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.leads4pass.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 are true about SSIDs?

A. Configuring the same SSID as that of the other Wireless Access Points (WAPs) of other networks will create a conflict.

B. SSIDs are case insensitive text strings and have a maximum length of 64 characters.

C. All wireless devices on a wireless network must have the same SSID in order to communicate with each other.

D. SSID is used to identify a wireless network.

Correct Answer: ACD

SSID stands for Service SetIdentifier. It is used to identify a wireless network. SSIDs are case sensitive text strings and have a maximum length of 32 characters. All wireless devices on a wireless network must have the same SSID in order to communicate with each other. The SSID on computers and the devices in WLAN can be set manually and automatically. Configuring the same SSID as that of the other Wireless Access Points (WAPs) of other networks will create a conflict. A network administrator often uses a public SSID that is set on the access point. The access point broadcasts SSID to all wireless devices within its range. Some newer wireless access points have the ability to disable the automatic SSID broadcast feature in order to improve network security.

QUESTION 2

Which of the following are the countermeasures against WEP cracking?

A. Using the longest key supported by hardware.

B. Changing keys often.

C. Using a non-obvious key.

D. Using a 16 bit SSID.

Correct Answer: ABC

A user can use some countermeasures to prevent WEP cracking. Although WEP is least secure, it should not be used. However, a user can use the following methods to mitigate WEP cracking: Use a non-obvious key. Use the longest key supported by hardware. Change keys often. Use WEP in combination with other security features, such as rapid WEP key rotation and dynamic keying using 802.1x. Consider WEP a deterrent, not a guarantee. Answer: D is incorrect. SSID stands for Service Set Identifier. It is used to identify a wireless network. SSIDs are case sensitive text strings and have a maximum length of 32 characters. All wireless devices on a wireless network must have the same SSID in order to communicate with each other. The SSID on computers and the devices in WLAN can be set manually and automatically. Configuring the same SSID as that of the other Wireless Access Points (WAPs) of other networks will create a conflict. A network administrator often uses a public SSID that is set on the access point. The access point broadcasts SSID to all wireless devices within its range. Some newer wireless access points have the ability to

disable the automatic SSID broadcast feature in order to improve network security.

QUESTION 3

A Cisco router can have multiple connections to networks. These connections are known as interfaces for Cisco Routers. For naming each interface, Cisco generally uses the type of interface as part of the name.

Which of the following are true about the naming conventions of Cisco Router interfaces?

A. An interface connected to a serial connection always starts with an S.

B. An interface connected to a Token Ring segment always starts with To.

C. An Ethernet interface that is fast always starts with an F.

D. An interface connected to an Ethernet segment of the network always starts with an En.

Correct Answer: ABC

A Cisco router can have multiple connections to networks. These connections are known as interfaces for Cisco Routers. For naming each interface, Cisco generally uses the type of interface as part of the name. Following are some of the naming conventions of Cisco Router interfaces:

1.

An Ethernet interface that is fast always starts with an F.

2.

An interface connected to a serial connection always starts with an S.

3.

An interface connected to an Ethernet segment of the network always starts with an E.

4.

An interface connected to a Token Ring segment always starts with To.

QUESTION 4

The Security Auditor\\'s Research Assistant (SARA) is a third generation network security analysis tool. Which of the following statements are true about SARA? (Choose two)

A. It operates under Unix, Linux, MAC OS/X, or Windows (through coLinux) OS.

B. It cannot be used to perform exhaustive XSS tests.

C. It cannot be used to perform SQL injection tests.

D. It supports plug-in facility for third party apps.

Correct Answer: AD

The Security Auditor\\'s Research Assistant (SARA) is a third generation network security analysis tool. It has the following functions:

1.

It operates under Unix, Linux, MAC OS/X, or Windows (through coLinux) OS.

2.

It integrates the National Vulnerability Database (NVD).

3.

It can be used to perform SQL injection tests.

4.

It can be used to perform exhaustive XSS tests.

5.

It can be adapted to multiple firewalled environments.

6.

It supports remote self scan and API facilities.

7.

It is used for CIS benchmark initiatives.

8.

It also supports plug-in facility for third party apps.

9.

It supports CVE standards.

10.It works as an enterprise search module.

11.It works in both standalone or demo mode.

Answer: C is incorrect. SARA can be used to perform SQL injection tests. Answer: B is incorrect. SARA can be used to perform exhaustive XSS tests.

Mode	Switch
Safe Mode	/safeboot:minimal /sos /bootlog /noguiboot
Safe Mode with Networking	/safeboot:network /sos /bootlog /noguiboot
Safe Mode with Command Prompt	/safeboot:minimal (alternateshell) /sos /bootlog /noguiboot
Enable Boot Logging	/bootlog
Enable VGA Mode	/basevideo
Directory Services Restore Mode (Domain Controllers Only)	/safeboot:dsrepair /sos
Debugging Mode	/debug

QUESTION 5

DRAG DROP

Each listener interface method has an event associated with it. Drag and drop the appropriate event names to match the respective listener interface methods.

Select and Place:

Correct Answer:

TheHttpSessionBindingEvent class extends the HttpSessionEvent class.

The HttpSessionBindingEvent class is used with the following listeners:

HttpSessionBindingListener: It notifies the attribute when it is bound or unbound from a session.

HttpSessionAttributeListener: It notifies the class when an attribute is bound, unbound, or replaced in a session.

The session binds the object by a call to the HttpSession.setAttribute() method and unbinds the object by a call to the HttpSession.removeAttribute() method.

HttpSessionEvent is a class that is used with the following listeners:

HttpSessionListener: It notifies the class when a session is created or destroyed.

HttpSessionActivationListener: It notifies the attributes when a session is activated orpassivated.

QUESTION 6

Network mapping provides a security testing team with a blueprint of the organization.

Which of the following steps is NOT a part of manual network mapping?

A. Gathering private and public IP addresses

B. Collecting employees information

C. Performing Neotracerouting

D. Banner grabbing

Correct Answer: C

Using automated tools, such as NeoTraceroute, for mapping a network is a part of automated network mapping. part of manual network mapping. Network mapping is the process of providing a blueprint of the organization to a security testing

team. There are two ways of performing network mapping:

Manual Mapping: In manual mapping, a hacker gathers information to create a matrix that contains the domain name information, IP addresses of the network, DNS servers, employee information, company location, phone numbers, yearly

earnings, recently acquired organizations, email addresses, publicly available IP address ranges, open ports, wireless access points, modem lines, and banner grabbing details.

Automated Mapping: In automated mapping, a hacker uses any automated tool to gather information about the network. There are many tools for this purpose, such as NeoTrace, Visual traceroute, Cheops, Cheops-ng, etc. The only

advantage of automated mapping is that it is very fast and hence it may generate erroneous results.

QUESTION 7

You are responsible for a large network that has its own DNS servers. You periodically check the log to see if there are any problems.

Which of the following are likely errors you might encounter in the log? (Choose three)

A. The DNS server could not create FTP socket for address [IP address of server]

B. The DNS server could not create an SMTP socket

C. Active Directory Errors

D. The DNS server could not create a Transmission Control Protocol (TCP) socket

E. The DNS server could not initialize the Remote Procedure Call (RPC) service

Correct Answer: CDE

There are a number of errors one could find in a Windows Server 2003 DNS log. They are as follows: The DNS server could not create a Transmission Control Protocol. The DNS server could not open socket for address. The DNS server

could not initialize the Remote Procedure Call (RPC) service. The DNS server could not bind the main datagram socket. The DNS Server service relies on Active Directory to store and retrieve information for Active Directory-integrated zones. And several active directory errors are possible. Answer: B is incorrect. DNS Servers do not create FTP connections. Answer: A is incorrect. DNS Servers do not create SMTP connections.

QUESTION 8

You work as the Network Technician for XYZ CORP. The company has a Linux-based network. You are working on the Red Hat operating system. You want to view only the last 4 lines of a file named /var/log/ cron.

Which of the following commands should you use to accomplish the task?

A. tail -n 4 /var/log/cron

B. tail /var/log/cron

C. cat /var/log/cron

D. head /var/log/cron

Correct Answer: A

The tail -n 4 /var/log/cron command will show the last four lines of the file /var/log/cron.

QUESTION 9

Which of the following statements are true about security risks? (Choose three)

A. They can be removed completely by taking proper actions.

B. They are considered an indicator of threats coupled with vulnerability.

C. They can be mitigated by reviewing and taking responsible actions based on possible risks.

D. They can be analyzed and measured by the risk analysis process.

Correct Answer: BCD

In information security, security risks are considered an indicator of threats coupled with vulnerability. In other words, security risk is a probabilistic function of a given threat agent exercising a particular vulnerability and the impact of that risk

on the organization. Security risks can be mitigated by reviewing and taking responsible actions based on possible risks. These risks can be analyzed and measured by the risk analysis process.

Answer: A is incorrect. Security risks can never be removed completely but can be mitigated by taking proper actions.

QUESTION 10

Which of the following types of audit constructs a risk profile for existing and new projects?

A. Technologicalposition audit

B. Technological innovation process audit

C. Innovative comparison audit

D. Client/Server, Telecommunications, Intranets, and Extranets audits

Correct Answer: B

Various authorities have created differing taxonomies to distinguish the various types of IT audits. Goodman and Lawless state that there are three specific systematic approaches to carry out an IT audit:

1.

Technological innovation process audit: This audit constructs a risk profile for existing and new projects. The audit will assess the length and depth of the company\\'s experience in its chosen technologies, as well as its presence in relevant markets, the organization of each project, and the structure of the portion of the industry that deals with this project or product, organization and industry structure.

2.

Innovative comparison audit: This audit is an analysis of the innovative abilities of the company being audited in comparison to its competitors. This requires examination of company\\'s research and development facilities, as well as its track record in actually producing new products.

3.

Technological position audit: This audit reviews the technologies that the business currently has and that it needs to add. Technologies are characterized as being either "base", "key", "pacing", or "emerging". Answer: D is incorrect. These are the audits to verify that controls are in place on the client (computer receiving services), server, and on the network connecting the clients and servers.

QUESTION 11

What are the different categories of PL/SQL program units?

A. Default

B. Unnamed

C. Primary

D. Named

Correct Answer: BD

A named block is a PL/SQL block that Oracle stores in the database and can be called by name from any application. A named block is also known as a stored procedure. Named blocks can be called from any PL/ SQL block. It has a

declaration section, which is known as a header. The header may include the name of a block, type of the block, and parameter. The name and list of formal parameters are known as the signature of a subroutine. Once a named PL/SQL

block is compiled, it gets permanently stored as p-code after compilation in the shared pool of the system global area. Therefore, the named block gets compiled only once.

An anonymous block is a PL/SQL block that appears in a user\\'s application and is neither named nor stored in the database. This block does not allow any mode of parameter. Anonymous block programs are effective in some situations.

They are basically used when building scripts to seed data or perform one- time processing activities. They are also used when a user wants to nest activity in another PL/SQL block\\'s execution section. Anonymous blocks are compiled each

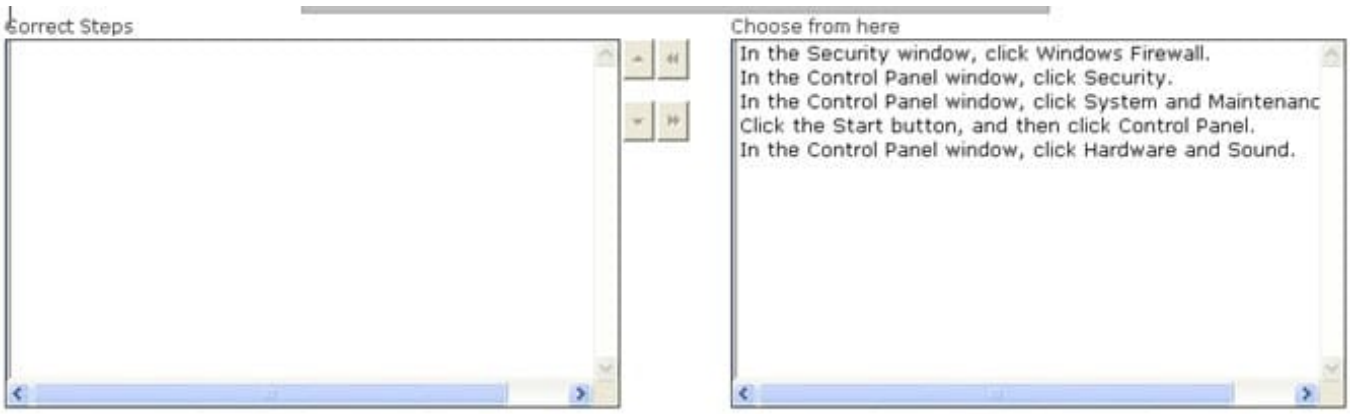
time they are executed.

QUESTION 12

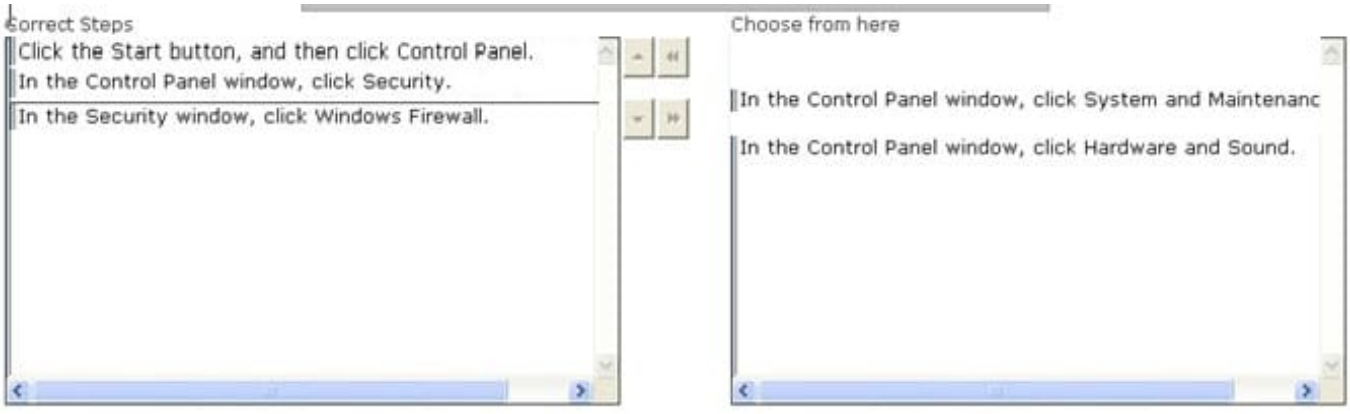
DRAG DROP

You work as a Network Administrator for SoftWorld Inc. All client computers in the company run Windows Vista. You want to view the status of Windows Firewall. Choose in the correct order the steps you will take to accomplish the task.

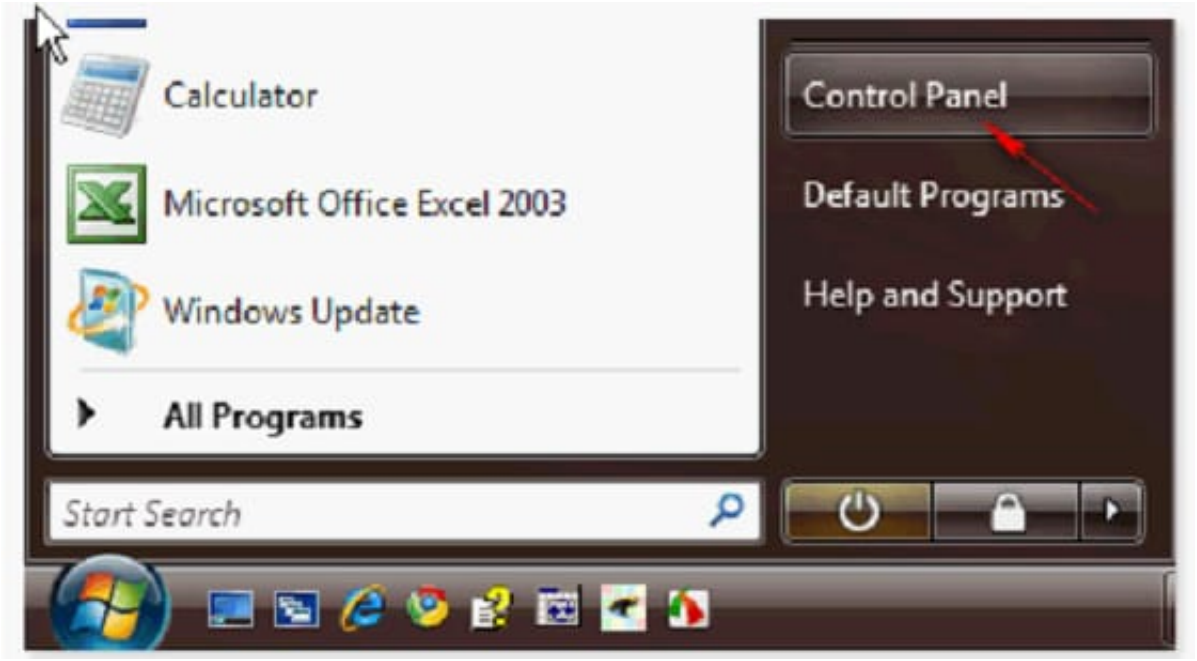
Select and Place:



Correct Answer:

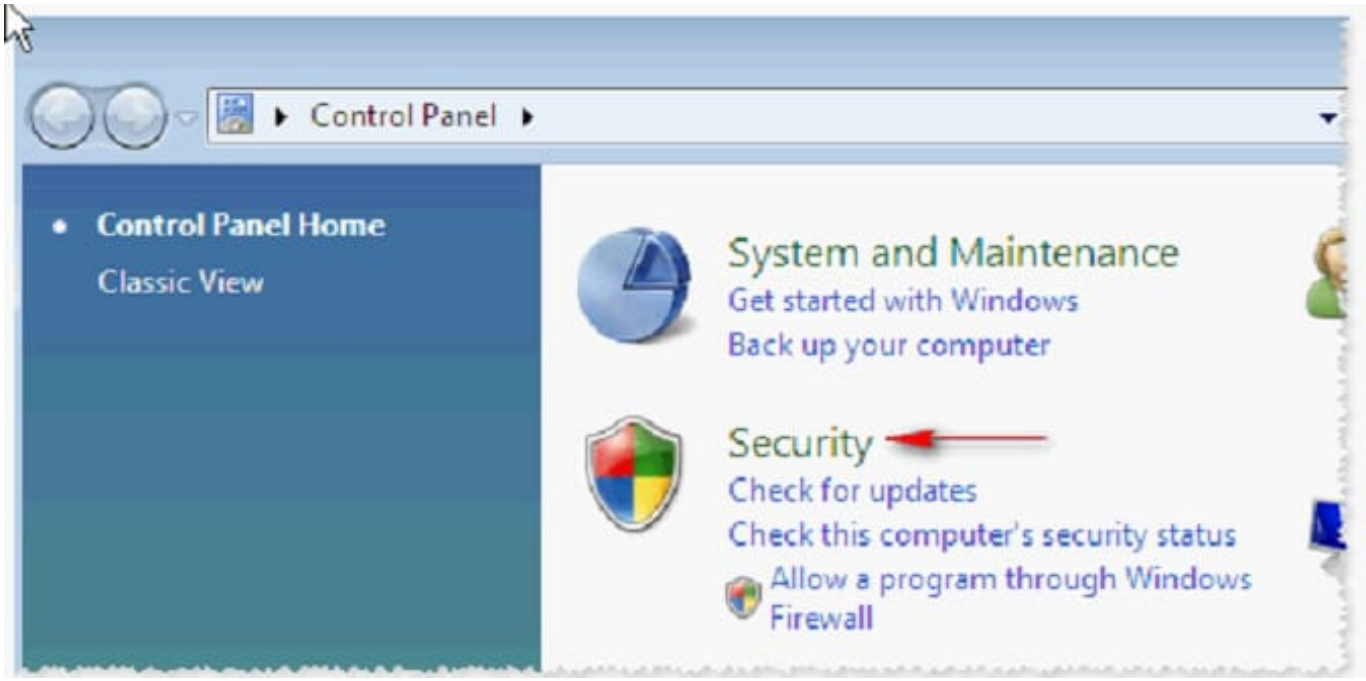


The steps to display the status of Windows Firewall are as follows: 1.Click the Start button, then click Control Panel.



2.In the Control Panel window, click Security.

3.In the Security window, click Windows Firewall.



4.The Windows Firewall dialog box appears, displaying the status of Windows Firewall.

QUESTION 13

TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. The combination of parameters may then be used to infer the remote operating system (OS fingerprinting), or incorporated into a device fingerprint. Which of the following Nmap switches can be used to perform TCP/IP stack fingerprinting?

A. nmap -sS

B. nmap -sU -p

C. nmap -O -p

D. nmap -sT

Correct Answer: C

The nmap -O -p switch can be used to perform TCP/IP stack fingerprinting. Nmap is a free open-source utility for network exploration and security auditing. It is used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port scanners, Nmap is capable of discovering passive services. In addition, Nmap may be able to determine various details about the remote computers. These include operating system, device type, uptime, software product used to run a service, exact version number of that product, presence of some firewall techniques and, on a local area network, even vendor of the remote network card. Nmap runs on Linux, Microsoft Windows etc. Answer: B is incorrect. The nmap -sU -p switch can be used to perform UDP port scanning. Answer: A is incorrect. The nmap -sS switch is used to perform a TCP half scan. TCP SYN scanning is also known as half-open scanning because in this a full TCP connection is never opened. Answer: D is incorrect. The nmap -sT switch is used to perform a TCP full scan.

QUESTION 14

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are- secure.com. He is working on the Linux operating system. He wants to sniff the we-are-secure network and intercept a conversation between two employees of the company through session hijacking.

Which of the following tools will John use to accomplish the task?

A. IPChains

B. Tripwire

C. Hunt

D. Ethercap

Correct Answer: C

In such a scenario, John will use Hunt which is capable of performing both the hacking techniques, sniffing and session hijacking.

Answer: D is incorrect. Ethercap is a network sniffer and packet generator. It may be an option, but John wants to do session hijacking as well. Hence, he will not use Ethercap.

Answer: A is incorrect. IPChains is a firewall.

Answer: B is incorrect. Tripwire is a file and directory integrity checker.

QUESTION 15

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.