on

hand should a legal request for such records come in. Answer: C is incorrect. User policies might determine what a customer has access to, but won\\'t help you identify what they actually did access.

Answer: A is incorrect. Group policies are usually pertinent to network administration, not the open and uncontrolled environment of an ISP.

Answer B is incorrect. Backup policies dictate how data is backed up and stored.

QUESTION 14

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 15

Which of the following applications work as mass-emailing worms? (Choose two.)

A. Chernobyl virus

B. I LOVE YOU virus

C. Nimda virus

D. Melissa virus

Correct Answer: BC

The Nimda and I LOVE YOU viruses work as mass-emailing worms.