GIAC

GSNA Exam

GIAC Systems and Network Auditor

[Questions & Answers Demo]

Question: 1

Sarah works as a Web Developer for BlueWell Inc. She is creating a Web site for her company. Sarah wants greater control over the appearance and presentation of Web pages. She wants the ability to precisely specify the display attributes and the appearance of elements on the Web pages. How will she accomplish this?

A. Use the Database Design wizard.
B. Make two templates, one for the index page and the other for all other pages.
C. Use Cascading Style Sheet (CSS).
D. Make a template and use it to create each Web page.

Answer: C

Explanation:
Sarah should use the Cascading Style Sheet (CSS) while creating Web pages. This will give her greater control over the appearance and
presentation of the Web pages and will also enable her to precisely specify the display attributes and the appearance of elements on the
Web pages.

Question: 2

You work as a Network Administrator for Net Perfect Inc. The company has a Windows Server 2008 network environment. The network is configured as a Windows Active Directory-based single forest single domain network. You have installed a Windows Server 2008 computer. You have configured auditing on this server. The client computers of the company use the Windows XP Professional operating system. You want to audit each event that is related to a user managing an account in the user database on the computer where the auditing is configured. To accomplish the task, you have enabled the Audit account management option on the server.
Which of the following events can be audited by enabling this audit option?
Each correct answer represents a complete solution. Choose all that apply.

A. Access to an Active Directory object
B. Change of password for a user account
C. Addition of a user account to a group
D. Creation of a user account

Answer: D, C, and B

Explanation:
Audit account management is one of the nine audit settings that can be configured on a Windows computer. This option is enabled to audit
each event that is related to a user managing an account in the user database on the computer where the auditing is configured. These

events include the following:
Creating a user account
Adding a user account to a group
Renaming a user account
Changing password for a user account
This option is also used to audit the changes to the domain account of the domain controllers.

Answer: A is incorrect. To monitor events related to access to an Active Directory object, you have to enable the Audit directory service
access option.

Question: 3

John works as a contract Ethical Hacker. He has recently got a project to do security checking for www.we-are-secure.com. He wants to find out the operating system of the we-are-secure server in the information gathering step. Which of the following commands will he use to accomplish the task?
Each correct answer represents a complete solution. Choose two.

A. nc 208.100.2.25 23
B. nmap -v -O www.we-are-secure.com
C. nc -v -n 208.100.2.25 80
D. nmap -v -O 208.100.2.25

Answer: D and B

Explanation:
According to the scenario, John will use "nmap -v -O 208.100.2.25" to detect the operating system of the we-are-secure server. Here, -v is
used for verbose and -O is used for TCP/IP fingerprinting to guess the remote operating system.
John may also use the DNS name of we-are-secure instead of using the IP address of the we-are-secure server. So, he can also use the nmap
command "nmap -v -O www.we-are-secure.com ".

Answer: C is incorrect. "nc -v -n 208.100.2.25 80" is a Netcat command, which is used to banner grab for
getting information about the
services running on any port.
Answer: A is incorrect. "nc 208.100.2.25 23" is a Netcat command, which is used to listen to a port for incoming connections.

Question: 4

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

Answer: B

Explanation:
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 a recent problem, the
router is unlikely to be the issue.

Question: 5

You run the wc -c file1.txt command. If this command displays any error message, you want to store the error message in the error.txt file. Which of the following commands will you use to accomplish the task?

A. wc -c file1.txt >>error.txt
B. wc -c file1.txt 1>error.txt
C. wc -c file1.txt 2>error.txt
D. wc -c file1.txt >error.txt

Answer: C

Explanation:
According to the scenario, you will use the wc -c file1.txt 2>error.txt command to accomplish the task. The 2> operator is an error
redirector, which, while running a command, redirects the error (if it exists) on the specified file.
Answer: D and B are incorrect. The > or 1> redirector can be used to redirect the output of the wc -c file1.txt file to the error.txt file;
however, you want to write the errors in the error.txt file, not the whole output.
Answer: A is incorrect. The >> operator will redirect the output of the command in the same manner as the > or 1> operator. Although
the >> operator will not overwrite the error.txt file, it will append the error.txt file.

Question: 6

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 wants to forward all the kernel messages to the remote host having IP address 192.168.0.1. Which of the following changes will he perform in the syslog.conf file to accomplish the task?

A. kern.* @192.168.0.1
B. !*.* @192.168.0.1
C. !kern.* @192.168.0.1
D. *.* @192.168.0.1

Answer: A

Explanation: According to the scenario, John will make the following entry in the syslog.conf file to forward all the kernel messages to the remote host having IP address 192.168.0.1:
kern.* @192.168.0.1
Answer: D is incorrect. This entry will forward all the messages to the remote host having IP address 192.168.0.1.
Answer: B is incorrect. This entry will not forward any message to the remote host having IP address 192.168.0.1.
Answer: C is incorrect. This entry will not forward any kernel message to the remote host having IP address 192.168.0.1.

Question: 7

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 -r
C. netstat -s
D. netstat -an

Answer: D

Explanation:
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: 8

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?
Each correct answer represents a complete solution. Choose all that apply.

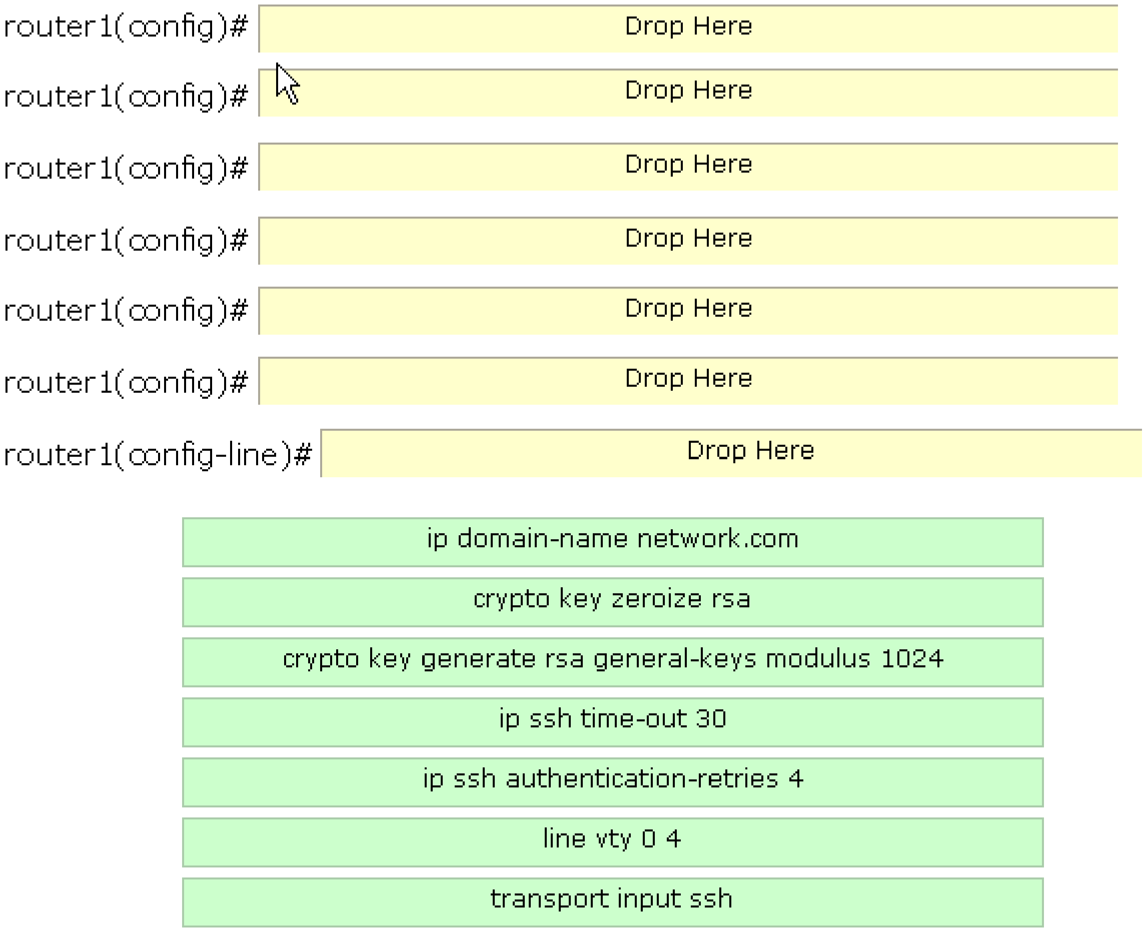
A. 802.11g
B. 802.11n
C. 802.11b
D. 802.11a

Answer: C, D, A, and B

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

Question: 9

You work as a Security Administrator in Tech Perfect Inc. The company has a TCP/IP based network. Three Cisco IOS routers- router1, router2, and router3 are currently working in the network. You want to accomplish the following tasks:
Configure router1 to act as an SSH server.
Configure domain name 'network.com'.
Generate a general-purpose RSA key pair and specify the IP key size of 1024.
Configure SSH time-out of 30 seconds and SSH authentication retries value 4.
Drag and drop the appropriate commands beside their respective command prompts in order to accomplish the tasks.



router1(config)# Drop Here

router1(config)# Drop Here

router1(config)# Drop Here

router1(config)# Drop Here

router1(config)# Drop Here

router1(config)# Drop Here

router1(config-line)# Drop Here

ip domain-name network.com

crypto key zeroize rsa

crypto key generate rsa general-keys modulus 1024

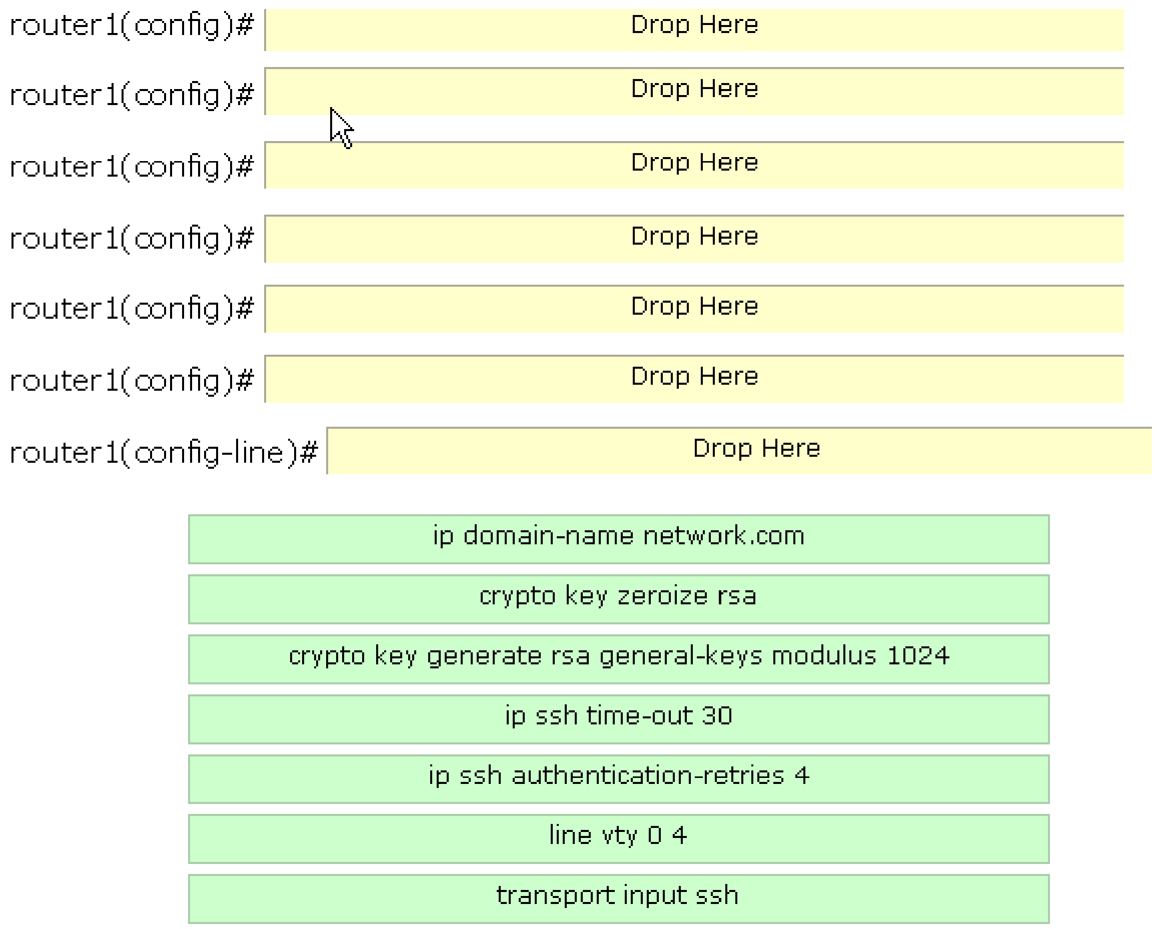
ip ssh time-out 30

ip ssh authentication-retries 4

line vty 0 4

transport input ssh

Answer::



router1(config)# Drop Here

router1(config)# Drop Here

router1(config)# Drop Here

router1(config)# Drop Here

router1(config)# Drop Here

router1(config)# Drop Here

router1(config-line)# Drop Here

ip domain-name network.com

crypto key zeroize rsa

crypto key generate rsa general-keys modulus 1024

ip ssh time-out 30

ip ssh authentication-retries 4

line vty 0 4

transport input ssh

Explanation:
In order to accomplish the given tasks, you will have to use the following commands:

```
router1(config)#ip domain-name network.com
router1(config)#crypto key zeroize rsa
router1(config)#crypto key generate rsa general-keys modulus 1024
router1(config)#ip ssh time-out 30
router1(config)#ip ssh authentication-retries 4
router1(config)#line vty 0 4
router1(config-line)#transport input ssh
```

Question: 10

Which of the following statements about the traceroute utility are true?
Each correct answer represents a complete solution. Choose all that apply.

A. It uses ICMP echo packets to display the Fully Qualified Domain Name (FQDN) and the IP address of each gateway along the route to the remote host.
B. It records the time taken for a round trip for each packet at each router.
C. It is an online tool that performs polymorphic shell code attacks.
D. It generates a buffer overflow exploit by transforming an attack shell code so that the new attack shell code cannot be recognized by any Intrusion Detection Systems.

Answer: A and B

Explanation:
Traceroute is a route-tracing utility that displays the path an IP packet takes to reach its destination. It uses ICMP echo packets to display the
Fully Qualified Domain Name (FQDN) and the IP address of each gateway along the route to the remote host. This tool also records the time
taken for a round trip for each packet at each router that can be used to find any faulty router along the path.
Answer: C and D are incorrect. Traceroute does not perform polymorphic shell code attacks. Attacking tools such as ADMutate are
used to perform polymorphic shell code attacks.

Question: 11

George works as an office assistant in Soft Well Inc. The company uses the Windows Vista operating system. He wants to disable a program running on a computer. Which of the following Windows Defender tools will he use to accomplish the task?
A. Allowed items
B. Quarantined items
C. Options
D. Software Explorer

Answer: D

Explanation:
Software Explorer is used to remove, enable, or disable a program running on a computer.
Answer: A is incorrect. Allowed items contains a list of all the programs that a user has chosen not to monitor with Windows Defender.
Answer: C is incorrect. Options is used to choose how Windows Defender should monitor all the programs running on a computer.
Answer: B is incorrect. Quarantined items is used to remove or restore a program blocked by Windows Defender.

Question: 12

You work as a Network Administrator for McNeil Inc. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. The company's management has decided to provide laptops to its sales team members. These laptops are equipped with smart card readers. The laptops will be configured as wireless network clients. You are required to accomplish the following tasks:
The wireless network communication should be secured.
The laptop users should be able to use smart cards for getting authenticated.
In order to accomplish the tasks, you take the following steps:
Configure 802.1x and WEP for the wireless connections.
Configure the PEAP-MS-CHAP v2 protocol for authentication.
What will happen after you have taken these steps?

A. Both tasks will be accomplished.
B. The laptop users will be able to use smart cards for getting authenticated.
C. The wireless network communication will be secured.
D. None of the tasks will be accomplished.

Answer: C

Explanation:
As 802.1x and WEP are configured, this step will enable the secure wireless network communication. For authentication, you have configured
the PEAP-MS-CHAP v2 protocol. This protocol can be used for authentication on wireless networks, but it cannot use a public key infrastructure
(PKI). No certificate can be issued without a PKI. Smart cards cannot be used for authentication without certificates. Hence, the laptop users
will not be able to use smart cards for getting authenticated.

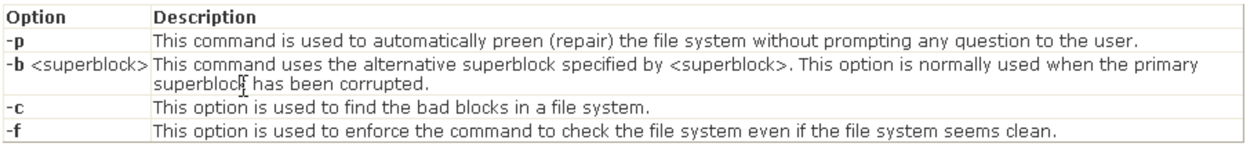
Question: 13

You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to print the super block and block the group information for the filesystem present on a system. Which of the following Unix commands can you use to accomplish the task?

A. e2fsck
B. dump
C. dumpe2fs
D. e2label

Answer: C

Explanation:
In Unix, the dumpe2fs command dumps the filesystem superblock and blocks the group information.
Answer: B is incorrect. In Unix, the dump command is used to back up an ext2 filesystem.
Answer: A is incorrect. The e2fsck command is used to check the second extended file system (E2FS) of a Linux computer.
Syntax:
e2fsck [options] <device>
Where, <device> is the file name of a mounted storage device (for example, /dev/hda1). Several options are used with the e2fsck command.
Following is a list of some important options:



Option	Description
-p	This command is used to automatically preen (repair) the file system without prompting any question to the user.
-b <superblock>	This command uses the alternative superblock specified by <superblock>. This option is normally used when the primary superblock has been corrupted.
-c	This option is used to find the bad blocks in a file system.
-f	This option is used to enforce the command to check the file system even if the file system seems clean.

Answer: D is incorrect. In Unix, the e2label command is used to change the label of an ext2 filesystem.

Question: 14

Which of the following is a wireless auditing tool that is used to pinpoint the actual physical location of wireless devices in the network?

A. KisMAC
B. Ekahau
C. Kismet
D. AirSnort

Answer: B

Explanation:
Ekahau is an easy-to-use powerful and comprehensive tool for network site surveys and optimization. It is an auditing tool that can be used
to pinpoint the actual physical location of wireless devices in the network. This tool can be used to make a map of the office and then perform
the survey of the office. In the process, if one finds an unknown node, ekahau can be used to locate that node.
Answer: D is incorrect. AirSnort is a Linux-based WLAN WEP cracking tool that recovers encryption keys. AirSnort operates by passively
monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.
Answer: C is incorrect. 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, and 802.11n 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: A is incorrect. KisMAC is a wireless network discovery tool for Mac OS X. It has a wide range of features, similar to those of
Kismet, its Linux/BSD namesake and far exceeding those of NetStumbler, its closest equivalent on Windows. The program is geared toward
network security professionals, and is not as novice-friendly as similar applications. KisMAC will scan for networks passively on supported
cards - including Apple's AirPort, and AirPort Extreme, and many third-party cards, and actively on any card supported by Mac OS X itself.
Cracking of WEP and WPA keys, both by brute force, and exploiting flaws such as weak scheduling and badly generated keys is supported
when a card capable of monitor mode is used, and packet reinjection can be done with a supported card. GPS mapping can be performed
when an NMEA compatible GPS receiver is attached. Data can also be saved in pcap format and loaded into programs such as Wireshark.

Question: 15

Which of the following tools works both as an encryption-cracking tool and as a keylogger?

A. Magic Lantern
B. KeyGhost Keylogger
C. Alchemy Remote Executor
D. SocketShield

Answer: A

Explanation:
Magic Lantern works both as an encryption-cracking tool and as a keylogger.
Answer: C is incorrect. Alchemy Remote Executor is a system management tool that allows Network Administrators to execute programs
on remote network computers without leaving their workplace. From the hacker's point of view, it can be useful for installing keyloggers,
spyware, Trojans, Windows rootkits and such. One necessary condition for using the Alchemy Remote Executor is that the user/attacker must
have the administrative passwords of the remote computers on which the malware is to be installed.
Answer: B is incorrect. The KeyGhost keylogger is a hardware keylogger that is used to log all keystrokes on a computer. It is a tiny
device that clips onto the keyboard cable. Once the KeyGhost keylogger is attached to the computer, it quietly logs every key pressed on the
keyboard into its own internal Flash memory (just as with smart cards). When the log becomes full, it overwrites the oldest keystrokes with
the newest ones.
Answer: D is incorrect. SocketShield provides a protection shield to a computer system against malware, viruses, spyware, and various
types of keyloggers. SocketShield provides protection at the following two levels:
1.Blocking: In this level, SocketShield uses a list of IP addresses that are known as purveyor of exploits. All http requests for any page in
these domains are simply blocked.
2.Shielding: In this level, SocketShield blocks all the current and past IP addresses that are the cause of unauthorized access.